Information and Communications Infrastructure

Confidential Presidential Working Paper

August 17, 2007

Table of Contents

Executive Summary

The events of April 16, 2007 and the response, investigation, and recovery at Virginia Tech that followed placed extraordinary demands on telecommunications network resources and university Information Technology professionals. This report provides a comprehensive inventory and analysis of the communications infrastructure and information systems used during this time period. It addresses resources depended upon by emergency responders, investigating law enforcement officers, university officials, media, faculty, staff, students, and families of the university community. It includes information about communications resources owned and operated by the University and relevant resources owned and operated by providers and responders.

To prepare this report, Earving L. Blythe, Vice President of Information Technology at Virginia Tech convened a Telecommunications Working Group (Working Group) including a broad group of experts representing information technology (IT), law enforcement, and university administration.

The report examines multiple areas including:

- Data Communications Utilization and Performance
- Web Communications Utilization and Performance
- Radio Communication Systems Utilization and Performance
- 911 Systems Utilization and Performance
- Cellular Service Utilization and Performance
- Traditional Telephone Service Utilization and Performance
- Video, Campus Cable Television, and Related Systems Utilization and Performance
- Information Technology Support Services
- Data Preservation
- Data Retrieval
- Managing Personal Information
- Response Centers
- Cyber-Security
- VT Alerts Automated Notification System

The main body of the report presents a summary of findings and tactical recommendations drawn from the comprehensive area reports which are presented as appendices.

Principal Findings

The telecommunications infrastructure comprising the data network, telephone system, cable TV, educational systems, and centralized information services on the university campus and in the community was dramatically stressed during the initial response period but performed adequately. Information Technology staff and telecommunications service providers responded to demands by load balancing systems and increasing capacities for network services. Lines connecting the campus telephone system to the public network experienced a five percent blocking rate for a short period in the face of a

three hundred percent increase in the number of call attempts. IT staff equipped eleven temporary emergency command and communications centers with telephones, computers, wireless hubs, faxes, printers, and other needed accessories.

Key contributions of Information Technology were in the areas of information-forensics and data storage and retrieval. Virginia Tech is fortunate to have strong expertise among research faculty and IT professional staff in the area of information security. Forensic information was provided to law enforcement for investigation. Personal records including email, voicemail, filebox, and other information were provided to families of victims.

Communications infrastructure that experienced degradation during the response:

Cellular Telephone Systems

During the initial response period on April 16, local cellular provider networks became congested and blocked calls. In-building coverage was inadequate. The strong and supportive response from service providers is noteworthy. After the initial response period on April 16, cellular providers including AT&T, Sprint-Nextel, Verizon Wireless, and US Cellular all dispatched technicians to increase tower capacity. By April 17, Sprint-Nextel, Verizon Wireless, and US Cellular each had "Cell on Light Truck" systems operating on campus and each had provided emergency-use phones and accessories. Sprint-Nextel installed an in-building antenna system at The Inn at Virginia Tech and worked with Virginia Tech Communications Network Services (CNS) to install an in-building antenna system at the command center in Lane Stadium.

Public Switched Telephone Network (PSTN)

Virginia Tech's campus telephone system connects to the rest of the world through the Public Switched Telephone Network (PSTN). Senior executives with the local telephone service provider initiated contact to offer support to the University early on the afternoon of April 16. The local provider informed us that call volume into the Blacksburg area increased several fold on April 16 and they acknowledge call blocking occurred. The PSTN is engineered to avoid call blocking under normal circumstances, but not during emergencies. This engineering method is the practice nationally.

Emergency Responder Radio Communications

Deficiencies in interoperability and coverage of police, fire, and rescue radio communications are decades-old problems in the United States. Local police and emergency agencies use a variety of radio systems and frequencies and are often unable to communicate directly with each other. Radio systems typically do not support mobile data, encryption, geographic information systems (GIS), and other advanced capabilities. Emergency responders reported radios did not work inside some areas of Norris Hall.

Principal Recommendations

The principal recommendations are strategic in nature. First, the University should develop a new information architecture designed from the ground up for resiliency, performance, applications integration, and ubiquitous access. Second, Virginia Tech should cooperate with community and regional emergency response agencies for development of a fully interoperable mobile communications system with advanced capabilities.

Principal Recommendation 1: A New Campus Information Architecture

The four phases of emergency management are Mitigation, Preparedness, Response, and Recovery. Traditional telecommunications systems have long been critical components for emergency response. But the existing telecommunications system in the United States will not support the innovation possible in emergency management using advancements in processing, visualization, sensors, and myriad other tools. Virginia Tech envisions the creation of a new information architecture capable of facilitating all phases of emergency management including Mitigation (avoidance and deterrence) and Preparedness.

Over the last year, the University has articulated plans to design and build a digital, Internet Protocol-based (IP) information architecture. Planning and design has occurred primarily in the context of creating a next-generation communications system to support the evolving needs of research and education. However, reflection following April 16 has strengthened the realization that the envisioned architecture will greatly enhance all phases of emergency management.

The new system will be founded on a diverse, survivable optical core and ubiquitous wireless and wired access. It will employ advanced network switching and processing technology. The new architecture will connect to the global network with diverse, optical connections to tier one network locations in metropolitan areas.

This new system will take advantage of the resilience inherent in IP-based networks to provide extremely high reliability and availability. It will integrate all types of communications including legacy voice, data, video, entertainment, and educational systems. It will replace aging and obsolete telephone and CATV systems and will augment the capabilities of Virginia Tech's high performance data network. The new architecture will support all types of IP access devices.

Employing innovative new technologies like massive sensor networks, intelligent threat analysis systems, pervasive computing, cognitive radio, and others, the new architecture will be designed from the ground up to facilitate all phases of emergency management. This new architecture has the potential to remediate virtually every problem and enable every innovation identified in this report. It will support education, research, high performance computing, entertainment, and communication needs of the University over the next decade.

Principal Recommendation 2: First Responder Radio Communications

> Virginia Tech should leverage the combined expertise of the multidisciplinary Wireless @ Virginia Tech research group and Information Technology professional staff available to support the efforts of community responder agencies to develop and implement a fully interoperable, advanced mobile communications system in the region. The University should encourage the coordinated effort already underway with leadership from the Virginia Tech Police and Virginia Tech Rescue Squad along with police, fire, and rescue groups from Blacksburg, Montgomery County, and surrounding communities.
>
> The system should be integrated into development of the campus and community IP-based information architecture. This integration will allow the system to take advantage of application development applying geographic information technology, identity management, location awareness, sensor networks, high speed links to state and national criminal information databases, and other resources. Virginia Tech will build on existing and new relationships with industry partners and federal agencies. Together with local responders, the University will coordinate with the Governor's Office of Commonwealth Preparedness.

In addition to these strategic recommendations, the Working Group offered over 120 tactical recommendations specific to particular functional areas. Although few of these recommendations would have been relevant to early detection or mitigation of the events of April 16, virtually all address issues or circumstances that would have made the hours and days following the event less chaotic. They could also be critical to response in different kinds of future emergency scenarios. These tactical recommendations are presented in Section 5 below.

1 Introduction

The events of April 16, 2007 and the response, investigation, and recovery at Virginia Tech that followed placed extraordinary demands on telecommunications network resources and university Information Technology professionals.

Commencing with the onset of the crisis and in the immediate aftermath, the campus communication fabric was subjected to dramatically increased load and unusual use requirements caused by the onslaught of first responders, law enforcement agencies, news media, and inquiries from concerned parties.

During the ensuing investigation, Information Technology resources and staff were called upon extensively in the pursuit of information-forensic data ("cyberforensics"). The collection, storage, and analyses of data regarding all facets of communication and computing for purposes of security and law enforcement are key areas of focus within Information Technology at Virginia Tech. The University is fortunate to have significant expertise in the areas of computing security and information forensics. This expertise was effective in aiding investigation following the tragedy.

During any large scale emergency, reliable, secure, and documented communication is paramount. Recent events including the 2001 terrorist attacks, the 2004 Asian tsunami, and the 2005 coastal devastation caused by Hurricanes Katrina and Rita have exposed weaknesses in the national and global communications systems. They have also stimulated increased interest in the potential to employ new and evolving information and communications technology to enhance prediction, early detection, warning, mitigation, response, and recovery.

The Federal Emergency Management Administration (FEMA) describes four phases of emergency management; mitigation, preparedness, response, and recovery. Telecommunications infrastructure integrity is critical especially during response and recovery. Evolving information technologies promise great improvements in the mitigation and preparedness phases.

The University will learn from this crisis and share the knowledge gained. Virginia Tech will contribute to improvements in the state of the art for resiliency and capability of communications infrastructure and develop strategy to employ emerging technology to mitigate future emergencies at the university level, regionally, nationally, and globally.

2 Report Goals

At the request of Virginia Tech President Dr. Charles Steger, this report has been prepared to review the effectiveness of communications infrastructure related to the tragic events of April 16 and the following response and recovery. This document, including individual area reports presented in the appendices, provides a comprehensive review of all information technology resources. Included are communications infrastructure resources on campus and off campus – as well as in the local and regional areas and beyond. The review includes all modes of telecommunication, wireless and wireline, from all sources including university-owned, responder-owned, and provider-owned. It includes relevant systems such as computing and storage.

The Working Group examined performance, stress-response, and interoperability of all communications elements. The report includes recommendations for rapid, short-term improvements as well as longer term, strategic recommendations.

Virginia Tech will continue to develop and expand the long-term strategy beyond the scope of this report. In the context of emerging technologies including pervasive computing, advanced sensors, next-generation surveillance technology, location-aware applications, cognitive radio, ubiquitous broadband, and many others, members of this Working Group and additional experts and researchers will articulate a plan for a 21st century pervasive communications architecture based on inherently resilient Internet Protocol technology.

Over the last year, the University has been laying the ground work for this new information architecture. The intent is to develop an Internet Protocol-based system fundamentally designed with capabilities to support emergency mitigation, planning, response, and recovery as well as encourage new modes of communication for research, learning, and enhanced quality of life. The goal is to create this new architecture at Virginia Tech to serve as a global model.

3 Methodology and Report Structure

The enterprise telecommunications infrastructure and information storage and retrieval systems serving the broad needs of a large research university are complex. In addition to university owned and operated resources, response and recovery depended on telecommunications infrastructure not owned by the University including local and regional telecommunications, cellular, emergency radio communications, 911, internet, and other information systems.

The Working Group divided analyses into multiple areas and assigned teams of experts to each topic. Team members were drawn from Virginia Tech's Information Technology division, from faculty with relevant expertise, from law enforcement, from outside communications equipment and service providers, and from other expert sources inside and outside the University. A team leader was designated to coordinate the investigative and reporting efforts of each team.

Each team prepared a comprehensive review and inventory of systems, activities, and results within the scope of their assigned areas. The teams examined the effectiveness of systems and identified challenges taking into account recorded performance measurement, comments from interviewed emergency responders and university community members, and observations and records of the University and communications providers.

Teams contacted and visited colleagues at several peer institutions to collect information regarding best practices. Ongoing collaboration is planned regarding development of the integrated information architecture.

The topic areas addressed include:

- Data Communications Utilization and Performance
- Web Communications Utilization and Performance
- Radio Communication Systems Utilization and Performance
- 911 Systems Utilization and Performance
- Cellular Service Utilization and Performance
- Traditional Telephone Service Utilization and Performance
- Video, Campus Cable Television, and Related Systems Utilization and Performance
- Information Technology Support Services
- Data Preservation
- Data Retrieval
- Managing Personal Information
- Response Centers
- Cyber-Security
- VT Alerts Automated Notification System

Teams created individual reports to include a statement of purpose, summary findings, a general description of the system or topic addresses, observations, conclusions, short-term recommendations, and long-term recommendations. A glossary of technical terms is provided in Appendix XIX.

In the "Summary Findings" section below are synopses of cross-cutting findings and recommendations describing:

- How communications infrastructure supported the response and recovery (what worked) and strategic recommendations to develop further capabilities.

- Challenges encountered in certain areas (what needs improvement) with recommendations in summary form. More detailed recommendations are presented in individual reports in the appendices.

4 Summary Findings

The crisis and the response of April 16 placed extraordinary stress on campus information technology resources. The university primary web page experienced nearly the same volume of information requests on April 16 as had previously been recorded during the entire busiest MONTH ever experienced. University and commercial provider telephone systems, data networks, cellular phone systems, and other information services were similarly stretched. The following table summarizes a few of the data highlighting these phenomena.

System	Normal	April 16	Effect
University Web Site Access	455 gigabytes per MONTH (largest ever)	432 gigabytes in a DAY	3000% increase
Virginia Tech Police Dispatch Center	400-500 calls per day	2,027 calls	450% increase
Cellular Provider Capacity and Coverage	Designed for non-emergency peak load, limited in-building coverage	Added 3 COLTs, 2 in-building antenna systems, 200 phones	By April 17, temporary coverage/capacity added
Internet gateway capacity	500 Mbps	Added 1 Gbps over 10GE research link	300% increase
University Switchboard	3,200 calls handled per week	9,878 calls handled 4/16-4/21	300% increase
Telephone calls into Blacksburg Central Office	Reported by local provider		Several fold increase
Virginia Tech Telephone System Inbound Calls	25,000 calls inbound daily on average	75,000+ calls inbound on April 16	300% increase
Centralized Computing Systems Data Storage	Prior to 4/16, roughly 300 Terabytes/day	Since 4/16, over 600 Terabytes/day	100% increase
Data Preservation (12 week period)	3,000 tapes	11,700 tapes	390% increase

The Working Group identified several elements of the communications infrastructure which present opportunities for improvement. Some represent “low hanging fruit” actions the University can take by reconfiguring existing technology or by implementing changes using comparatively simple or readily available solutions.

Longer term, strategic opportunities were identified involving fundamental research and development, substantial investments, and/or innovation in policy, methods, and technology across multiple disciplines. Many of these strategies are already underway.

4.1 Communications Infrastructure and Information Technology Supporting Response and Recovery (What Worked) and Future Strategy

4.1.1 Campus Telecommunications Network Infrastructure and Future Direction:

Virginia Tech operates a high performance Internet Protocol-based (IP) data network providing communication among computers with a diverse, reliable fiber optic core and modern wireline and wireless access services throughout campus. Like other major research universities, the capacity and capabilities of Virginia Tech's data network exceed the characteristics of networks at other types of enterprises. Advanced, high performance computing and high performance network technology and widespread access are required for competitiveness in modern scientific and engineering research.

Virginia Tech also owns and operates campus telephone and cable television (CATV) systems serving academic, administrative, and residential areas of campus. This existing infrastructure is relatively old, though well maintained.

University Information Technology Support Services (ITSS) provides centralized management, monitoring, and user support. The Virginia Tech Operations Center (VTOC) provides monitoring and management of all campus communications network infrastructure including the IP network, the telephone system, the CATV system, as well as centralized IT services. The VTOC also provides monitoring and management support for Virginia Tech's statewide and regional network programs including NetworkVirginia, the Mid Atlantic Terascale Partnership (MATP), VORTEX, and National LambdaRail (NLR). University Computing Support (UCS) provides technical support to the university community for an array of information services.

Response: Internet Capacity

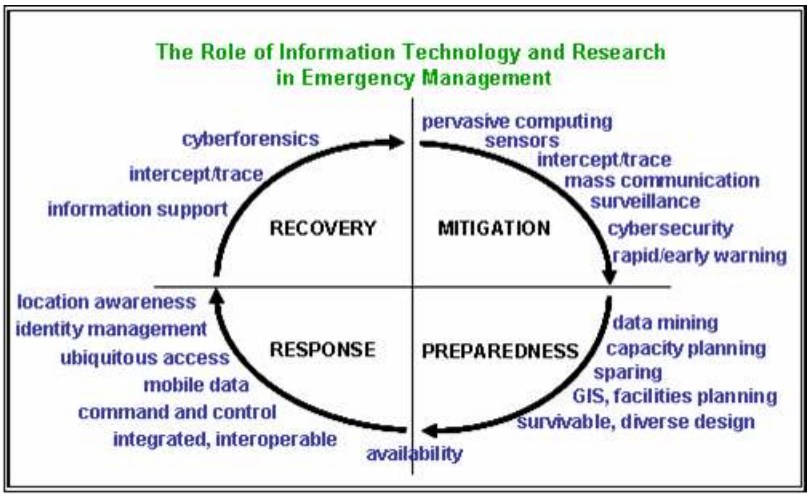
During the crisis response, University Network Operations Center staff monitored a dramatic increase in load on network resources. Anticipating a shortage of capacity to the Internet, network engineers reconfigured a National LambdaRail research network connection to add 1 Gbps capacity to Level3 commodity internet service. This change was accomplished in less than 30 minutes avoiding a bottleneck in information flow over the internet.

During the response period, university network infrastructure systems and support services experienced increased load but performed adequately. The campus telephone system processed calls without internal failures or blocking although blocking was experienced on the lines connecting the campus and the town of Blacksburg to outside telephone services. This blocking is addressed in the "Traditional Telephone Systems" report and recommendations appearing elsewhere in this document. The cable television system was essentially unaffected. Data network engineers were able to make on-the-fly adjustments, as reported in detail in the Data Network section, to increase network capacity where needed and to open access to the campus wireless data network for emergency responders.

During the crisis, University faculty and staff responsible for development and management of these infrastructure facilities were primarily involved with carrying out requests to install telephone and data communications for temporary command, response, and counseling centers. They adjusted network resources to balance unusual traffic load, and did whatever was necessary to assist law enforcement, administration, university community members, and families. Small gaps were identified during the course of the analyses (and reported in the respective individual reports) but the bottom line is the Virginia Tech data, telephone switching, video, and instructional systems infrastructure was essentially effective in supporting responders and the university community in the face of the increased load with no significant breakdown.

However, Virginia Tech has for some time been developing a vision to create a new, next-generation information architecture capable of going beyond the mode of simply supporting the response phase in an emergency situation. Prior to April 16, the University articulated plans to create a new information architecture built from the ground up to provide a platform for all stages of emergency management including mitigation or avoidance.

The University is on the cusp of replacing the legacy, separate data, telephone, and CATV systems with a digital, fully integrated, IP-based multimedia communications architecture. The new architecture will be based on a diverse fiber core using state of the art optical technology designed to survive multiple environmental hazards. It will provide ubiquitous, very high capacity access with a combination of wired and wireless services and will support virtually any type of access device. The traditional distinctions between telephone, video, data, and instructional systems applications will disappear. The new architecture will support integrated multimedia applications, advanced security and authentication capabilities, and new features including sensor networks and pervasive computing models.



With respect to emergency management, the new information architecture will create the capability to integrate virtually all communications infrastructure and information systems to assist with all phases of emergency management, including mitigation and preparedness in addition to response and recovery. These new capabilities will be under the complete control of university administration, law enforcement, and emergency responders.

Virginia Tech intends to build the new architecture to serve as a next-generation communications model for universities, communities, and enterprises.

4.1.2 Information Forensics

A key contribution of Information Technology during the response and recovery efforts has been support to law enforcement and university administration in pursuit of information forensics, often referred to as "cyberforensics." Virginia Tech is fortunate to have particular expertise in multiple areas related to cyberforensics and information security at both professional IT and research levels.

Communications systems and databases required to operate the Information Technology enterprise create and store data which are highly valuable for memorializing events and carrying out subsequent investigation. With appropriate authorization, IT personnel are called upon to provide information stored in e-mail, web, and administrative systems as well as call records and assistance for call intercept and call tracing for law enforcement. For security purposes, the University invests significant effort and resources into collecting, protecting, and managing personal information required for authentication of persons using network and computing systems as well as for other administrative and academic functions.

Information contained in data stores from email, fileboxes, ePortfolios, voicemail and other university resources may be helpful to families seeking personal information pertaining to loved ones who were victims of the tragedy. The preservation of such information and management of release requires significant attention.

On April 16, the University halted routine recycling of backup tapes for centrally managed systems and expiration of system logs and began preserving data from these systems including content for selected individuals. In recent years, the volume of data created by the proliferation of computing has led to an explosion in requirements for data storage. The requirements created by the event, however, has more than doubled the volume of daily storage from roughly 300 Terabytes per day to over 600 Terabytes per day. More than 11,700 backup tapes have been acquired to date.

Privacy concerns, legalities, and business practices make the handling of this information delicate and complex. Stewardship of confidential information is a paramount concern. Federal and state regulations including the provisions of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) must be observed. Virginia Tech requires involvement of university legal counsel to process requests for release of confidential material or information which may infringe upon privacy.

One Working Group team conducted a thorough review of this area. Their detailed observations and findings together with recommendations for improvements and opportunities to leverage this information in new ways are presented in the attached report entitled "Data Retrieval".

4.1.3 Routing of Cellular 911 Calls

Anecdotal concerns regarding the routing of cellular calls to local emergency 911 call centers have been raised. As presented in detail in the attached report "911 Systems

Performance," a team investigated these concerns. They also reviewed system configuration and performance and interviewed law enforcement officers and Information Technology specialists with the Virginia Tech, Blacksburg, and Christiansburg police departments and with the Montgomery County Sheriff's office.

Problem Identified: PSAP Forwarding

While investigating cellular 911 call routing, the review team discovered wireless calls from campus were being transferred from PSAP consoles to non-emergency lines within the Virginia Tech Police dispatch center rather than to designated 911 emergency lines. This did not result in dropped calls on 4/16 but was identified as a procedural error and corrected.

The review concluded that calls to 911 from both wireline and wireless phones were, in fact, effectively routed through the provider cellular network and by local police divisions which receive those calls. Cellular 911 calls are routed to an assigned local Public Safety Answering Point (PSAP) associated with a cell tower sector. Calls originating on the Virginia Tech campus would be expected to be routed to PSAPs at either the Blacksburg Police Department or Montgomery County Sheriff dispatch centers. Those originating on campus are forwarded from the PSAP to the Virginia Tech Police dispatch center. While the overall call volume including non-emergency calls at the Virginia Tech police department was extraordinarily high on April 16, the number of cellular 911 calls originating on campus requiring transfer routing did not place a significant burden on the system.

The review did identify a configuration issue which has been remedied as a result of the review. The report offers strategic recommendations for the 911 Dispatch Center not related to call routing. The most pressing of the needed changes are to 1) create a back-up location Center in the event the existing Sterrett Facilities Complex becomes compromised, and 2) make personnel or policy (non-infrastructure) provisions to handle dramatic increases in call volume during emergencies.

4.1.4 Command and Call Centers

Information Technology played a significant supporting role in the rapid provisioning of several command and call centers set up to respond to the events of April 16. Eleven specialized centers were established to respond to the needs of parents and families, emergency responders, law enforcement, counseling, university development, and media.

Virtually all IT staff pitched in to physically assist as required to rapidly install phones, faxes, wireless network access hubs, computers, printers, cable TV, and other communications facilities as requested. Supplies were retrieved from inventory, borrowed from non-priority facilities, and purchased on an emergency basis as needed.

Response: Parent Information Center

One call center, the Virginia Tech Parent Information Response Center was set up in a lab in the Network Infrastructure and Services building on the afternoon of April 16 upon determination that the Dean of Students office could not accommodate it. CNS employees pitched in around the clock to provide direct support to this Center including running down information, and providing food and drink while it operated in the building.

Call and command centers included:

- Virginia Tech Parent Information Response Center in Research Building 14 (NI&S)
- Public Information Office in Burruss Hall.
- University Relations Media in Alumni Center Board Room.
- Student Assistance at The Inn at Virginia Tech, later relocated to Squires.
- Command Posts for Virginia Tech Police, State Police, Federal Bureau of Investigations, and Bureau of Alcohol, Tobacco, and Firearms at Burruss Hall, Lane Stadium, and the Airport.
- Alumni Development in Research Building 14 (NI&S)
- College of Engineering Center in Durham Hall

One problem encountered, particularly in the Parent Information Center was difficulty responding to callers who spoke languages other than English. The review team offered a recommendation that the University develop a resource list of individuals with foreign language skills to assist in emergency situations.

4.1.5 VT Alerts Emergency Notification System

A significant challenge during an emergency is providing mass notification of a threat and instructions for response. Prior to April 16, University Relations used seven methods of communicating urgent messages to members of the university community. All of these methods were used on April 16:

- Broadcast e-mail to @vt.edu addresses (via LISTSERV)
- Broadcast voicemail to campus phones (offices and residence halls)
- Recorded message on the WeatherLine/Hotline (540/231-6668)
- VT.edu (www.vt.edu) and the Virginia Tech News website
- University switchboard
- Public media (TV, radio, news websites)
- Siren system

Fast Track: VT Alerts Implementation

Virginia Tech was working on implementing an automated notification system prior to April 16 and had a specification in hand. Once the decision to expedite was made, the university completed evaluation and contract negotiation by May 16. The system was installed, configured, advertised, and operational by July 2. Second to the System X supercomputer, this is probably the fastest large scale IT project completed in recent times.

The University had been considering the implementation of an automated event notification system to provide delivery to multiple contact modes simultaneously in the event of an emergency. The purpose of these systems is to provide hosted services that can send emergency messages, or other communications, to cellular telephones or other wireless devices through SMS (Short Message Service; so-called text messaging), through e-mail, or to voice services. The University elected to expedite implementation of a VT Alerts automated notification system.

Virginia Tech students, faculty, and staff can now subscribe to an automated event notification system that will notify them of an emergency situation. Each subscriber can select up to three different methods to be contacted. These contact methods include:

- Text message (SMS) to mobile devices
- Instant message (AOL, MSN, ICQ, and Yahoo)
- E-mail (including non-Virginia Tech addresses)
- Phone call to office
- Phone call to residence
- Phone call to mobile number
- Phone call to another destination

All of the above methods of urgent and emergency communications have been branded as "VT Alerts". The part requiring subscription is referred to as VT Alerts Automated Notification System and it augments the prior methods of notification which will still be used.

Members of the university community are not required to subscribe and may "opt-in" at their discretion. An aggressive public relations campaign was undertaken to advertise availability of the system to faculty, staff, and students. During the first week of operation, more than 4,000 people subscribed and subscriptions continue at a brisk pace.

4.2 Infrastructure Challenges (What Needs Work)

The Working Group identified areas where the existing communications infrastructure posed challenges to response and recovery efforts following the events of April 16 and/or possible future emergencies. Following are summary descriptions of these identified challenges. Individual area reports included in the appendices provide more detailed information and recommendations.

4.2.1 Cellular Phone Service

One challenge is inadequate cellular phone coverage and provider capacity on the university campus and within the surrounding community.

First responders reported there were locations in the vicinity of Norris Hall where they were not able to make and receive calls. During the incident and the hours that followed, specific campus locations identified as having poor cellular coverage also include Derring Hall, Durham Hall, Whittemore Hall, War Memorial Hall, Squires Student Center and The Inn at Virginia Tech.

Network congestion accounted for many of the incomplete call attempts individuals experienced. Wireless carrier radio frequencies that do not easily penetrate buildings account for the areas of no service or marginal signal strength.

Wireless carriers serving the Blacksburg area built out their networks by adding traditional macro cellular service sites on rooftops or towers in the area to improve coverage and capacity for their customers. These systems were generally designed to provide a reliable quality of cellular coverage in-car or on-street level. Their coverage

objectives did not initially extend to in-building coverage. Some of the area providers routinely augment their systems for sporting events or other university activities such as commencement to accommodate the need for increased capacity.

Several cellular telephone providers serving the Blacksburg area responded quickly to the emergency on April 16 to alleviate congestion and coverage issues and also to provide loaned phones and other equipment to responders.

> *AT&T* – upon monitoring a spike in wireless phone traffic in Blacksburg, AT&T dispatched technicians to add equipment to increase capacity to five cell sites serving Blacksburg.
>
> *Sprint-Nextel* – on Monday, April 16 between 1:30pm and 5:00pm Sprint-Nextel added equipment to expand capacity to cell sites serving Blacksburg. By 6:30pm Sprint began to configure Wireless Priority Access and Priority Dispatch for responders on-site. On Monday evening, Sprint Field Operations personnel were dispatched to install an in-building antenna system for The Inn at Virginia Tech and a Cell on Light Truck (COLT) system was dispatched. Both the in-building antenna system and the COLT were on-air by morning on April 17. An in-building antenna system was also installed to support the law enforcement command center at Lane Stadium with assistance from Virginia Tech Communications Network Services. During the event, Sprint provided 60 batteries, 40 power chargers, and 51 phones.
>
> *Verizon Wireless* – on Monday April 16, Verizon informed Virginia Tech they had monitored a dramatic increase in cellular call volume. Verizon Wireless provided a Cell on Light Truck (COLT) system on the morning of April 17 which was deployed in the vicinity of Litton Reeves with consultation with CNS. Verizon also provided 50 wireless phones with an additional 50 held in reserve in Roanoke. Verizon expedited activation of a new cellular site located at the University Gateway building to improve capacity and coverage.
>
> *US Cellular* – On Monday April 16 US Cellular dispatched technicians to add equipment to existing cell sites. By the morning on April 17, a US Cellular COLT dispatched from Morgantown, West Virginia was operating in Parking Lot B.

Beyond the immediate Blacksburg area, basic availability of cellular phone service could present challenges during future emergencies. Several contiguous rural areas have little or no service. The lack of uniform cellular phone service is a national issue in the U.S. beyond the scope of this report. However, the University has special concern for the region surrounding campus. Some university administrators live in areas where cell phone and pager service does not operate creating potential gaps in the ability to reach them during an emergency. Also, regional institutional and community growth is encumbered by the lack of this basic infrastructure.

Information Technology' Network Infrastructure and Services division will follow through on the following report recommendations:

- With the cellular carriers, discuss any planned coverage improvements to their existing macro-cell networks serving the Blacksburg area.

- Establish a procedure to ensure cellular carrier emergency response groups notify and coordinate with appropriate university personnel regarding their presence on-campus in an emergency.
- Pursue qualification in the Federal Wireless Priority Service (WPS) program to receive calling queue priority with cellular service providers.

During the design and implementation of a new, integrated communications architecture as discussed throughout this report, the University will work with providers to maximize cellular coverage inside and outside buildings on campus. The University will draw on the deep expertise within Virginia Tech's Wireless @ Virginia Tech multidisciplinary research group to address technical challenges and to incorporate innovation emerging from fundamental research into the fabric of the architecture.

4.2.2 Public Switched Telephone Network

The term "Public Switched Telephone Network" (PSTN) refers to the worldwide network of telephone systems. Virginia Tech operates a private telephone system which connects to the PSTN via a group of trunks. Trunks are communication paths that connect two telephone systems allowing callers on one system to talk to callers on another system. All incoming and outgoing calls between the Virginia Tech telephone system and the PSTN are made utilizing this group of trunks.

The local telephone service provider's system serving Virginia Tech and the rest of the Blacksburg community is connected to a regional telephone system in Roanoke via another group of trunks. The number of available trunks in this group determines how many simultaneous calls can occur between the two systems.

Telephone service providers apply historical utilization statistics as part of a capacity engineering process to limit the number of blocked call attempts between telephone systems. The group of trunks between the service provider's Blacksburg and Roanoke system is designed so that not more than five in one thousand calls are blocked under normal conditions. The capacity engineering process does not account for emergency or other extraordinary events.

During the events of April 16, capacity limitations on the trunk group connecting the service provider's Blacksburg and Roanoke systems caused calls between the PSTN and Virginia Tech to be blocked. The service provider has acknowledged that they did experience blocking and that the blocking was caused by a several fold increase in call attempts on April 16.

In the short term, the team recommended a number of tactics to alleviate call congestion during an emergency. One suggestion, for example, is to set up automated call processing on the front end of call centers to shorten and reduce repetitive calls.

Strategically, the team recommends working with telephone service providers to try to influence capacity planning and service availability issues relative to connecting the Virginia Tech telephone system to the PSTN.

More forward looking, Virginia Tech's plan to implement an integrated digital IP network architecture includes plans to migrate telephone services to "Voice over IP" technology.

This strategy provides the most promising prospects for mitigating engineering and capacity issues outside control of the University in the legacy PSTN.

The planned system will connect to the PSTN not over aging regional telephone switching infrastructure but rather through high capacity, diverse optical connections to multiple IP services access points. Virginia Tech already operates such a facility located in McLean Virginia currently providing access to the internet and to research networks including the National LambdaRail. As described elsewhere in this report, network engineers were able to reconfigure data internet access on the fly to increase capacity through this McLean node to avoid congestion on internet network access. Migrating telephone service to this regional, national, and global IP infrastructure will afford to telephony applications the robustness, diversity, and survivability inherent in the internet.

4.2.3 Emergency Responder Radio Communications

Interoperability and coverage of first responder radio systems is a decades old problem in the United States. Virginia Tech Information Technology staff together with faculty from the Mobile and Portable Radio Group and others prepared a major report for the Virginia State Police in 1998 entitled “Implementation Plan for a Statewide Shared Land Mobile Radio System”. The problems and issues addressed in 1998 continue to plague police, fire, rescue, and other emergency responders today.

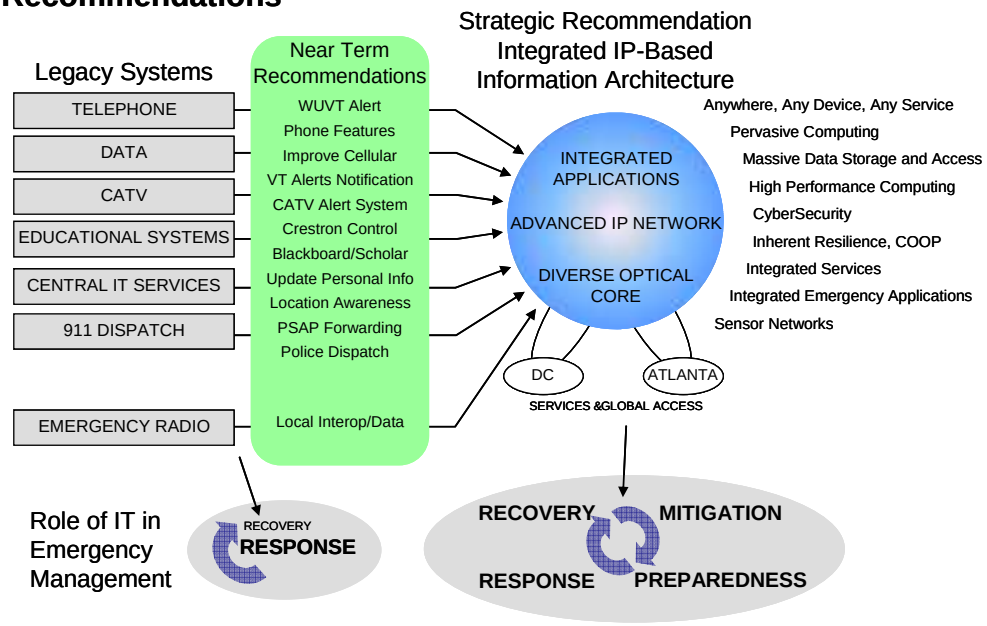
The attached report “Radio Communications Systems” provides details regarding performance of radio systems used by Virginia Tech, Blacksburg, Montgomery County, Virginia State, and other police and rescue responders. Interoperability, coverage, and lack of support for capabilities such as encryption, mobile data, and geographic information systems application support were all cited as problem areas.

In 2004, Virginia established a Commonwealth Interoperability Coordinator’s Office (CICO) within the Governor’s Office of Commonwealth Preparedness. CICO has recently published a 2007 Strategic Plan for statewide interoperability which includes this vision, “By 2015, agencies and their representatives at the local, regional, state, and federal levels will be able to communicate using compatible systems, in real time, across disciplines and jurisdictions, to respond more effectively during day-to-day operations and major emergency situations.”

The CICO Strategic Plan contains excellent information. While 2015 may be a realistic goal for full statewide interoperability, the local community should pursue a more aggressive schedule for achieving interoperability and implementing advanced capabilities. Virginia Tech has significant expertise within the Wireless @ Virginia Tech research group and experience within Information Technology and the Virginia Tech Police Department to help drive the capabilities, interoperability, and coverage of campus and surrounding community radio infrastructure.

The IP-based information architecture planned at Virginia Tech will provide a foundation for development, testing, and deployment of advanced first responder communications. For example, new-generation dispatch consoles use LCD touch screens allowing hierarchies of virtual buttons to be configured for more flexible and powerful controls. They can connect to radio repeater controllers over an IP network which simplifies cabling and permits repeaters to be located or relocated almost anywhere.

Communications Infrastructure Tactical and Strategic Recommendations



5 Tactical Recommendations

This section contains summary excerpts of short-term, tactical recommendations. More details for each section are included in the reports appearing as appendices.

5.1 Data Communications Utilization and Performance

- Improve the upstream network capacity to commodity Internet service providers to ensure appropriate bandwidth is available to keep pace with escalating needs. Web hosting and other services will increase the need for capacity to serve additional users and allow the distribution of richer content.
- Further develop multiple, physical access routes to upstream service providers to ensure there is no single point of failure that could compromise data communications.
- Begin to upgrade network backbone equipment to increase capacity, decrease vulnerabilities, and allow for increased tuning of configuration.
- Ensure building distribution systems have enough physical connectivity for rapid expansion and network bandwidth headroom by including those needs as part of the network infrastructure plan.
- Ensure the requirements to support necessary Virginia Tech personnel working from home or other remote locations are in the University's Continuity of Operations planning.
- Determine other services that may benefit from the redundancy and increased capacity provided by load balancing.
- Improve the efficiency of the process for provisioning guest access.
- Acquire the wireless network management software used during the response period.
- Develop a more automated DNS process to update the system.
- Increase inventory of spare equipment and parts to facilitate rapid deployment.
- Develop processes for rapid reassignment and access to motor pool vehicles during emergency deployments.
- All departmental emergency support plans should include provisions to support emergency personnel basic needs during a crisis situation. For example, water, food, and appropriate storage for medication will be supplied.

5.2 Web Communications Utilization and Performance

- Develop and deploy servers and applications supporting all centralized web communications and the associated databases that allows, at a minimum, a fully redundant, load distributed system that can be easily expanded or upgraded without loss of service.
- Review and update the agreement with a sister institution to host a web presence for the University during emergency situations.

5.3 Systems Support Utilization and Performance

- A review of which PIDs provided to the listserv distribute application has been conducted. This list will be more inclusive and be delivered in a timelier manner.
- Evaluate the web interface used by University Relations to determine if it should be adjusted to change the default to “Immediate Delivery” to avoid confusion and possibly eliminate the delivery delays experienced during this event.
- Implementation of a separate page for emergency announcements only --such as www.emergency.vt.edu-- could provide more immediate information distribution with less manual intervention required.
- Provide a site requiring authentication so only Virginia Tech affiliates could reach it, leaving generic, public browsing to another page. If such a methodology were deployed, we must ensure the authentication services are robust enough to handle the process, but the additional traffic there could be offset through increased use of the Virginia Tech Portal (My VT).
- Discussions between the application administrators (DBMS), the systems administrators (Systems Support), and University Relations should be held regularly to ensure a seamless transition when emergencies force changes.
- Continue to provide a pool of additional servers, similar to the arrangement in use for the Virginia Tech homepage, which can be moved into production if and when necessary.
- Add a third production server to support increased use and provide a failover system to improve reliability.
- Expand use of this service, which includes the ability to create group chat rooms on-the-fly and allows for secure communications (through SSL).
- An integrated announcement system, to include the new VT Alert Automated Notification System as well as all existing and potential future announcement mechanisms (e-mail, IM, radio, cable TV, Web postings, RSS feeds, public address system, etc.), should be developed. The goal is to enable a rapid, multi-tiered/multi-modal communication system through an easy-to-use, web-based interface.
- Redundant hardware should be reviewed and tested for all communications services (e-mail, web services, portal services, chat/IM services, etc.) for failover reliability and on-the-fly capacity increase.

5.4 Radio Communications Systems Utilization and Performance

- Upgrade the current VTPD dispatch consoles and assess the need for additional primary and backup consoles, including the associated radio room facilities. Install secondary, or backup, consoles and radio facilities in an alternate location for survivability.
- Expand the Virginia Tech Dispatch Center audio recording system.
- Expand Virginia Tech Police and Rescue portable radio caches, including extra batteries and chargers.
- Install vehicle computers with mobile broadband access for Virginia Tech Police and Rescue.
- Consider adding local hospitals to dispatch console and interoperability systems.
- Partner with the Town of Blacksburg and other area agencies to plan cooperative improvements for public safety communications.

- Determine the need for additional radio channels and coverage.
- Integrate GIS-mapping capability into the Virginia Tech Dispatch Center's Computer Aided Dispatch system and implement methods for transmitting the information to first responder operation centers and to first responders in the field.
- Acquire fully equipped mobile command units for the Virginia Tech Police and the Virginia Tech Rescue Squad.
- Consider using cognitive radio technology when available.

5.5 911 Systems Utilization and Performance

- Create a backup location for the VTPD 911 dispatch center in the event the Sterrett Facilities Complex is not available or inoperable.
- Implement procedural changes with the Blacksburg Police Department, Montgomery County Sheriff's Office, and the Christiansburg Police Department to terminate transferred calls on the 911 lines instead of administrative lines.
- Determine what would be required to send overflow calls to the Blacksburg Police Department when the Virginia Tech Police 911 center is busy and implement those changes if appropriate.
- Make provisions for emergency staffing and increased phone coverage to handle increased call volumes.
- Establish ongoing collaboration/regular meetings of area public safety groups and their representatives with Communications Network Services to discuss communications needs.
- Collect data at the VTPD dispatch center regarding incoming calls to the non-emergency line to identify the root cause of any misdirected calls. Implement changes to operating practices in order to reduce the number of calls transferred to the non-emergency/administrative lines.
- Continue site visits to study and review best practices in public safety dispatch environments.
- Redesign the Virginia Tech Police dispatch office to include technology improvements and an appropriately designed dispatch environment and workstations.
- A solution to monitor both phone lines and radio frequencies on a single headset should be implemented.
- Implement interoperability and console-integration solutions to allow field units to communicate with each other and other law enforcement agencies.
- Reverse 911 or 911 Broadcast systems should be utilized to augment the current methods of emergency notification.

5.6 Cellular Service Utilization and Performance

- With the cellular carriers, discuss any planned coverage improvements to their existing macro-cell networks serving the Blacksburg area.
- With cooperation from cellular providers, have phones on hand and wireless data cards on site ready to activate and deploy in an emergency.
- Establish a procedure to ensure cellular carrier emergency response groups notify and coordinate with appropriate university personnel regarding their presence on-campus in an emergency.

- Pursue qualification in the Federal Wireless Priority Service (WPS) program to receive calling queue priority with cellular service providers.
- Develop solutions to enhance cellular coverage on the Virginia Tech campus.
- Consider engaging the Mobile and Portable Radio Research Group (MPRG) and Wireless @ Virginia Tech in an effort to assess and enhance wireless mobility on campus through research of leading-edge technology and infrastructure such as cognitive radio (see Radio Communications Systems Utilization and Performance Report, Appendix IV, Exhibit A).

5.7 Traditional Telephone Utilization and Performance

- Continue to optimize the capacity-planning and resource-engineering practices of the campus telephone systems for improved performance in crisis situations
- Convert analog direct-inward-dial (DID) trunks to integrated services digital network (ISDN) trunks to provide access to calling number information on all inbound trunk resources and to improve audio quality for inbound calls to campus. This long-term project had been underway for some time and was completed on April 20th, 2007.
- Leverage existing, remote access trunks as overflow resources for the primary, inbound trunk group to allow up to 184 additional, inbound calls to campus during peak usage periods. This long-planned project was completed on August 7th, 2007.
- Install a dedicated ISDN circuit for priority personnel to ensure they have access to the PSTN during crisis situations.
- Engage the local service provider to discuss their capacity-planning and resource-engineering strategies relative to crisis situations.
- Investigate the ability to provide an informational announcement to callers before connecting them to an operator to reduce repetitious information exchanges during crisis situations
- Review Communications Network Services' (CNS) departmental emergency plan to ensure the department is positioned to utilize other departmental personnel resources as operators during crisis situations.
- Work with the Virginia Tech Police Department and the local service provider to ensure emergency trace requests are processed expeditiously.
- Replace the current telephone system with components designed to integrate telephony applications into an Internet Protocol-based architecture.
- Engage peer institutions to discuss policies and procedures relative to providing traditional telephone service in a university environment. Focus discussions on the technology, processes, policies, and strategies currently utilized to ensure effective wireline communications during periods of extraordinarily high call volume. Develop an understanding of common issues and concerns by comparing continuity of operations, emergency preparedness, and disaster recovery initiatives. Facilitate ongoing information-sharing sessions with those institutions where future interactions would be mutually beneficial.
- Install the core network infrastructure required to support IP telephony. Develop an implementation strategy for the following telephony features:
  - Malicious call trace
  - Multi-level preemption with precedence

  - Virtual call centers
  - Extension mobility
- Develop a strategy for creating additional diversity with regard to the connectivity between the campus telephone system and the public switched telephone network (PSTN). Engage local telephone service providers to develop a more detailed understanding of capacity-planning and service-availability issues relative to connecting the Virginia Tech telephone system to the PSTN.

5.8 Video, Campus Cable Television, and Related Broadcast Systems Utilization and Performance

- Add a CATV Emergency Alert System (EAS) for use on campus
- Add FM receivers to allow the insertion of both WVTF and WUVT onto the Campus CATV information and instructional channels
- Integrate a CATV EAS with other campus alert mechanisms
- Deploy in-room cabling and equipment required to connect the 71 centrally scheduled classrooms not currently connected to the CATV system or capable of viewing cable TV programming
- Work with the colleges to deploy similar systems in all classrooms not centrally scheduled
- Deploy cable drops and televisions in other key locations
- Replace the current coaxial-based cable system with a digital IP-based CATV system provisioned over the University's highly reliable and diverse data network
- Enhance the current system to enable sending an audible alarm, flashing icon, and/or a text message to classroom Crestron Control systems
- implement server redundancy for the Crestron Control software
- Equip every classroom with a Crestron Control system
- Provide conditioned power for all Crestron Systems
- Investigate the feasibility of deploying enhanced Crestron systems capable of supporting two-way audio/video
- The University should negotiate policies and procedures for the emergency use of WUVT to issue campus alerts and emergency information to the campus community
- Carry WUVT's audio signal on one or more of the Campus Cable TV instructional channels
- Expand WUVT's coverage area by relocating the transmitter to Price's Mountain
- Integrate the WUVT Emergency Alert System (EAS) with other campus alert mechanisms
- Integrate Blackboard and Scholar with other campus alert mechanisms
- Begin discussions with VDOT to determine the feasibility of using the 511 Virginia system to alert travelers to a Virginia Tech emergency
- Investigate using the 511 Virginia system to direct travelers to tune to WUVT for additional information
- Investigate the placement of additional message boards in the Blacksburg/New River Valley region
- Work with local agencies to determine the feasibility of using low-power AM/FM transmitters

5.9 Information Technology Support Services

- The University should regularly review and, as needed, update the process for distributing emergency response information to initial points of contact such as the university switchboard, call centers, and help desks.
- The University should assess the need to provide security to extended areas of campus–including university offices located in the Corporate Research Center--in an emergency situation.
- The University should provide training and detailed information on the campus building layout as it relates to structures north/south/east/west of the drill field. This information is needed when the University enacts the evacuation process.
- Evaluate leveraging the VTOC and UCS staff expertise in call center operations to help answer calls normally delivered to other call centers during times of emergency.

5.10 Data Preservation

- Formulate and present a long-term data preservation methodology to university management
- Continue to move toward disk-to-disk backup. This migration was planned and implementation was in initial phases when the event occurred.
- Continue to encourage movement of users to centrally managed e-mail, storage, and backup facilities
- Establish a task force to study the issue of university-owned and/or controlled data repositories as they relate to ownership of information. Define what is private and personal information versus what is university or public information as required by policy, state, or federal laws
- Establish institution-wide policies and procedures related to data preservation.

5.11 Data Retrieval

- Develop a report for inclusion on the Hokie SPA to provide information on instructors/students by building. This development is already in progress.
- Develop strategies, policies, procedures, and processes for promoting availability of emergency contact information for students and employees.
- Implement an operating policy to ensure that as soon as the University is notified of the death of a student, faculty or staff member, digital files the individual may have held on the e-mail servers, Filebox, ePortfolio, or any future storage services should be backed up in case the information is needed. The digital information should be placed on CDs when the official request for it is received. The content of these files must not be reviewed in the process of retrieving and copying the information.
- Continue to use a university representative to assist a victim's family members. This procedure proved to be a valuable process for determining a family's desire for any digital information and ensuring these files were provided to the proper individual.
- Develop a consolidated and comprehensive personal locator information system while considering personal privacy and security. Much of this information already exists in disparate information systems such as Banner, Hokie Passport, and

telecommunications systems. Existing information such as name, class schedule, emergency contact information, electronic card access logs, photo id, office address, and telecommunication service information could be consolidated into a data warehouse application. Another approach could be to make this information available to a personal locator application via Web Services interfaces to existing information systems.

- Existing personal locator information should be enhanced to include information on lab usage and location information for employee types such as wage and adjunct faculty.
- As telecommunications and pervasive computing systems evolve to include presence information, those sources of information could be made available as well.
- The system should leverage geographic information system (GIS) and computer-aided design (CAD) information as well to improve location based query functionality.
- Use identity management systems as a mechanism for more effectively managing diverse, campus constituent services and populations.
- Develop a consolidated, customized user interface for Virginia Tech Police to access appropriate university information.

5.12 Managing Personal Information

- Create a data policy group to make decisions regarding use, maintenance, and management of personal information
- Continue to make students and employees aware of the VT Alerts Automated Notification System and the importance of providing accurate information to the VT Alerts subscription service
- Educate students and employees about the importance of providing accurate personal information
- Identify additional ways to make emergency notices and information available to those people who are on campus but might not be reached by the VT Alerts Automated Notification Systems
- Provide students and employees with information about the need to manage sensitive personal identifying information
- Provide students and employees with information about how Virginia Tech manages sensitive personal information
- Create a university data stewardship council, selected from responsible positions among data stewards and data users, to review and coordinate implementation of data policies and recommendations
- Undertake an effort to determine the types of emergency contact and locator information needed for faculty, staff, and students
- Evaluate the need for emergency contact and locator information for individuals coming to campus for only a short time. Based on the finding, develop an implementation plan.
- Perform additional integrity checks on data entered into Banner, the Enterprise Directory, and the VT Alerts Automated Notification System
- Use various online processes to present opportunities for people to update their personal information

- Review data stewardship roles and communicate those roles to the university community.
- Classify university data according to Policy 7100, the Administrative Data Management and Access Policy.
- Investigate issues surrounding biometric identification including the associated privacy and security implications
- Create an enhanced, standardized, notification process for any potentially serious exposure of personal identifying information

5.13 Response Centers

- Establish a team to develop an overall plan for call/response/command centers. The plan should address the following:
  - Developing a list of rooms easily able to be converted to call/response/command centers. Rooms should be geographically dispersed around campus and include off-campus locations.
  - Installing phone connections to allow both incoming and outgoing calls
  - Staging phones close to the proposed center locations, ready for deployment
  - Installing Ethernet portals and video connections
  - Identifying computers available for use in a call/response/command center. Sources include the laptop loan program operated by Information Technology Acquisitions (ITA) and university computer labs. Identify labs able to serve as call centers or from which computers can be "borrowed." ITA also has a relationship with hardware vendors allowing computers to be purchased or borrowed very quickly.
  - Identifying software to be loaded on each computer for use in an emergency situation. Address security as part of the setup.
  - Compiling a list of system administrators, along with their contact information, who could be reached to set up computers and load software
  - Equipping every center with operating supplies (e.g. white board, phone books, etc.)
  - Equip every center with a fax machine and printer
- Maintain two "800 numbers' in reserve for use in emergency situations. Ensure the Continuity of Operations Plan (COOP) for the University notes the availability of these numbers.
- Develop a script of Frequently Asked Questions (FAQs) for use by those answering the phones. These questions should include those applicable to any situation and those that are situation-specific.
- Develop a resource list (with contact information) of individuals who speak languages other than English
- Develop a procedure with instructions for the handling of malicious calls.
- Engage the International Association of Campus Law Enforcement (IACLEA) to consult with Virginia Tech about the establishment of command centers
- Provide timely information updates to all university call centers that interface with the public and with university employees
- Implement a unified response center for all responding and emergency teams.
- Develop a plan for establishing emergency call, response, and command centers for critical support areas.
- Conduct drills to test emergency call/response/ command centers deployment.

5.14 Cyber Security

- Improve the provisioning process for wireless guest service during emergency situations
- Ensure critical services have the capacity to handle peak loads such as those occurring during emergency situations
- Continue to enhance off-site redundancy for critical services
- Educate students and employees on the importance of providing accurate personal information
- Provide students and employees with information and standards on how to manage sensitive personal identifying information
- Develop a secure method to allow non-Virginia Tech affiliates to access the Virginia Tech network in an emergency. Ensure the network access provided for guests:
  - supports the ability to identify a resource with an ongoing problem in order to isolate it from the network or require the owner to secure the resource. (See University Policy 7010, Policy for Securing Technology Resources and Services)
  - can be enabled quickly during an emergency
- Upgrade aging equipment to reliably support services that must be available during an emergency situation
- Build redundancy into critical new systems and services
- Improve interoperability of radio communications used by emergency personnel in multiple agencies
- Improve operation of radios and cell phones inside buildings to increase availability of those services. Where radio and cell phone service is poor, using the University's wireless network could be a solution, as long as secure guest access to the wireless data network is provided.
- Evaluate the need for encrypted communications technologies for law enforcement officers
- Establish institutional policies and procedures for data protection, preservation, and retrieval to maintain the security of the data and the privacy of the individual
- Establish a university data stewardship council, with members selected from responsible positions among data stewards and data users, to review and coordinate implementation of data policies and recommendations. Classifying data according to University Policy 7100, Administrative Data Management and Access Policy, will facilitate the work of this council.
- Implement an identity management system to more effectively manage the University's diverse campus constituent services and populations

5.15 VT Alerts Automated Notification System

- Require every eligible subscriber (faculty, staff, and students) to either opt-in or opt-out of VT Alerts automated notification system
- Work with Virginia Tech Police to determine if individuals from outside Virginia Tech (law enforcement and first responders) should be included in the VT Alerts Automated Notification System.

- Identify other individuals, or groups of individuals, who are not students, faculty, or staff, but have a university-related business reason to be on a Virginia Tech campus, and decide if these individuals are eligible to subscribe to VT Alerts Enhanced Notification System.
- Expand the methods for making emergency notices and information available to those people who are on campus, but might not be reached by the VT Alerts notification systems.
- Continue to have personal information in VT Alerts Automated System provided and maintained only by the subscriber.
- Provide kiosks throughout the campus and encourage their use for subscribing to VT Alerts Automated Notification System.
- Develop a single interface from which University Relations can create an urgent message (in both text and voice format) and choose methods for delivery, order, and timing. While messages from VT Alerts Automated Notification System can be sent using one interface, other types of VT Alerts notifications require different interfaces.

Attachment A: President's Charge Letter

VirginiaTech

Charles W. Steger, President

210 Burruss Hall (0131)
Blacksburg, Virginia 24061
540/231-6231 Fax: 540/231-4265
E-mail: president@vt.edu
www.vt.edu www.president.vt.edu

May 25, 2007

Mr. Earving Blythe
Vice President for Information Technology
Campus (0169)

RE: Telecommunications Working Group

Dear Erv:

I very much appreciate your willingness to serve as chairman of the Telecommunications Working Group. As chair, you should appoint other members as you see fit, incorporating the necessary expertise as well as representation of constituents.

The charge to the group is to examine our existing systems and determine what enhancements to them would strengthen our emergency response/notification capabilities in the future and/or propose a new system or systems that might accomplish the task. In doing so, you are encouraged to look at best practices employed by other institutions.

The work of your group should begin immediately, with your report to be completed by August 17. I would also request that you provide me with a weekly update on the progress of the working group.

The group's interim and final reports should be marked "Attorney-Client Privileged Communication" and sent in electronic and hard copy to Kay Heidbreder, University Legal Counsel. There should be no other copies of those documents for file purposes or otherwise.

Thank you, Erv, for providing leadership to this important effort.

Sincerely,

Charles W. Steger
President

ko

Information and Communications Infrastructure: Appendices

Confidential Presidential Working Paper

August 17, 2007

Appendix: Table of Contents

Appendix I: Data Communications Utilization and Performance

Purpose

The purpose of this report is to examine the performance of the university's existing, centrally operated data communications systems which encompass the university Internet Protocol (IP) network including Border, Core, Distribution, and Access network components as well as Remote Access, and Data Center networking systems. The report seeks to determine how these systems performed during the tragedy of April 16th. In the aftermath of those events, with special attention on network performance, network support services, and network operations. The report recommends enhancements that will strengthen the centrally operated data communications systems in the future.

Summary

- The data communications network was effective in supporting information distribution and applications related to the response.
- No user data communications network problems were reported to the Virginia Tech Operations Center during the first week of the response. There were no issues with the data network which hampered either emergency response or longer-term response efforts.
- The incident generated increased network traffic triggering automated monitoring systems alarms. As traffic consistently surpassed the 70-80% capacity mark, network engineers responded to implement capacity increases. Dramatic increases in demand for access to the university website, central e-mail systems, and other information sources combined with increased requirements from media and emergency response personnel were greater than the reductions in traffic volume from routine applications.
- The data communications network supported the needs of law enforcement and the media.

General Description

Virginia Tech's data communications network is comprised of approximately 3,200 active devices providing wired and wireless connectivity to the university community. This report will address the four major components of the university's communications network architecture in addition to remote access to the Data Center systems.

The architecture of the data communications network is divided into four hierarchical components including:

1. **Border** – connects the campus network to external networks including community area networks, the Internet service provider, and national and international research and education networks such as National LambdaRail and Internet2.
2. **Core** – includes campus backbone components located within and between six campus service regions.
3. **Distribution** – includes building backbone components located within building communications rooms.

4. **Access** - provides network connectivity directly to a user's equipment including both wired and wireless connectivity.

Conceptually, a computer connects to the network using access network components--a copper or fiber-optic line or wireless link. The access system carries information to and from distribution system components which aggregate traffic within buildings and then transmit it to core components in one of the six main nodes on the Blacksburg campus. If the information is bound for another university or research laboratory, the core transmits it to a border component which hands off to the National LambdaRail node in Washington, D.C. or another national or international networks.

In addition to the four-part campus network system, this report will address two additional related components:

1. **Remote Access** - includes facilities used to support access to the campus network for persons off-campus or out of the area. Primarily, these services are supported by the modem pool and Virtual Private Network (VPN) systems for use over the Internet.
2. **Data Center** - the university's centralized location for servers and other equipment providing services such as e-mail, accounting, web hosting, and other data services for the university and individual departments and colleges.

Information for this report was gathered from Information Technology, VT Police and University Relations.

Network Performance

This section will discuss how the equipment and architecture of the Virginia Tech internal Internet Protocol (IP) network performed during the recovery period.

All network equipment performed as designed while handling the increased traffic load coincidental with university and public access to resources. While adequate to meet the challenges of responding to this particular crisis, the plan for the university's network infrastructure is to continue to incorporate upgrades and enhancements in order to remain responsive, robust, scalable, and reliable during periods of extraordinarily high utilization.

On-site engineers with specific knowledge of and experience with the network infrastructure at Virginia Tech were able to react quickly to changing conditions and develop proactive strategies to ensure the stability of the network throughout the response period.

The following sections discuss the different parts of the network in more detail.

Border

Observations

- On the morning of April 16th, as the public became aware of the tragic events unfolding at Virginia Tech, the university's high-capacity connections to the global Internet began to experience a dramatic increase in traffic loads. Increased demand for access to the university's information resources (e.g. www.vt.edu) by

the university community and the public at large led to the increased utilization of the network's border capacity.

- At 11:05 AM on the morning of April 16, technicians in the Virginia Tech Operations Center (VTOC) became aware of increased utilization of border resources through automated notifications received from network management/monitoring systems. Engineers worked quickly to configure more capacity to compensate for the increased demand.
- Utilizing in-place resources available through the Mid-Atlantic Terascale Partnership (MATP), the university's network engineers were able to rapidly engage the services of Level 3, a commodity Internet service provider, to provide additional Internet capacity to the university. The additional capacity was delivered via fiber-optic links normally dedicated to research activities associated with National LambdaRail, Internet2, and High-Performance Computing (HPC).
- By 11:00 AM the morning of April 17 the network capacity was roughly tripled by adding a gigabit per second link to the existing capacity. This allowed the campus border network to returned to normal operating status with utilization levels staying well below 50% capacity for the duration of the recovery process. The added capacity at the border is still in operation and available for Virginia Tech's use.

Conclusions

- The architecture of the border network allows rapid increases in capacity as needed.

Recommendations

- Improve the upstream network capacity to commodity Internet service providers to ensure appropriate bandwidth is available to keep pace with escalating needs. Web hosting and other services will increase the need for capacity to serve additional users and allow the distribution of richer content.
- Further develop multiple, physical access routes to upstream service providers to ensure there is no single point of failure that could compromise data communications.

Core and Distribution

Observations

- The core and distribution networks experienced no significant problems throughout the response period. Although the equipment and software used in these networks is more than seven years old, there were no incidents causing loss of network communications throughout the campus.
- Under a different set of circumstances—involving, for example, an act of cyber-terrorism--the network may not remain stable, resulting in large-scale communications outages for the campus. If the network is experiencing loads similar to those during the response period, a notable incident of cyber-terrorism may create less than acceptable network performance.

Conclusions

- The continued use of aged technologies in the core and distribution fabric places the network at risk.

- The vulnerabilities can be resolved by replacing the related network routing and switching equipment.

Recommendations

- Begin to upgrade network backbone equipment to increase capacity, decrease vulnerabilities, and allow for increased tuning of configuration.
- Ensure building distribution systems have enough physical connectivity for rapid expansion and network bandwidth headroom by including those needs as part of the network infrastructure plan.

Access Components

- The network access components provide network connectivity directly to the user's equipment. Network access is provided using Ethernet, Wireless LAN, and remote access technologies such as Virtual Private Network (VPN). The following subsections will discuss each access technology.

Ethernet Access

Ethernet access is provided by twisted-pair, copper cable and is used primarily by desktop computers and servers.

Observations

- All Ethernet access networks performed within normal operating ranges. There were no abnormal alarms or notifications from the monitoring systems. No user problems were reported during the recovery process. As various command and response centers were established on the campus, network technicians extended Ethernet access services to these locations, typically by setting up access equipment in close proximity to network users.
- In 20% of the approximately eighty buildings with more than eighteen data connections and 75% of the approximately one-hundred smaller buildings, the Ethernet access network is connected via distribution networks utilizing aging and/or obsolete technologies that might preclude the use of these sites as command/response centers. In this particular situation, the locations selected for the command centers were such that this limitation was not a factor.

Conclusions

- Due to the capacity of aging and obsolete technologies, not all buildings on campus can support large increases in the number of users. This situation is a potential limiting factor during an emergency response period.

Wireless Access

Wireless access, commonly referred to as WiFi, covers over 90% of Virginia Tech's academic and administrative areas. WiFi was the prime means of access for university visitors during the response period.

Observations

- Approximately 750 members of the press and over 600 members of various law enforcement agencies added many users needing wireless access to the network. The network handled the additional load without incident, but users had problems understanding and utilizing the process for obtaining access. To solve

the access problem quickly and efficiently, Information Technology (IT) opened the wireless network to all users bypassing the normal authentication and authorization processes. This change is discussed in more detail in the Authenticated Network Access section of this report.

Conclusions

- The wireless network performed as designed throughout the response period.
- Opening wireless access to all users exposed the network to potential abuse without appropriate audit trails to indicate a possible offending user.

Recommendations

- (See Authenticated Network Access section)

Remote Access

Remote Access services leverage dial-up modem pool resources and Virtual Private Network (VPN) technology to facilitate off-campus access to Virginia Tech's network. VPN access, in particular, is critically important when a large portion of the university's workforce is working from home or other remote locations.

Observations

- Remote access services performed without triggering capacity alarms, and no problems were reported by end users.

Recommendations

- Ensure the requirements to support necessary Virginia Tech personnel working from home or other remote locations are in the university's Continuity of Operations planning.

Data Center

The Data Center switches provide gigabit Ethernet connectivity to the centralized servers for the university and were upgraded during the summer of 2006.

Observations

- During the response period, the Data Center infrastructure performed as designed. It supported the thirty fold increase in traffic to the university's web servers and all other systems. Physical capacity was available to add the four additional web communications servers to handle the increased traffic.

Conclusions

- The Data Center network is adequate for handling increased traffic on an on-demand basis.

Network Support Services

Load Balancing

Load balancing is a technique used to redistribute work traditionally done on one computer to multiple computers in order to increase the amount of work able to be done and/or provide redundancy. Information Technology supports a fully redundant load

balancing system. An upgraded, fully redundant load balancing system was installed in the Data Center in the summer of 2006.

Observations

- The system administrators for the Virginia Tech homepage requested load balancing service as access to the university's web servers increased during the recovery period. Within four hours of the decision to load balance www.vt.edu, additional servers were online, and all required configurations completed. No problems were reported with access or response once the systems were load-balanced.

Conclusions

- Load balancing services played a crucial role in helping the university's communications systems respond to the extraordinarily high traffic loads experienced during the first days of the response period.

Recommendations

- Determine other services that may benefit from the redundancy and increased capacity provided by load balancing.

Authenticated Network Access

Access to the university's wireless network and to Ethernet connections in campus public spaces is controlled by a device using a unique Personal IDentifier (PID) and associated password to identify and authenticate authorized users. Visitors who wish to use the network normally gain access through a Virginia Tech sponsor.

Observations

- As press and law enforcement personnel arrived on campus, it quickly became apparent that the normal process of registering guests for wireless network access was proving too cumbersome for both visitors and sponsors. The time required for registration, instruction, and the support needed to process each request was too great. The high number of requests from the influx of law enforcement and media personnel required the evaluation of other options.
- Initially, the best solution was to bypass wireless authentication in any building for which Information Technology received multiple access requests. By the morning of April 18th, Information Technology staff determined the best way to handle the large number of visitors needing access to the wireless network was to open access to all users in all locations.
- This approach immediately provided access to everyone who needed it. Information Technology acquired an evaluation license for wireless management software to provide an increased level of network monitoring. The new software assisted in diagnosing wireless problems, but it could not identify the specific party causing the problems. Normal authentication procedures for network access were reinstated on May 17, 2007, prior to the start of summer classes.

Conclusions

- Open access to the network created potential for abuse (distributing spam, initiating denial-of-service attacks, copyright violations, etc.) that could not be traced to a particular individual.

- The evaluated management software proved helpful in diagnosing and rectifying network access problems with user equipment.

Recommendations

- Improve the efficiency of the process for provisioning guest access.
- Acquire the wireless network management software used during the response period.

Domain Name System

The Domain Name System (DNS) translates human-readable hostnames, such as www.vt.edu, to IP addresses the network uses for delivering the request or information. Virginia Tech runs several DNS servers to serve both the campus population and those persons off-campus seeking to utilize Virginia Tech resources.

The process to make changes to DNS requires updates be sent to the Virginia Tech hostmaster. The hostmaster then makes the appropriate changes to the database and restarts the servers for the changes to take effect. DNS is restarted twice a week or as needed by special request.

Observations

- The hostmaster team completed three special restarts during the week of April 16 and five normal restarts during the following two weeks to support changes to the university's computing services in support of efforts related to the tragedy.

Conclusions

- Although the manual DNS update process caused little delay in updating network changes, an automated process would reduce the number of people required, and potentially the amount of time, to make rapid changes to the network.

Recommendations

- Develop a more automated DNS process to update the system.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is used by networked computers to obtain IP addresses and other configuration information from centralized DHCP servers.

Observations

- All DHCP servers worked properly throughout the incident period. In some areas of campus, particularly in Burruss Hall, a user's computer must be registered as an authorized computer to obtain access to the network. Network engineers were able to register the computers installed in the command center, but there were slight delays in configuring the authorization as a result of the necessary security restrictions.

Conclusions

- DHCP performed as designed without incident or user impact.

Network Operations

Network Operations includes the direct resources necessary to design, deploy, operate, and maintain the data communications network. The university, law enforcement, and the media all had needs requiring rapid deployment of network services or quick changes in network configuration. This section will discuss the processes and resources used to provision these services during the response period.

Equipment Deployment

Requests for large increases in the quantity of network ports occurred as command centers were deployed. Displaced employees needed network connectivity in their new locations. Law enforcement personnel from many agencies set up operations on campus. These needs required rapid deployment and configuration of data network services.

Observations

- The equipment deployed came from contingency equipment for in-process projects. This effort depleted the stock of applicable inventory. Network equipment is purchased on a just-in-time basis. As the emergency deployments were not planned, network engineers had some delay in bringing together a few of the smaller items needed to interconnect the equipment.
- In those buildings where new services were most needed, the infrastructure met the demands. However, excess capacity in the building distribution systems was depleted in the process.
- Burruss Hall became a hub of many activities following the event and, therefore, had greatly increased security. Network technicians were delayed gaining entry to telecommunications rooms in Burruss Hall since they did not have the necessary clearance. Departmental and university IDs were not sufficient as a result of the unusual circumstances.

Conclusions

- The deployment process functioned as anticipated. Network engineers were able to obtain the necessary equipment to deploy all requested services with little delay.
- In order for rapid deployment of network resources at the scale required during the response period, buildings must have available infrastructure and distribution capabilities.

Recommendations

- Increase inventory of spare equipment and parts to facilitate rapid deployment.

Internal Communications

Communications between and among personnel in various Information Technology units are critical in the ability to respond rapidly to service requests and discuss potential solutions to developing concerns.

Observations

- During the period starting shortly after the event, many of the external voice communications channels became overloaded making them temporarily

ineffective for communications. Virginia Tech's internal communications systems worked well throughout the recovery period. Communications technologies that worked effectively included the internal phone system, instant messaging, e-mail, cellular short message service, and two-way land-mobile radios. Technologies relying on the voice circuits provided by external vendors reached saturation levels at times making them unreliable for communications. Some of the technologies experiencing problems included cellular phone service, traditional telephone service, and paging.

- A newer technology supporting the recovery process was the IT internal wiki. The wiki is a web application allowing multiple people to create and maintain content on a web page accessible to other authorized individuals or groups. Much of the documentation for data communications and the Customer Support Center's dashboard is maintained on the internal wiki. The wiki proved to be a very effective method for IT staff to locate required information during the response period.

Conclusions

- Relying on outside communications providers proved problematic. All internal communications services remained reliable. In particular, services relying on voice communication services between the campus systems and those supported by external vendors were saturated at times. See Traditional Telephone Service Utilization and Performance and Cellular Service Utilization and Performance reports for additional information.

Transportation

Vehicles are maintained for transportation of equipment and field crew staff. These vehicles are assigned to specific work groups for use in their normal duties.

Observations

- The urgency required to meet the requests for new data services necessitated an increase in staff assigned to field duties. The temporary redistribution of work tasks did not include the temporary reassignment of service vehicles. The problem was solved by shuttling staff using both university and personal vehicles.

Conclusions

- During an emergency situation, reassignment of internal vehicles and easy access to motor pool vehicles is necessary for rapid deployment of new and expanded services.

Recommendations

- Develop processes for rapid reassignment and access to motor pool vehicles during emergency deployments.

Staffing

The organization operates using the Emergency Personnel designation under University Policy 4305—Policy on Authorized Closing (http://www.policies.vt.edu/4305.pdf).

Observations

- The staff's depth of cross-training and skill-level provided the capacity to form numerous additional field teams from across the organization. The short duration of the need for rapid support allowed the entire network engineering staff to dedicate their efforts to incident-related tasks without major delay to the normal pending work.

Conclusions

- Emergency personnel have needs that must be addressed during emergency situations.

Recommendation

- All departmental emergency support plans should include provisions to support emergency personnel basic needs during a crisis situation. For example, water, food, and appropriate storage for medication will be supplied.

Appendix II: Web Communications

Purpose

The purpose of this report is to examine the management and performance of the university's existing, centrally operated web communications systems which encompass the university Web Hosting servers including associated databases and applications. The report seeks to determine how these systems performed during the tragedy of April 16th. In the aftermath of those events, with special attention to the university's home page, news page, and other related pages, the report recommends enhancements that might strengthen the centrally operated web communications systems in the future.

Summary

- The university homepage was the internal and public-facing source for official information and updates.
- The university homepage was changed to a "light" version allowing more users to access information.
- Over the first 30 hours of response, the central web servers received multiple upgrades in an effort to keep up with 150,000 unique visitors per hour.

Description

World Wide Web-based communications have become the ubiquitous standard for distributing information. Virginia Tech uses web distribution for both internal communications and for public use. This technology was particularly important during the response period in providing news and official information about the incident and general Virginia Tech information. The Virginia Tech web services also kept student, faculty, and staff informed about the status of the university and planned events during the recovery.

Information Technology (IT) provides centralized web hosting services for university constituents. The two primary hosting services are Secure Hosting and Filebox. Each service includes all operations and maintenance of the servers, databases, software applications, storage, and network connectivity needed to host web and other content. Users are responsible for managing the content and screen layout including any dynamic elements such as page transitions, changing content, or moving images.

The Secure Hosting service supports about 1,200 websites for the university and its colleges, departments, and organizations. The Filebox service is an Internet-accessible file-storage space for documents, webpages, and similar items allowing university constituents to post information that is accessible to others. Filebox is available to all faculty, staff, and students. All equipment is housed in the university's central Data Center providing the redundant systems necessary to maintain a high-availability service.

University Relations managed the university websites with highest access during the recovery period. These sites include the university homepage at www.vt.edu, the Virginia Tech news page at www.vtnews.vt.edu and other content including general university information and campus maps.

Information for web communications was gathered from staff in Information Technology and University Relations.

System Architecture

The architecture of the system providing web services changed in response to needs encountered during the first week after the event. This document will start with the original configuration as of the morning of April 16th and progress through subsequent changes.

Initially, when a user requested a page from a Virginia Tech website, the request was sent to the single, dedicated Secure Hosting server for processing. Redundancy for this service was provided by a hot standby server that could be in production within minutes of any failure on the primary server. Some webpages also contain dynamic content which was maintained on a database server. Again, a dedicated primary server with hot standby was used for database purposes.

Filebox resides on a pair of load-balanced servers with the content stored on Virginia Tech's Network Attached Storage (NAS) system.

The equipment used for web hosting services is located in the university's Data Center which provides rack space, uninterruptible electrical power systems with generators, air conditioning, and physical security of the equipment.

Observations

As soon as IT learned of an incident in Ambler Johnson, system administrators increased their monitoring of the web servers for signs of potential problems. In the 9:26 AM e-mail to university affiliates, people were directed to www.vtnews.vt.edu for more up-to-date information. Virginia Tech News uses the database service to dynamically present news articles to the user. This process rebuilds the page for each request requiring more resources from the server than the presentation of static content requires. This process works efficiently under normal conditions, but it was too resource-intensive for the number of information requests about the incidents. Additionally, official e-mail notifications and word-of-mouth communications caused people from campus and around the world to start looking for more information about the tragedy and Virginia Tech. The load on the server increased to such levels that users noticed delays of up to thirty seconds or more from the time they made a web request until they received a response.

The first actions to make Virginia Tech's websites more responsive were to reduce the complexity of the content and decrease other heavy uses of the server's resources. University Relations maintains two versions of the Virginia Tech homepage--the standard version and a "light" version that is less resource-intensive in creating and delivering page content. Though the same resources are used, switching to the light version allowed more people access to the critical information, but without the rich content of the standard page. University Relations also switched to the use of static pages thereby releasing server resources used for dynamic page-building. These actions freed resources to support users' requests. This process also included moving the primary information source from Virginia Tech News and making the university homepage the primary web-based information outlet for Virginia Tech.

The move to "light," static content greatly reduced the resource requirements for the main webpages, but others, such as those supporting university maps and other information, still operated with the more resource-intensive, dynamic content. Throughout the day, efforts continued to reduce resource requirements for processing user requests.

The university is currently installing a Content Management System (CMS) to allow changes to many Virginia Tech webpages at the same time. This enhancement will greatly reduce the time it will take to implement changes across multiple Virginia Tech websites and prepare the web hosting service to support other high-access events.

At the same time University Relations reduced resource requirements, IT system administrators were redeploying the hot standby server to function as a dedicated server for the university homepage. This action spread the load previously running on one server to two. System administrators increased the number of users the server could support before refusing connections. This effort provided more people access to the page at a cost of slower response for each user.

Filebox was chosen when an outlet was needed for distribution of audio from President Steger's press conference. Filebox was hosted on a separate dual-server, load-balanced system thereby operating without impacting the main university web server. The web servers remained in this configuration throughout the rest of April 16th, and all systems were monitored extensively throughout the night.

Prior to the April event, the largest month of activity on www.vt.edu involved the transfer of 455 gigabytes of information to service user requests. The amount of traffic on April 16th alone was 432 gigabytes. These statistics imply we need roughly 30 times normal capacity to keep web communications viable during a crisis. This multiplier may need to be higher depending on the content the university wishes to provide during an event and how extensively procedures like switching content to a "lighter" version are able to be used.

On the morning of April 17th, the load to the web servers was still high, and system administrators decided more resources were needed to handle the continuing requests. They determined moving to a multi-server, load-balanced system was the best solution. Within four hours of the decision, using servers from the testbed and other servers recently retired from production, www.vt.edu was load-balanced across four servers. This action resolved all response problems making university information more accessible. The hot standby server previously dedicated to www.vt.edu now became available for other uses.

Well-wishers from around the world sent condolences and comments to the university. To handle these communications, University Relations created a memorial site where people could post their comments to an online guest book. Those comments were available for others to read by dynamically creating pages showing the most recent comment first. The standby server freed up by load balancing www.vt.edu was used to host this service. As the number of comments increased, this server became overloaded to the point where it crashed and required manual intervention to keep it operational. In order to address more important issues, the university moved the memorial site to www.legacy.com on Friday, April 20th.

Conclusions

- The university homepage became the primary, official view of Virginia Tech for people around the world.
- The architecture of the centralized web communication services did not have the excess capacity available to handle extraordinary events.

Recommendations

- Develop and deploy servers and applications supporting all centralized web communications and the associated databases to allow, at a minimum, a fully redundant, load-distributed system that can be easily expanded or upgraded without loss of service.
- Review and update the agreement with a sister institution to host a web presence for the university during emergency situations.

Appendix III: Systems Support Utilization and Performance

Purpose

The purpose of this report is to examine the performance of the university's centrally operated data communications systems during the April 16th event. The report also reviews actions taken to ensure critical functions (Banner, e-mail, Directory Services, Courseware, Windows Domain services) were maintained and to determine what improvements might be made to increase their reliability during emergency events.

Summary

- E-mail services performed well despite the additional load experienced.
- Web services provided by the Virginia Tech homepage were affected by the load, but changes were made quickly (within 4-24 hours) to accommodate the traffic.
- The VT Portal (my.vt.edu) performed well and experienced no disruptions.
- The Instant Message/Chat server (still in pilot in April 2007, but moved to production in July) was used extensively for internal communications and provided much-needed, immediate access to staff who were off-site and whose movement was restricted. This service proved particularly useful when telephone service became congested.

General Description

University Relations began distributing mass e-mails to the entire campus community at 9:26 AM April 16th. The mailings continued throughout the day with little problem (see observations below for specific issues). The Virginia Tech homepage website responded poorly once news of the event was made public until steps were taken by University Relations to simplify/streamline the content. The other systems administered by Information Technology (Banner, Courseware, Enterprise Directory, Data Warehousing, Information Technology Acquisitions, Portal, storage and backup systems, Windows Domains) all performed at optimal levels.

Observations

Electronic mail (e-mail)

E-mail messages were processed at their normal rate throughout the emergency. (See Exhibit A showing comparative graphs on traffic flow.) Broadcast messages sent by University Relations were delivered through the "distribute" function of the Listserv Server. Some constituents (adjunct faculty, transfer students, students who were only "auditing" classes) did not receive the mailings. At least two messages from the University Relations office were delayed by several hours (not actually delivered until after 10:00 PM on 4/16/07). However, an analysis showed this delay to have been the result of staff not selecting the correct delivery time (Immediate versus After-Hours; the default is After-Hours which delivers messages after 9:00 PM).

Virginia Tech Home Page (www.vt.edu)

Stress on the service was well beyond the normal load or any abnormal loads seen up to this point in time. This situation was exacerbated by public interest regarding the day's events and links to the Virginia Tech homepage being posted on various news sites. Previously planned load balancing actions were implemented on April 17th to immediately provide additional resources. Information Technology staff from Communications Network Services (CNS), Systems Support and Database Management Services (DBMS) coordinated activities to improve performance for this critical service. Four hosts are now in the pool for the main page, and others could be easily provisioned in an emergency situation. University Relations, having learned from the "Morva incident," quickly adjusted the page's content--reducing graphical content and removing database calls--to enable it to load more quickly. Statistics showed the number of hits experienced by the homepage on April 16th, 2007 equaled the number normally received during an entire, very busy month.

Virginia Tech Portal (My VT)

This service experienced no noticeable service interruptions or delays. Steps taken after the emergency on the first day of fall semester 2006 included enabling the service with the new CNS load-balancing equipment and repairing a program error that caused channel timeouts. These improvements seemed to pay dividends during the latest emergency situation.

Instant Messaging (IM or chat)

The open source–based ("Jabber") instant messaging server planned to provide individual and group chat functions for most central Information Technology (IT) units has just recently completed its pilot stage and is now in full production mode. Application and systems administration functions are being performed by members of the Systems Support Department, while development and upgrade work is still being handled by the Collaborative Technologies Unit. The IM service was used extensively and performed well during the event. This service provided much-needed contact among IT support staff. Use of this service relieved pressure from the e-mail and telephony systems especially for internal communications.

Conclusions

Lessons learned during the incident on the first day of fall semester 2006 ("The Morva Incident') were put to good use. The Virginia Tech website, now load balanced, should perform more robustly in the future.

Short Term Recommendations

Electronic mail (e-mail)

- A review of which PIDs provided to the listserv distribute application has been conducted. This list will be more inclusive and be delivered in a timelier manner.
- Evaluate the web interface used by University Relations to determine if it should be adjusted to change the default to "Immediate Delivery" to avoid confusion and possibly eliminate the delivery delays experienced during this event.

Virginia Tech Home-page (www.vt.edu)

- Implementation of a separate page for emergency announcements only --such as www.emergency.vt.edu-- could provide more immediate information distribution with less manual intervention required.
- Provide a site requiring authentication so only Virginia Tech affiliates could reach it, leaving generic, public browsing to another page. If such a methodology were deployed, we must ensure the authentication services are robust enough to handle the process, but the additional traffic there could be offset through increased use of the Virginia Tech Portal (My VT).
- Discussions between the application administrators (DBMS), the systems administrators (Systems Support), and University Relations should be held regularly to ensure a seamless transition when emergencies force changes.

Virginia Tech Portal (My VT)

- Continue to provide a pool of additional servers, similar to the arrangement in use for the Virginia Tech homepage, which can be moved into production if and when necessary.

Instant Messaging (IM or chat)

- Add a third production server to support increased use and provide a failover system to improve reliability.
- Expand use of this service, which includes the ability to create group chat rooms on-the-fly and allows for secure communications (through SSL).

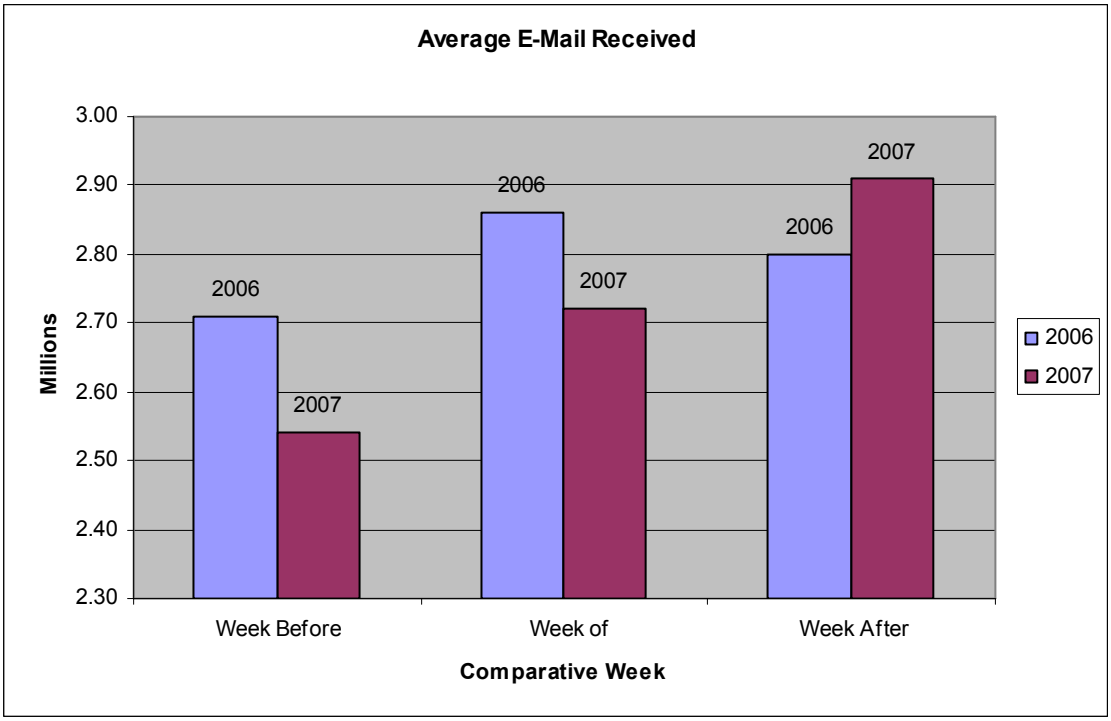
Long Term Recommendations

- An integrated announcement system, to include the new VT Alert Automated Notification System as well as all existing and potential future announcement mechanisms (e-mail, IM, radio, cable TV, Web postings, RSS feeds, public address system, etc.), should be developed. The goal is to enable a rapid, multi-tiered/multi-modal communication system through an easy-to-use, web-based interface.
- Redundant hardware should be reviewed and tested for all communications services (e-mail, web services, portal services, chat/IM services, etc.) for failover reliability and on-the-fly capacity increase.

Exhibit A: E-mail flow for selected periods

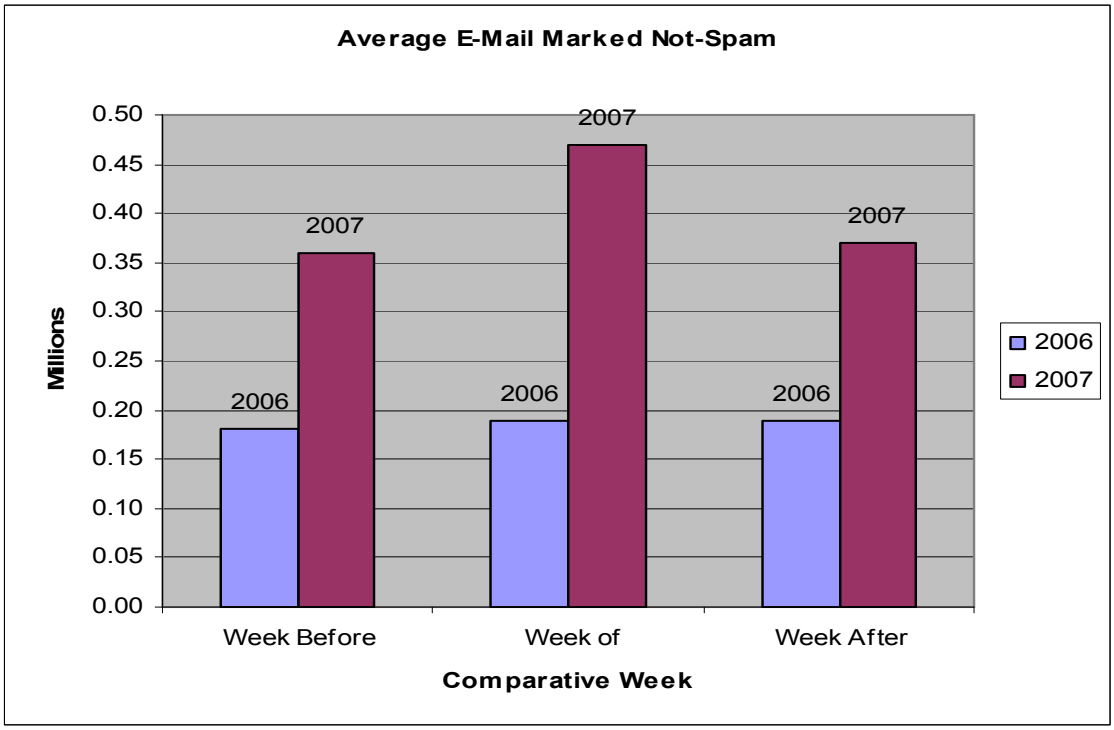
	Last Year (2006)			This Year (2007)		
Averages:	**Week Before**	**Week of 4/16**	**Week After**	**Week Before**	**Week of 4/16**	**Week After**
A. Total E-mail	2.71	2.86	2.80	2.54	2.72	2.91
B. E-mail Marked Not-Spam	0.18	0.19	0.19	0.36	0.47	0.37
(Numbers represent millions of messages received and processed)						

Graph A below displays the number of e-mail messages received during the weeks of April 16, 2006 and 2007 as well as the number of messages received the week before and after. Note the week before and week of the incident showed reduced traffic in 2007, but the week after the event showed increased e-mail traffic. Approximately 110,000 more messages were received in 2007 compared to the same week in 2006.



Graph A

Graph B displays the numbers of messages not tagged as unsolicited (i.e., "spam") for comparative weeks in 2006 and 2007. Note the increase of legitimate (non--spam) messages (approximately 250,000) received during the week of the event as compared to 2006.



Graph B

Appendix IV: Radio Communications Systems Utilization and Performance

Purpose

The purpose of this report is to examine the existing radio communications systems serving the Virginia Tech campus and surrounding area; to determine how these systems performed during the tragedy of April 16th; and, in the aftermath of the tragedy, determine what enhancements may strengthen the systems in the future.

Summary

- The Virginia Tech Police Department (VTPD) radio communications infrastructure includes two dispatch consoles, [Redacted] repeater control radios, a multi-channel audio recorder, [Redacted] radio repeater sites, 15 vehicles with multiple radios, and 80 portable VHF radios.
- The Virginia Tech Rescue Squad radio communications infrastructure includes [Redacted] repeater control unit, [Redacted] radio repeater site, two ambulances with radios, one utility vehicle [Redacted], one patient transport vehicle [Redacted], 45 portable VHF radios, and two portable UHF radios.
- The VTPD Dispatch Center was overloaded with incoming calls following the April 16th incident. Other observations include the following:
  - dispatch consoles could be improved
  - radio interoperability with other agencies is a concern
  - Nextel push-to-talk and cell calls are not recorded
  - extra portable radios and charged batteries were needed
  - better radio coverage is desirable
  - mobile broadband Internet access in vehicles is desirable
  - incident geographic information system (GIS) map information is needed by first responders
  - command vehicles are desirable for Virginia Tech Police and for Virginia Tech Rescue

General Description of the Radio Environment

First responder radio communications infrastructure described in this section includes that of Virginia Tech Police and Rescue, the Blacksburg Fire Department, and other surrounding agencies. Virginia Tech does not have an on-campus fire department.

It is important to note that VHF (Very High Frequency), Low Band VHF, UHF (Ultra High Frequency), and 800 MHz radios use different frequency bands. A radio designed for one band generally will not work with a radio designed for another band. Also, frequency channels in the same band used by agencies within a region are typically different. They may not interoperate or be configured to interoperate.

Virginia Tech Police Department Radio Infrastructure

Radio communication infrastructure for the Virginia Tech Police Department located at the Sterrett Facilities Complex includes:

- Multi-channel recorder for all audio channels connected to the dispatch consoles

- [Redacted] Zetron radio-dispatch consoles with push-to-talk access to repeater control radios (transmitters/receivers/antennas) and direct repeater control for communications with [Redacted] VTPD radio-channel repeaters[Redacted]
- 15 vehicles with multiple radios
- 80 portable radios
- Nextel push-to-talk cell phones

Virginia Tech Rescue Squad Radio Infrastructure

The Virginia Tech Rescue Squad radio communication infrastructure includes the following:

- One repeater control system [Redacted]
- One radio-channel repeater [Redacted]
- Two ALS (Advanced Life Support) ambulances [Redacted]
- One Chevy Tahoe ALS First Response Utility vehicle [Redacted]
- One John Deere 6x4 Gator vehicle converted to patient transport—[Redacted]
- 45 VHF portable radios
- Two UHF portable radios

Blacksburg Fire Department Radio Infrastructure

The Blacksburg Fire Department serves Virginia Tech's campus and the local area. They primarily use VHF radios. The primary and secondary repeaters [Redacted].

The Blacksburg Fire Department has a command trailer on standby for major athletic events and incidents. It contains radios for most frequency bands used in the area, including Low Band-VHF, VHF, UHF, and 800 MHz. The trailer also contains a radio interoperability box that can patch together radios using different frequency bands and channels for intercommunications

Surrounding Agencies and Frequency Bands Used

Surrounding agencies and main frequency bands used:

- Blacksburg Fire (two stations) - VHF
- Blacksburg Police - 800 MHz
- Blacksburg Rescue - VHF
- Carilion Transport - UHF
- Christiansburg Police - UHF
- Christiansburg Fire - UHF
- Christiansburg Rescue - Primary - UHF
- Elliston Fire - VHF
- Floyd County Fire - UHF
- Floyd County Sheriff - UHF
- Giles County Fire - UHF
- Giles County Sheriff - UHF
- Giles Rescue - UHF
- Longshop-McCoy Fire and Rescue - UHF
- Montgomery County Sheriff - UHF
- Montgomery Fire - UHF
- Montgomery Regional Hospital - VHF
- Pulaski County Fire - UHF

- Pulaski County Sheriff - UHF
- Pulaski County REMSI Rescue (Regional Emergency Medical Services Inc.) - UHF
- Radford City Fire and Rescue - VHF
- Radford City Police - VHF
- Radford University Police - UHF
- Radford University EMS – VHF
- Radford-Carilion Rescue - VHF
- Riner Fire - VHF
- Shawsville Rescue - VHF
- Virginia State Police - VHF (STARS—Statewide Agencies Radio System)
- Virginia Tech Police - VHF
- Virginia Tech Rescue - VHF

Observations

Radio Infrastructure for the Virginia Tech Police Department Dispatch Center

The radio system infrastructure for the VTPD Dispatch Center at the Sterrett Facilities Complex includes the radio-dispatch console system, multiple repeater-control radios with associated outdoor antennas, radio repeaters, and a multi-channel audio recording system.

The VTPD Dispatch Center has two radio-dispatch console positions. Following the April 16th incident, the dispatchers were overwhelmed with incoming telephone calls. In addition to radio communications, dispatchers take 911 calls, answer telephone/cell calls, operate a computer-assisted dispatch (CAD) database system, and perform other dispatch functions.

The center's dispatch console system is configured to access [Redacted] radio-repeater channels. Dispatchers can use a console to access one repeater channel at a time, create one patch between two channels, or broadcast to multiple channels. [Redacted] repeaters are accessed with control radios located in the radio room down the hall from the Dispatch Center. Each radio has an external antenna located [Redacted]. The dispatch consoles are ten years old and are no longer manufactured. Repair parts are becoming difficult to obtain.

The console system routes audio from each repeater channel to a multi-channel audio recorder system. This process is required so audio messages and the associated timelines can be reviewed. It is desirable to record other audio communications, including selected Nextel push-to-talk calls, cell phone calls, wireline calls, officer conversations, and field radio simplex transmissions. In the near future, it will be desirable to log and record selected Voice over Internet Protocol (VoIP) calls and instant text messages.

At incident locations, Emergency Response Teams (ERTs) use their portable radios in simplex mode for direct portable-to-portable communications. These communications are not accessible to central dispatch systems; therefore any desired recording must be done by equipment in the field within simplex range of an incident.

Cache of Portable Radios

Agency ERTs responding to a campus incident without an interoperable radio may be assigned a portable radio from Virginia Tech that uses the particular band and frequency for the incident. The VTPD and Virginia Tech Rescue Squad keep caches, or stockpiles, of radios to be distributed during incidents. There was a need for additional portable radios and charged batteries after the April 16th incident. The Virginia Tech Police Department would like each ERT member to have two radios (one for regular duty and the other for ERT). Extra portables would also be used for other major events on campus.

Radio Signal Coverage

Virginia Tech and Blacksburg rescue squads reported their radios did not work in some areas inside Norris Hall. Radio signals are particularly attenuated inside buildings when they pass through dense walls and floors. Because Emergency Response Teams may be using different equipment, frequencies, and repeaters, coverage and performance may vary.

Mobile Broadband Internet Access

Mobile broadband Internet access was not used by Virginia Tech Police and Virginia Tech Rescue Squad during the April 16th incident.

Mobile Command/Response Vehicles

For the April 16th incident, the Blacksburg Fire Department deployed their mobile command trailer to the incident scene. As previously described, it contains radios for first-responder frequency bands used in the area, including Low Band-VHF, VHF, UHF, and 800 MHz. It also contains a radio interoperability box that can patch together radios using different frequency bands and channels for intercommunications.

If multiple incidents occur, the VTPD and Virginia Tech Rescue Squad do not have equivalent mobile command vehicles and/or trailers to deploy. Police command vehicles and rescue command vehicles generally need to be deployed to different locations.

Mobile command vehicles need multi-channel audio recorders to log and record incident communications, including simplex radio conversations.

Technology Considerations

New-Generation Dispatch Consoles and Interoperability Systems

Many first responder agencies sent personnel and equipment to provide aid to Virginia Tech during the April events. As shown in the previous section on "Surrounding Agencies and Frequency Bands Used," we see four different bands are commonly used (Low Band VHF, VHF, UHF, and 800 MHz). Radios for one band will not work with radios for a different band. The Virginia Tech Police Department uses VHF radios. The two closest responding police agencies are the Town of Blacksburg Police Department and the Montgomery County Sheriff's Department. The Blacksburg Police Department uses 800 MHz radios, and the Montgomery County Sheriff's Department uses UHF radios. Most other police/fire/rescue agencies in the area use VHF radios with different

channels. When multiple agencies converge to provide aid for an incident, they need to communicate with each other. If their radios are not directly interoperable, there is a critical need to patch them together via an interoperability system. The interoperability function can be integrated into new-generation dispatch consoles or provisioned as an add-on system.

New-generation dispatch consoles use LCD touch screens allowing hierarchies of virtual buttons to be configured for more flexible and powerful controls. They support patching multiple parallel calls and multiple talk groups together. They can connect to radio-repeater controllers over an IP (Internet Protocol) network, as opposed to the current cabled methods. This process simplifies cabling and permits repeaters to be located almost anywhere an IP network can be accessed. It also facilitates easy relocation of dispatch consoles which would be useful when the Virginia Tech Police Department and the Virginia Tech Rescue Squad move to a new building.

New-generation enterprise wireless, telephone, data, messaging, and video systems use IP networking. The next telephone system at Virginia Tech will likely provide substantial VoIP call capabilities. Almost all wired and wireless computer access at Virginia Tech uses IP. Applications over IP will become increasingly important to first responders for public safety purposes. Virginia Tech currently uses several thousand IP switches, routers, and wireless access points to provide wired and wireless IP network access.

The VTPD could potentially leverage the expertise of the Virginia Tech Information Technology organization to field-test an advanced interoperability system to determine feasibility for production deployment. The City of Danville, Virginia, and Bryant University in Massachusetts are examples of two entities deploying advanced systems.

Mobile Broadband Internet Access

Mobile broadband Internet access service is available in the Blacksburg, Christiansburg, and Radford areas. Currently, the sole provider is Citizens Telephone Cooperative (see http://www.citizens.coop/internet/mobilebroadband.shtm). The service could be used by Virginia Tech Police and Virginia Tech Rescue personnel from their vehicles for a number of applications that currently require personnel to go into the office for computer network access. Use of the service in vehicles would enhance public safety efforts, improve officer productivity, and increase the presence of officers in the field.

There are two main methods for access. One is to plug a wireless adapter card into a portable computer device for direct access to the service. The other is to install a Wi-Fi access router in a vehicle with an external mount antenna and connect computer devices via the router's Ethernet ports and/or via the router's Wi-Fi access. The Blacksburg Transit Authority is using this second method to provide Wi-Fi access to passengers on their buses.

The mobile broadband Internet service can be configured to provide priority for public safety applications. The service can support peak download speeds up to three megabits per second for IP voice, data, and video. Downstream speeds vary with distance from a base station antenna and the terrain, but speeds of about one megabit per second have been unofficially measured throughout much of the main Virginia Tech campus area. An external, vehicle-mounted antenna provides the best performance.

Repeater Control Radios

Radio repeaters and their antennas are generally located on the tops of buildings or on towers. The repeaters may be controlled from dispatch center console systems directly over telephone twisted-pairs (using direct current or tone control), over fiber-optic cable, or via control radios located in, or near, the dispatch center. Control radios are similar to base station radios, except they only talk to a repeater.

Geographic Information Systems

First responders frequently need detailed maps and/or floor drawings to pinpoint the location of incidents. When incident location information is entered into an advanced Computer Aided Dispatch (CAD) system, it can use information from a Geographic Information System (GIS) to display the location on a map, or floor drawing, which can be transmitted to first responders along with associated text information.

The Floyd County E911 Center has implemented CAD GIS functionality for their region, although they do not have building floor drawings available. They are currently transmitting incident GIS information to their Rescue Operation Center. They are in the testing phase of sending GIS information to first responders in the field using mobile broadband Internet service.

The Virginia Tech Information Technology organization has implemented a prototype, network-accessible, GIS database system. It could potentially evolve to a production system providing secure access to the most current Virginia Tech GIS base maps, orthographic overlays, and building floor drawings.

Conclusions

Given the radio communication issues that occurred on April 16th, radio infrastructure upgrades and enhancements should be considered. Improvements should take into consideration the infrastructure needed for backup (redundancy and diversity) and for potential scenarios involving multiple, parallel incidents.

Upgrades and/or enhancements should be considered for the following:

- Dispatch consoles, including capabilities for radio/cell phone/landline interoperability
- Diversity and redundancy for repeater control radio facilities
- Expanded multi-channel recording capabilities
- Expanded portable radio caches
- Improved radio communications signal coverage
- Portable computers with mobile broadband Internet access for first responder vehicles
- Implement access to GIS base maps, orthophotography, and floor drawings to the Virginia Tech Dispatch Center and the ability to transmit the information to first responders in the field
- Mobile command/response vehicles or units

Short Term Recommendations

- Upgrade the current VTPD dispatch consoles and assess the need for additional primary and backup consoles, including the associated radio room facilities.

Install secondary, or backup, consoles and radio facilities in an alternate location for survivability.
- Expand the Virginia Tech Dispatch Center audio recording system.
- Expand Virginia Tech Police and Rescue portable radio caches, including extra batteries and chargers.
- Install vehicle computers with mobile broadband access for Virginia Tech Police and Rescue.
- Consider adding local hospitals to dispatch console and interoperability systems.

Long Term Recommendations

- Partner with the Town of Blacksburg and other area agencies to plan cooperative improvements for public safety communications.
- Determine the need for additional radio channels and coverage.
- Integrate GIS-mapping capability into the Virginia Tech Dispatch Center's Computer Aided Dispatch system and implement methods for transmitting the information to first responder operation centers and to first responders in the field.
- Acquire fully equipped mobile command units for the Virginia Tech Police and the Virginia Tech Rescue Squad.
- Consider using cognitive radio technology when available.

Exhibit A: Cognitive Radio at Virginia Tech

The Virginia Tech Electrical and Computer Engineering Department is researching cognitive radio technology. Two projects are funded by grants from the National Institute of Justice (NIJ) and the National Science Foundation (NSF). Professor Charles Bostian serves as the faculty lead. The NIJ effort involves building a radio that can recognize and interoperate with three commonly used and mutually incompatible public safety waveform standards. The NSF effort extends the technology to investigate spectrum access and to study networks containing both legacy and cognitive radios. The two current projects should significantly contribute to commercialization, which is expected within the next five to 10 years.

A cognitive radio combines artificial intelligence with software-defined radio technology to create a portable aware of the RF environment, its own capabilities, policies defining legal operation, and its user's needs and operating privileges. The cognitive engine sets the software-defined radio's operating parameters, observes the results, and optimizes operation within the governing rules.

The Virginia Tech cognitive radio team is collaborating with Virginia Tech Police Department to understand their needs. They are currently demonstrating a prototype radio that provides a bridging function between a Virginia Tech Police Department VHF radio and an FRS (Family Radio Service) radio plus other functions.

NIJ deliverables are:

- A fully functional Public Safety Cognitive Radio using the Unified Radio Architecture radio platform, including fully tested cognitive engine software.
- A GNU (GNU is a recursive acronym that stands for "GNU's Not Unix") Radio/ Universal Software Radio Peripheral based Public Safety Cognitive Radio that supports (1) multiple Media Access Control layers (including Carrier Sense Multiple Access/Collision Avoidance) to enable the full use of the radios as a TCP/IP network interface, (2) radio-over-IP for interoperability and increased coverage, (3) support for readily reconfigurable multicast talk groups, (4) a P25-capable implementation without trunking.

See "Radios that Think and Learn," http://www.ece.vt.edu/news/ar06/andlearn.html for more information.

Exhibit B: Methods, Guidelines, and Standards

Many federal, state, professional, and other organizations provide information about methods, guidelines, and standards useful for first responder infrastructure planning.

A partial list of organizations and their Web links includes the following:

- APCO (Association of Public-Safety Officials-International, Inc.), http://www.apcointl.org/
- ARRL (Amateur Radio Relay League), http://www.arrl.org/
- CALEA (Commission on Accreditation for Law Enforcement Agencies, Inc.), http://www.calea.org/
- DCJS (Department of Criminal Justice Services), http://www.dcjs.virginia.gov/index.cfm
- DHS (Department of Homeland Security), http://www.dhs.gov/index.shtm
- DOJ (Department of Justice), http://www.usdoj.gov/
- DOJ COPS (Community Oriented Policing Services), http://www.cops.usdoj.gov/
- DOJ OJP (Office of Justice Programs), http://www.ojp.usdoj.gov/
- DOJ OJP NIJ (National Institute of Justice), http://www.ojp.usdoj.gov/nij/
- DOJ OJP NIJ CommTech (Communications Technologies), http://www.ojp.usdoj.gov/nij/topics/technology/communication/welcome.htm
- FCC (Federal Communications Commission), http://www.fcc.gov/homeland/
- FCC Public Safety and Homeland Security Bureau, http://www.fcc.gov/pshs/
- FEMA (Federal Emergency Management Agency), http://www.fema.gov/index.shtm
- FEMA NIMS (National Integration Center ((NIC)) Incident Management Systems Division), http://www.fema.gov/emergency/nims/index.shtm
- FEMA Emergency Management Institute, http://training.fema.gov/, see online courses
- IACP (International Association of Chiefs of Police), http://www.theiacp.org/
- IAFC (International Association of Fire Chiefs), http://www.iafc.org/
- ITIL (Information Technology Infrastructure Library), http://www.itil-officialsite.com/home/home.asp
- NACo (National Association of Counties), http://www.naco.org/
- NENA (National Emergency Number Association), http://www.nena.org/
- NLECTC JUSTNET (National Law Enforcement and Corrections Technology Center, Justice Technology Information Network), http://www.nlectc.org/justnet.html
- NSA (National Sheriffs' Association), http://www.sheriffs.org/home.shtml
- USFA (U.S. Fire Administration), http://www.nfaonline.dhs.gov/, see online courses
- VDEM (Virginia Department of Emergency Management), http://www.vaemergency.com/
- VITA (Interoperability in Virginia), http://www.interoperability.virginia.gov/

Exhibit C: Proposal to Test the use of Advanced Mobile Communications Applications

Purpose

The purpose of this section is to propose a pilot project to demonstrate how mobile devices can be used by executives, staff, and others to provide quick voice and text messaging communications for participating users, and how Bluetooth devices can provide access control to university facilities.

Technology Description

There are three proposed mobile device applications to be tested. The first is Push-to-Talk with presence awareness. The second is instant text messaging with presence awareness. The third is the use of Bluetooth devices for controlling access to university facilities, such as building and room entrances.

Push-to-Talk

Push-to-Talk for mobile voice communication devices provides quick communications between participating users by providing a half-duplex walkie-talkie capability. There are at least two methods for providing the functionality.

One method is a proprietary service offered by mobile wireless providers. The service provides one-to-one and one-to-many communications by allowing a user to set up predefined groups of contacts. The Push-to-Talk application provides visual presence information for each contact, which is updated automatically for events such as a user turning their phone off, or if the person is currently out of cell phone range. A feature of the service allows users to be tagged so that members can be notified when they become available. Another feature is that it uses a secure and encrypted communication channel. The Push-to-Talk over cellular technology is being standardized by the Open Mobile Alliance organization for enterprise telephony to provide always-on service across Session Initiation Protocol (SIP) based wireless platforms.

A second method for implementing Push-to-Talk functionality over wired and wireless networks utilizes Voice over Internet Protocol (VoIP) with SIP signaling. Push-to-Talk applications can be supported by new generation VoIP telephone systems.

Mobile Instant Text Messaging

A mobile instant messaging client allows users to stay connected to a group of participants through text-based communication. It allows for mobile-to-mobile and mobile-to-desktop computer communication. It supports persistent communication so users can send and receive messages anytime and anywhere they have access in near real time. It can be used when voice is not an option and when a quick text communication method is needed.

Mobile instant messaging clients also support visual presence information for each contact. This information is updated automatically and is based on a larger set of parameters than Push-to-Talk. Availability is determined from calendars and whether the contact is logged onto their computer or mobile device.

Gartner, Inc., is a leading information technology research and advisory company. In a June 2007 press release, Gartner stated that for many knowledge workers, instant messaging (IM) is as critical as having access to a telephone or to e-mail and enterprises that haven't already done so should start incorporating IM into their critical business processes immediately. Gartner predicts that by the end of 2011, IM will be the de facto tool for voice, video and text chat with 95 percent of workers in leading global organizations using it as their primary interface for real-time communications by 2013. Instant messaging is being morphed into a fully converged unified communications platform with presence at the center. Organizations need a real-time collaboration architecture that makes presence information available beyond the confines of an IM application.

Bluetooth for Access Control

Bluetooth wireless technology is designed into many cell phone, PDA (Personal Data Assistant), Pocket PC, and similar devices. It provides a standardized short-range communication method to allow devices to talk to each other wirelessly. The concept of Bluetooth Access Control is to enable personal Bluetooth devices to open door locks that have existing swipe card technology. For example, a person's mobile phone could be used as a wireless security badge to gain access to secure areas.

Bluetooth could be used in a couple of different methods for building access. Areas could be set up to only require physical possession of the device in order to gain access, or it could be set up to require a key code to also be entered on the device. Use of a key code requires both physical possession of the device and knowledge of a secret piece of information to obtain access. Since Bluetooth is a wireless technology, the receiver for a door could be physically mounted behind walls or located within buildings several feet from the actual door, which could protect the receiver from outside elements and tampering.

The application of Bluetooth access control on a university campus offers a potential for a number of innovations. It puts more emphasis on a single device that can be used for multiple purposes. Benefits are that users would only have one device to keep track of on a day-to-day basis and adding the service to such a ubiquitous device has some potential to ease future scalability. Additionally, smart cell phones have potential for future integration into other services on campus and this could be the first step to utilize the platform.

Observations

The Virginia Tech Police and several other groups on campus currently use proprietary Push-to-Talk services. However, many executives, their staff, and other groups are not making use of the technology.

Instant text messaging is not yet being utilized by the Virginia Tech Police and many other organizations on campus. It is being more heavily utilized by students. Instant text messaging is a subset of new generation unified communications solutions that are being planned by the Virginia Tech Information Technology organization.

Bluetooth access control is not currently being utilized for building access at Virginia Tech.

Conclusions

A pilot project could test the capabilities, benefits, and identify potential users for:

- Push-to-Talk voice communications (proprietary and VoIP)
- instant text messaging (cellular and IP)
- Bluetooth access control

Push-to-Talk and instant messaging technologies need to be considered for integration into the planned university VoIP telephony and unified communications solutions.

Appendix V: 911 Systems Utilization and Performance

Purpose

The purpose of this report is to examine the existing 911 systems serving the Virginia Tech campus in Blacksburg and the surrounding area, to determine how these systems performed during the tragedy of April 16th, and in the aftermath of the tragedy, with special attention to the challenges provided by cellular phones, determine what enhancements might strengthen the 911 programs in the future.

Summary

During the months of June and July 2007, team members met with the communications officers and uniformed officers of the law enforcement agencies responsible for the 911 systems serving Virginia Tech, the Town of Blacksburg, the Town of Christiansburg, and Montgomery County. These officers reported their 911 systems enabled them to respond to students, faculty, staff, and local citizens, and direct emergency service providers where they were needed on April 16th. A review of 911 call counts, both wireless and wireline, for the time period indicate increased traffic compared to a typical day. In addition, the calls to non-emergency/administrative lines were extremely heavy throughout the day. The wireless 911 calls received by the local Public Safety Answering Points (PSAPs) for emergency response by the Virginia Tech Police were transferred from the PSAPs' communications consoles to the non-emergency/administrative lines at the Virginia Tech Police Department (VTPD) dispatch center. The transfer process created a problem by reporting an emergency to a telephone line used for general information and non-emergency calls, especially in light of the volume of calls these "administrative" lines received following the tragedy on the morning of April16th.

- A programming change has already been implemented for the transfer of 911 calls from the local PSAPs to the Virginia Tech Police Department 911 line.
- Additional staffing and communications equipment in the Virginia Tech Police Department's dispatch center to handle an increased volume of calls in the event of an emergency is warranted, especially to process calls to non-emergency/administrative lines.
- The dispatch environment of the Virginia Tech Police Department should be updated to reflect changes in public safety communications technology and to include appropriate workstations.

General Description

Blacksburg Police Department

The Blacksburg emergency services communications center is the central point of contact for law enforcement officers and members of the Blacksburg community. The Police Communications Center is staffed 24 hours a day by nine full-time, professionally certified, communications officers. These officers respond to both emergency and non-emergency requests for police, fire, and first-aid assistance. Communications officers monitor [Redacted] phone lines and [Redacted] active radio frequencies.

The Blacksburg Police Department operates a Public Safety Answering Point (PSAP) and receives calls from both wireline and wireless 911 callers. [Redacted]. The telephone system is provided and maintained by Verizon.

Christiansburg Police Department

On the Christiansburg Police Department website, the Communications Division is described as "the core of the police department." In the Town of Christiansburg, this group answers all calls for the police department. These calls can be for routine service, for another division of the police, or emergency calls. While answering requests for service, both "routine" and emergency calls, communications officers are also responsible for dispatching fire and rescue units. The Christiansburg Police Department is an "assisting agency" for the Virginia Tech Police Department.

The Christiansburg Police Department operates a Public Safety Answering Point (PSAP) and receives calls from both wireline and wireless 911 callers. There are [Redacted] communications officers and one Lead Communications Officer in the Communications Division. They answer [Redacted] administrative lines, [Redacted] 911 cell lines, and [Redacted] 911 landlines. [Redacted] The telephone system is provided and maintained by Verizon.

Montgomery County Sheriff's Office Communications Division

As indicated on the county's website, every 911 and other emergency call originating from the county is handled in the Sheriff's Office Communications Division. The dispatch center is manned 24 hours a day, 365 days a year. The communications officers have many duties, and they are often carrying them out simultaneously. They are responsible for the operation of multiple radio channels through which they receive reports, requests, and dispatch mobile law enforcement and other agencies including fire and rescue units. The communication operators are responsible for maintaining the location and status of each deputy and each fire and rescue unit.

They receive all emergency 911 calls, both wireless and wireline, originating from outside town limits but within Montgomery County. The communications operation has a multi-line telephone call center to receive information, complaints, and requests for assistance. Most calls for the Sheriff's Office come through this center and are then transferred by the operators to the proper extension.

The communications officers are trained to operate several computer terminals in order to enter and retrieve information through various local, state, and national file systems, including Virginia's Department of Motor Vehicles car and driver information. These computer networks also allow them to access or report information on stolen property, wanted persons, and missing persons.

The Montgomery County Sheriff's Office operates a Public Safety Answering Point (PSAP) and receives calls from wireless callers. [Redacted] Communications Officers transfer calls to the Virginia Tech Police via a speed-dial button programmed on their consoles.

Virginia Tech Police Department

The Virginia Tech Police Department (VTPD) is a full-time, full-service, nationally accredited police department. Its jurisdiction is on the immediate campus in Blacksburg, Virginia. Through a concurrent jurisdiction agreement, Virginia Tech Police officers also have jurisdiction on all property in Montgomery County.

The Virginia Tech Police Department Communications Division currently consists of up to 10 uniformed, unarmed personnel responsible for 911 calls, rescue calls, burglar and fire alarms, as well as general information. These personnel gather information from callers and disseminate it to a responding officer. The dispatch office is staffed 24 hours a day, seven days a week to answer questions or to have an officer respond to emergency or non-emergency requests for service on the Blacksburg campus.

The Virginia Tech Police operate a Public Safety Answering Point (PSAP) for the Blacksburg campus. Police, fire, and rescue emergency calls are completed by dialing 911 from any campus phone. The non-emergency telephone number is 231-6411. Wireless 911 calls are answered by other localities depending on where the calls originate and are transferred to the VTPD. Wireless 911 calls are NOT answered directly by the Virginia Tech Police. The dispatch office is located within the Virginia Tech Police Department facility behind Lane Stadium. There is no alternate location.

When a caller dials 911 from a campus wireline telephone, the caller is connected to a dedicated, outbound trunk group (special telephone circuits) hard-wired to a dedicated, inbound trunk group that connects the call to a shared extension on two dispatch telephones. This trunking arrangement ensures call detail records are generated for all 911 calls. If the primary dispatch extension is busy, calls will forward to a group of alternate, shared extensions on the dispatch telephones. [Redacted]

Additional 911 functionality is provided for The Inn at Virginia Tech (The Inn). Once a 911 call originating from a hotel room at The Inn is answered by Virginia Tech Police Department dispatch, a visual alert is displayed on [Redacted]. The purpose of this system is to allow management at The Inn to be aware of a 911 call immediately and respond appropriately according to their procedures.

Wireless 911 Background

According to the FCC, the number of 911 calls placed via wireless phones has more than doubled since 1995. The number of calls is approximately 50 million per year, and public safety personnel estimate 30% of all the 911 calls they receive are made from wireless phones. Because wireless phones are mobile and essentially radios transmitting and receiving information via radio frequencies instead of wire, there is not a fixed location or address connected to a call originating from a wireless phone.

Wireless 911 calls are answered by the local Public Safety Answering Point (PSAP) where the cellular call is initiated. The Code of Virginia required that all localities should take the wireless 911 calls made from within their jurisdiction by July 1, 2003.

PSAPs have geographically-defined boundaries typically conforming to a city or county boundary. It is important that a wireless 911 call be routed to and answered by the appropriate PSAP. Each cellular tower array is divided into sectors, often three sectors providing 360 degree coverage. A wireless 911 call is routed to the appropriate PSAP

based on routing information, stored in special tables, for each cellular sector. The location of a caller dialing 911 from a cellular phone is associated with the tower sector receiving the call. That sector is linked with a specific, primary PSAP and a backup PSAP. According to Verizon Wireless, cellular calls are routed to the appropriate dispatch agency through a cooperative effort between the carriers and PSAPs.

Methodology

Information for this report was gathered from interviews, data collection, and a review of best practices.

Observations

Blacksburg Police Department

On the day of the tragedy, the Police Services Division in Blacksburg reported the communications officers and the 911 system itself performed well. The volume of emergency calls was greater than normal, and the volume of non-emergency/administrative calls was extremely high. On the scene, communication was "not an issue" because officers were standing "shoulder-to-shoulder." Police personnel did indicate information between officers en route to the scene could be improved. They cited interoperability issues between the Town and university radio systems creating problems resulting in limited information and potentially conflicting information while en route.

Call Counts by Line Group

Inbound Calls on April 9, 2007

911 Cell Lines	15
911 Landlines	12
Administration Lines	182
Total	209

Call Counts by Line Group

Inbound Calls on April 16, 2007

911 Cell Lines	52
911 Landlines	23
Administration Lines	790
Total	865

Christiansburg Police Department Communications Division

For the events of April 16, 2007, the Lead Communications Officer indicated it was an average day in the dispatch office. Call counts by line group were close to normal, and there was a slight increase in the number of administrative/non-emergency calls which she attributed to "concerned citizens."

Call Counts by Line Group

Inbound Calls on May 16, 2007

911 Cell Lines	5
911 Landlines	5
Administration Lines	108
Total	118

Call Counts by Line Group

Inbound Calls on April 16, 2007

911 Cell Lines	5
911 Landlines	8
Administration Lines	147
Total	160

Montgomery County Sheriff's Office Communications Division

During the events of April 16, 2007, the Communications Supervisor in the Montgomery County Sheriff's Office reported they received two phone calls from within Norris Hall via cellular phones. One phone call was lost, and the dispatcher was able to stay on the line with the other caller. As indicated above, wireless 911 calls originating from Virginia Tech and received at the Sheriff's Office dispatch center are transferred via the communications console to the non-emergency/administrative lines at the VTPD dispatch center. The calls are handled via a "warm transfer" joining the two parties together before Montgomery County releases the caller. A cellular test call placed by a Montgomery County officer and originating within the county was transferred to the Virginia Tech Police and answered on one of the non-emergency/administrative lines.

Call Counts by Line Group

Inbound Calls on April 9, 2007

911 Cell Lines	25
911 Landlines	18
Administration Lines	294
Total	337

Call Counts by Line Group

Inbound Calls on April 16, 2007

911 Cell Lines	47
911 Landlines	21
Administration Lines	432
Total	500

Virginia Tech Police Department

The lieutenant on duty the morning of April 16th was in the dispatch office the entire day, beginning at 8:00 AM and ending at midnight. Several dispatchers worked their usual shifts, but the lieutenant was on site in dispatch through the entire event and the remainder of the day. During the events of April 16th, the lieutenant reported no unusual 911 call volume, but police non-emergency/administrative lines were unusually busy with what were initially believed to be wireless 911 calls referred by the Montgomery County Sheriff's Office and Blacksburg Police Department PSAPs.

As indicated above, the VTPD Communications Division has a primary extension and [Redacted] additional, shared extensions on the dispatch telephones for 911 calls. There are additional line appearances for non-emergency/administrative calls. The 911 calls "roll over" to the non-emergency/administrative lines; that is, a call goes from a busy line to the next available line, where it is answered by the communications officers on duty. The non-emergency/administrative lines do NOT roll over to the 911 lines. On April 16th, referring to the non-emergency lines, personnel in the Communications Division report, "we couldn't answer them fast enough…" At times during the day of the tragedy, the inbound call volume was so great that outgoing calls could not be made from the dispatch office.

Adding to the difficulty of the increased call volumes was the fact the communications officers cannot use a single headset to receive both radio messages and telephone calls. In the current configuration, there are compatibility issues regarding the use of headsets for both radio and telephone communications.

VTPD personnel report that while incident-specific calls diminished after the initial hours, call volumes related to media inquires and calls from parents of students increased as the day continued. Parents with concerns were directed to a telephone number for the Dean of Students. Given the high volume of inquiries to the Office of the Dean of Students, callers who reached a busy signal or did not get an answer there, redialed the Virginia Tech Police Department.

The Virginia Tech Police reported receiving misdirected calls from the university switchboard. The Police Department believes they are often used as the information contact of "last resort"--for example, directions to Virginia Tech, inquiries about the location of buildings on campus, and questions regarding campus events are all very common requests directed to the police non-emergency line.

Call Counts by Line Group

As reported by the Communications Division, inbound calls received by the Virginia Tech Police on a "typical Monday," total approximately 452 for both the 911 lines and the non-emergency administration lines. On April 16, 2007, the Virginia Tech Police dispatch office handled a total of 2027 inbound calls.

Inbound Calls on March 26, 2007

911 Cell Lines	Does Not Apply
911 Landlines	10
Administration Lines	442

Total	452

Call Counts by Line Group

Inbound Calls on April 16, 2007

911 Cell Lines	Does Not Apply
911 Landlines	181
Administration Lines	1846
Total	2027

Conclusions

The Campus Emergency 911 program and 911 services in the surrounding area enabled students, faculty, staff, and citizens to reach first responders as designed. Initial concerns that the very high call volumes experienced in the Virginia Tech Police Department dispatch office were related to wireless 911 calls appear to be unfounded. If all the wireless 911 calls reported from the PSAPs were transferred to Virginia Tech via the non-emergency administrative lines, they would account for only a small percentage of the total call volume received that day.

In the course of discussing Campus Emergency 911 system performance, other issues related to changes in technology, best practices, and enterprise management have surfaced that are "cross cutting concerns"—that is, issues that potentially affect other communication systems.

Short Term Recommendations

- Create a backup location for the VTPD 911 dispatch center in the event the Sterrett Facilities Complex is not available or inoperable.
- Implement procedural changes with the Blacksburg Police Department, Montgomery County Sheriff's Office, and the Christiansburg Police Department to terminate transferred calls on the 911 lines instead of administrative lines.
- Determine what would be required to send overflow calls to the Blacksburg Police Department when the Virginia Tech Police 911 center is busy and implement those changes if appropriate.
- Make provisions for emergency staffing and increased phone coverage to handle increased call volumes.
- Establish ongoing collaboration/regular meetings of area public safety groups and their representatives with Communications Network Services to discuss communications needs.
- Collect data at the VTPD dispatch center regarding incoming calls to the non-emergency line to identify the root cause of any misdirected calls. Implement changes to operating practices in order to reduce the number of calls transferred to the non-emergency/administrative lines.
- Continue site visits to study and review best practices in public safety dispatch environments.

Long Term Recommendations

- Redesign the Virginia Tech Police dispatch office to include technology improvements and an appropriately designed dispatch environment and workstations.
- A solution to monitor both phone lines and radio frequencies on a single headset should be implemented.
- Implement interoperability and console-integration solutions to allow field units to communicate with each other and other law enforcement agencies.
- Reverse 911 or 911 Broadcast systems should be utilized to augment the current methods of emergency notification.

Exhibit A: References

Blacksburg Police Department Fiscal Year Report 2005-2006

Christiansburg Police Department Webpage

Commonwealth of Virginia, Wireless E-911 Services Board,
FY 2006 Draft Annual Report

Federal Communications Commission
Consumer Publications
Wireless 911 Services

The Official Montgomery County Government Website

Virginia Tech Police Annual Report of 2006

Appendix VI: Cellular Service Utilization and Performance

Purpose

The purpose of this report is to examine the existing cellular networks serving the Virginia Tech campus and surrounding area, determine how these networks performed during the tragedy of April 16th, and, in the aftermath of the tragedy, determine what enhancements might strengthen the future performance of the cellular networks on campus.

Summary

- Wireless service providers responded to the events of April 16th by adding capacity to their networks through the provision of temporary cell sites and antenna systems. They also made user equipment available to first responders, university personnel, families, and community volunteers.
- Telecommunications networks, whether they are wireless or wireline, are designed to accommodate peak busy hours, not peak usage in the event of a disaster.
- Continued study is required to recommend solutions to enhance cellular coverage on the Virginia Tech campus.

General Description

Communications Network Services (CNS) is the university auxiliary enterprise providing telephone, data, and video services to students, faculty, staff, and the entire university community. CNS is responsible for the daily operation of the university's communications systems. Telephone service at Virginia Tech is provided through a Siemens Computerized Branch Exchange serving approximately 15,000 lines across 14 nodes. Voicemail is provided via a voice messaging system. There are also over 25,000 switched Ethernet data connections and 5,000 cable television connections which, combined with the telephone connections, comprise the campus voice, data, and video network.

CNS provides cellular telephone services for faculty and staff under a statewide cellular contract. The contract includes both cellular service and equipment, and it is administered through the auxiliary. A consortium of providers led by Alltel provides the service and equipment. In Blacksburg, U.S. Cellular provides the calling plans.

CNS also operates a system supporting multiple e-mail-capable cellular phones, wireless handhelds, and device operating systems providing secure, real-time, reliable wireless information access on a variety of palmOne™ and Microsoft® Windows Mobile™ handhelds. The cellular service and equipment is supplied by several wireless providers under Cooperative Procurement agreements, and the program uses a CNS-provided enterprise server to support continuous, wireless synchronization in order to access and update e-mail, address lists, and other information from the Exchange server.

CNS does not currently provide cellular telephone service for students.

Wireless operators serving the Blacksburg area built out their networks by adding traditional macro-cellular service sites on rooftops or towers in the area to improve coverage and capacity for their customers. These systems were generally designed to provide a reliable quality of cellular coverage in cars or on street level. Their coverage objectives did not initially extend to in-building coverage. Some of the area providers routinely augment their systems for sporting events or other university activities such as commencement to accommodate the need for increased capacity.

There are no wireless carriers operating on the campus of Virginia Tech; their base station infrastructure is located off-campus.

Methodology

Information for this report was gathered through interviews, data collection, and a review of industry practices.

Observations/Findings

First responders reported there were locations in the vicinity of Norris Hall where they were not able to make and receive calls. During the incident and the hours that followed, specific campus locations identified as having poor cellular coverage also included Derring Hall, Durham Hall, Whittemore Hall, War Memorial Gymnasium, Squires Student Center, and The Inn at Virginia Tech (The Inn). Network congestion accounted for many of the incomplete call attempts individuals experienced. Wireless carrier radio frequencies, which do not penetrate all buildings on campus, accounted for the areas of no service or marginal signal strength.

AT&T

During the events of April 16th, AT&T observed a significant spike in wireless phone use in Blacksburg. According to correspondence forwarded from the AT&T Vice President and General Manager with responsibility for Virginia and West Virginia to University Relations, technicians were dispatched to the five cell sites serving Blacksburg and the surrounding area in order to add capacity to the AT&T wireless network.

Sprint Nextel

On Monday, April 16th, Sprint Nextel Public Sector Sales teams contacted the Virginia Tech Police Department, Blacksburg Police, the State Emergency Operations Center, and the Governor's Office to offer assistance. The Virginia Department of Emergency Management contacted Sprint Nextel regarding Sprint Emergency Response Team services. Sprint placed a portable cell site, known as a satellite Cell on Light Truck (COLT), on stand-by.

Sprint was also contacted by Federal agencies regarding their willingness to support the situation in Blacksburg. A Sprint Emergency Response Team prepared for deployment with the satellite COLT, a Deployment Support Vehicle, and 200 handsets. The Sprint Public Sector Senior Vice President contacted President Steger's office to offer assistance and discuss Sprint's capabilities.

On Monday, between 1:30 PM and 5:00 PM, additional capacity was added to the existing Sprint cellular towers. Seven additional radios were brought on-air at one

location and three additional radios were on the air at another location. By 2:00 PM on Monday afternoon, Virginia Tech Police advised Sprint that communications had "stabilized." However, police personnel required additional batteries and chargers. The Inn at Virginia Tech was identified as the "family center," and problems with in-building cellular coverage were identified.

Sprint notified the Montgomery County Emergency Operations Center that additional phones would be provided, and they subsequently delivered batteries and a multi-bay charger for their use. By 6:30 PM, sales teams began to identify the account numbers of first responders and arranged for Wireless Priority Access and Priority Dispatch through the Public Sector Customer Care organization in Temple, Texas.

The Sprint Public Sector Senior Vice President communicated with the United States Secret Service and FBI regarding support required for President Bush during the Convocation scheduled at Cassell Coliseum on Tuesday, April 17th. On Monday evening, Sprint Field Operations personnel were en route with equipment to install an in-building antenna system for The Inn at Virginia Tech. The satellite COLT was also en route and arrived at The Inn at approximately 11:00 PM.

By the morning of Tuesday, April 17th, a Sprint in-building antenna system was operating at The Inn, and the satellite COLT was on the air and processing calls (iDEN technology). Sprint Nextel Account Team members were in Room 1872 of the Inn at Virginia Tech with cellular phones, batteries, and chargers which were made available to families, university staff, the Red Cross, the Salvation Army, and others. Local account team members remained on site until Thursday afternoon to assist the university community.

During the event, 60 batteries, 40 power chargers, and 51 phones were utilized. Some non-Sprint accessories were also provided to Virginia State Police utilizing other wireless service providers. The satellite COLT remained in service until Thursday, April 26th. At the request of the Virginia Tech Police Chief, a Sprint in-building antenna system was installed with assistance from CNS personnel at Lane Stadium to support the law enforcement Command Post.

Verizon Wireless

On the morning of Monday, April 16th, the Verizon Business Group President of Government and Education contacted Virginia Tech's Vice President of Information Technology to offer assistance and discuss the university's communications needs in the wake of the tragedy. The Verizon Group President remained in contact with the university in the days that followed through the office of the Associate Vice President of Network Infrastructure and Services.

On the afternoon of Monday, April 16th, Verizon's Wireless Director of Network Engineering contacted Communications Network Services (CNS) about the dramatic increase in Verizon Wireless traffic on Virginia Tech's campus. Verizon Wireless offered to add capacity via a COW (Cell on Wheels) or COLT (Cell on Light Truck) to support communication efforts. Verizon also advised that the Roanoke-based account team would deploy emergency cellular phones for university use. A new Verizon Wireless cellular site, planned for the University Gateway building and already being installed,

was activated and began processing calls three weeks earlier than originally expected.

The afternoon of Monday, April 16th, Verizon's Wireless Manager of Strategic Sales in Roanoke, Virginia, contacted CNS to advise that 100 emergency cell phones had been deployed to Roanoke for Virginia Tech's use.

On the morning of April 17th, CNS personnel met with Verizon Wireless Performance engineers to discuss the placement of the COLT. The university campus map was reviewed at that time. Based on coverage needs and the location of existing Verizon Wireless sites providing coverage to the university, the area in the vicinity of Litton-Reaves parking lot was identified as the best place to deploy the COLT. Virginia Tech's Director of Transportation approved the deployment location, and a request was made to approach the campus from Route 460 to Southgate Drive to Duck Pond Drive. CNS personnel took the Verizon Wireless engineers to view the proposed site while the COLT was en route to Blacksburg.

The Roanoke-based account team provided 50 wireless phones available for loan to CNS, with an additional 50 in reserve in Roanoke. Six Treo Smartphones and spare battery modules were made available to CNS, and on-site support was provided to facilitate executive-level requests for assistance.

U.S. Cellular

On Monday, April 16th, the U.S. Cellular Mid-Atlantic Direct Sales Manager telephoned Communications Network Services (CNS) to advise that CNS would be contacted by the U.S. Cellular Operations Manager in Roanoke regarding the placement of a COLT (Cell on Light Truck) on campus to add capacity. U.S. Cellular sites are alarmed and monitored 24 hours a day, seven days a week, and local technicians were paged once the switches began operating over a certain threshold due to the events on campus. Technicians were dispatched to add additional capacity to existing cell sites, and the COLT was deployed from Morgantown, West Virginia. By Tuesday morning, the U.S. Cellular COLT was in place and operating in Parking Lot B.

CNS worked with U.S.Cellular Public and Media Relations in Portsmouth, New Hampshire, to gather data and with the Operations Manager in Roanoke, Virginia, regarding the COLT deployment. CNS was subsequently contacted by the U.S. Cellular Senior Director, East Operations, regarding coverage and capacity issues on campus. Decisions were made locally to support Virginia Tech by self-directed work teams responding to the needs of the situation.

Conclusions

Wireless service providers quickly responded to the events of April 16th by bringing strategic resources to the aid of the Virginia Tech community. An effective combination of equipment, personnel and portable cell sites relieved network congestion and improved cellular coverage in the hours and days that followed the tragedy on campus.

Telecommunications networks, whether they are wireless or wireline, are designed to accommodate peak busy hours, not peak usage in the event of a disaster.

Due to materials used in building construction and radio frequency penetration issues, cellular phone reception was limited inside buildings. Similar problems were reported in

connection with conventional radio (two-way radio) transmissions in addition to cellular radio (cellular phone calls).

Short Term Recommendations

- With the cellular carriers, discuss any planned coverage improvements to their existing macro-cell networks serving the Blacksburg area.
- With cooperation from cellular providers, have phones on hand and wireless data cards on site ready to activate and deploy in an emergency.
- Establish a procedure to ensure cellular carrier emergency response groups notify and coordinate with appropriate university personnel regarding their presence on-campus in an emergency.
- Pursue qualification in the Federal Wireless Priority Service (WPS) program to receive calling queue priority with cellular service providers.

Long Term Recommendations

- Develop solutions to enhance cellular coverage on the Virginia Tech campus.
- Consider engaging the Mobile and Portable Radio Research Group (MPRG) and Wireless @ Virginia Tech in an effort to assess and enhance wireless mobility on campus through research of leading-edge technology and infrastructure such as cognitive radio (see Radio Communications Systems Utilization and Performance Report, Appendix IV, Exhibit A).

Appendix VII: Traditional Telephone Utilization and Performance

Purpose

The purpose of this report is to examine the traditional telephone system serving the Virginia Tech campus; determine how the system performed during the tragedy of April 16th; and in the aftermath of the tragedy, determine what enhancements might strengthen on-campus telephone service in the future.

General Description

Campus Telephone System

Traditional telephone networks are divided into two resource categories: (1) switching resources and (2) transmission resources. Switching resources are telephone systems (also known as telephone switches), switches, exchanges, or private branch exchanges (PBX.) A telephone system is primarily tasked with establishing and managing connections between two or more ports connected to the system. Ports are generally connected to the system via transmission resources. The two most common types of ports on a telephone system are line ports, which connect phones, fax machines, modems, and other communication devices to the system; and trunk ports, which provide a means for interconnecting two telephone systems.

Telephone service on the main campus is provided by a group of 14 ROLM PBXs originally installed in 1987. The individual PBXs, or nodes, are interconnected via redundant, fully meshed networks to form a single logical PBX. The ROLM PBX provides service to 14,000 line ports and 1,100 trunk ports. The PBX nodes are distributed across six switch centers which serve subscribers in approximately 175 buildings on the university's 2600-acre campus.

Public Switched Telephone Network Connectivity

Connectivity from the Virginia Tech telephone system to the public switched telephone network (PSTN) is provided by a collection of inbound and outbound trunks supplied by several telephone service providers.

Inbound trunk service is provided by a single service provider through a central office located in downtown Blacksburg. The inventory of inbound trunks is reviewed twice annually and adjusted based on utilization statistics provided by the service provider. The number of trunks in the group is engineered, based on historical utilization, so not more than one in every 1000 inbound calls is blocked—that is, the caller receives a busy signal because all the trunks are in use.

Outbound trunk service is provided by five different service providers and can be classified into the following categories:

Local

Local trunking is provided by two service providers using the Blacksburg central office and a Roanoke central office.

The trunks in the primary group are provided by a competitive local exchange carrier (CLEC) through a connection to a Roanoke central office. Calls using the primary group are switched in the CLEC's Roanoke central office to a special kind of facility that connects trunks in the same network or between networks. This facility is called a "tandem office." It is located in Roanoke and the local outbound trunks serving Virginia Tech are switched back to the Blacksburg central office from the Roanoke location.

Trunks in the secondary group are provided by the incumbent local exchange carrier (ILEC) and are directly connected to ILEC's central office in Blacksburg. The telephone system is configured to use an optimization feature that chooses the primary group if there are available trunks and utilizes trunks in the secondary group when all trunks in the primary group are busy.

The number of local trunks in the primary group is engineered, based on historical utilization, so that not more than one in every 100 calls will overflow to the secondary group. The number of local trunks in the secondary group is engineered, based on historical utilization, so not more than one in every 100 calls is unable to be completed because all the trunks are in use. Utilizing the route optimization feature to leverage trunk resources in multiple groups reduces the probability of blocking for local calls to not more than one in every 1000 calls.

Dedicated Long Distance

Two service providers provide dedicated long distance trunking through special facilities providing direct connections between the campus telephone system and the service provider networks. The numbers of trunks in these groups are engineered, based on historical utilization, so not more than one in every 100 calls overflows to regular, switched long distance lines.

Switched Long Distance

Switched long distance trunks are provided by using local trunk resources from a single service provider connected through the Blacksburg central office. These trunks act as overflow resources for the dedicated long distance trunks. Any calls using switched long distance lines are included in the local trunk resource engineering process.

Dedicated Toll-Free

A single service provider provides dedicated, toll-free trunks through facilities using direct connections between the campus telephone system and the service provider's network. The number of trunks in the group is engineered, based on historical utilization, so not more than one in every 100 calls overflows to a backup, switched, toll-free trunk group.

Switched Toll-Free

Switched toll-free trunks are provided using local trunk resources from a single service provider through the Blacksburg central office. These trunks act as overflow resources if all the dedicated toll-free trunks are in use. Any calls overflowing to the switched toll-free lines are included in the local trunk resource engineering process.

University Operators

The university operators are primarily tasked with providing directory assistance for callers from within and from outside of the university. The switchboard is staffed 24 hours a day, seven days a week, with as many as six operators. The operators assist individuals who contact the university's main telephone number by providing telephone listings for on-campus students, faculty, staff, and departments at Virginia Tech. The operators also assist callers by explaining proper dialing procedures for on-campus, local, long distance, and international calls.

Emergency Call Traces

Emergency call traces are performed at the request of law enforcement in response to threatening or harassing telephone calls to Virginia Tech telephone numbers. The procedure for tracing emergency or malicious telephone calls typically involves interaction between several entities:

- Targeted individual (the person who received the phone calls)
- Virginia Tech Police Department
- Communications Network Services (CNS)
- Telephone service provider (for example, Verizon or AT&T)

The targeted individual typically reports the incident directly to the Virginia Tech Police Department providing the called telephone number and the date/time of the incident as source information. The Virginia Tech Police Department, in turn, engages CNS with the source information for a preliminary assessment.

CNS engineers have real-time access to completed call information via an internally developed Emergency Call Trace application and Adtran Atlas (not to be confused with the ATLAS information system) devices.

Adtran Atlas devices are used as intermediary, integrated services digital network (ISDN) switches with connectivity to the public switched telephone network (PSTN) and the Virginia Tech telephone system. These devices are utilized primarily for their ability to convert ISDN signaling from the PSTN to channel associated signaling (CAS) from the Virginia Tech telephone system. Utilizing the Atlas devices enables the university to use ISDN circuits for all incoming connectivity from the PSTN. ISDN circuits provide the capability for caller ID information to be delivered for incoming calls to university telephone numbers. The Atlas devices log all inbound and outbound calls providing an audit trail for malicious or suspicious calls.

If the originating caller's telephone number is available via the Emergency Call Trace application or Adtran Atlas transaction logs, CNS provides that information to the Virginia Tech Police Department for further investigation. If the caller ID has been blocked or spoofed, CNS and/or the Virginia Tech Police Department engage the external telephone service provider.

Caller ID spoofing is the practice of causing the telephone system to display a number on the recipient's caller ID display and the telephone system's transaction logs that is not the actual number of the originating caller. Caller ID spoofing can be facilitated by web-based telephone service providers who initiate calls on behalf of their subscribers allowing the subscriber to specify the originating telephone number, the destination telephone number, and the caller ID.

On June 27, 2007, the United States Senate Committee on Commerce, Science, and Transportation passed S.704, a bill that would make it a crime to spoof caller ID. Dubbed the "Truth in Caller ID Act of 2007," the bill would outlaw causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement is exempted from the proposed rule.

Observations

Campus Telephone System

There were no service-impacting failures in the campus telephone system on April 16th. There was no indication of internal calls not being completed because all the system's core switching resources were in use on April 16th. External call blocking is discussed later in this section of the report.

The call center group providing information for family members of the victims reported several occurrences of "hang-up calls" during the late evening of April 16th and early morning of April 17th. The problem was intermittent and could not be isolated to any single phone or trunk resource. Network Infrastructure and Services switch engineers replaced several trunk resource modules on April 17th. The frequency of the hang-up calls decreased after replacing the modules.

Public Switched Telephone Network Connectivity

On April 16, 2007, there were [Redacted] analog, direct-inward-dial (DID) trunks and [Redacted] integrated services digital network (ISDN) trunks available for calls coming into the university's phone system. According to statistics provided by the local telephone service provider, the average number of inbound calls to campus from the public switched telephone network (PSTN) between April 1st and April 15th was less than 25,000 calls per day. On April 16th, there were more than 75,000 inbound calls to campus from the PSTN. Approximately 5% of the inbound calls to campus from the PSTN were blocked between 10 am and 1 pm on April 16th because all Virginia Tech inbound trunk resources were in use and no more inbound calls could be connected to campus telephone numbers.

In response to the very heavy call volume, switch engineers arranged for a group of existing trunks to be set aside for use by priority personnel for inbound and outbound calling. Dedicating trunk resources for priority personnel required changing the resources on the campus telephone system for prioritized outbound calling and coordinating with the local service provider for prioritized inbound calling.

During the event, there were [Redacted] trunks available for outbound, local calls. The [Redacted] trunks in the primary group experienced busy conditions between 9:00 AM and 1:00 PM, which caused 2075 calls to overflow to the secondary group. All trunks in the secondary group were busy for two seconds between 11:00 AM and 12:00 PM. Switch engineers experienced intermittent busy conditions while making test calls to the PSTN on April 16th. The busy test call attempts were experienced during a time when there were trunks available in Virginia Tech's primary and secondary local trunk groups

indicating congestion, not unexpected given the tremendous increase in traffic that day, in the PSTN.

During the event, there were [Redacted] trunks available in the dedicated long distance groups. There is no indication of outbound long distance calls being blocked on April 16th because there were no available resources in the dedicated long distance trunk groups.

During the event, there were [Redacted] trunks available in the dedicated toll-free group. There is no indication of outbound toll-free calls being blocked on April 16th because there were no resources available in the dedicated toll-free group.

Switched long distance trunks serve as overflow resources for the dedicated long distance groups. Switched long distance trunks were not used for long distance traffic on April 16th.

Switched long distance trunks serve as overflow resources for the dedicated toll-free groups. Switched long distance trunks were not used for toll-free traffic on April 16th.

University Operators

The average daily call volume for the university operators is less than 1000 calls. On April 16th, there were more than 3,900 calls to the university operators with approximately 8% of callers hanging up before reaching an operator. There were four operators on staff on April 16th. Campus security restrictions prevented the group's manager from calling in additional operators to assist with the high volume of calls.

Emergency Call Traces

Over a period of several weeks following April 16th, threatening calls were reported to the Virginia Tech Police, who, in turn, engaged CNS engineers to perform emergency call traces. In response to these requests, CNS provided copies of call detail records and copies of available, related voicemail to law enforcement. Caller ID information for all the threatening calls was either spoofed or blocked. Therefore, law enforcement forwarded the information provided by CNS to the telephone service provider to get the actual calling number.

Conclusions

The campus telephone system is currently configured at approximately 50% of its maximum capacity. The system proved to be adequate in providing basic telephone service during a brief period of extraordinarily high utilization.

Telephone service requests on April 16th can be divided into the following categories:

- Priority trunking
- Malicious call trace
- Call center groups
- Telephone relocations

The campus telephone system is twenty years old and has limited support for prioritizing trunk resources or tracing malicious calls. The system does not support virtual call centers or easy moves of telephone extensions.

The functionality of the PBX ad hoc priority trunking feature was limited due to the technical limitations of the analog trunks. The solution, as implemented, did not provide direct-inward-dialing (DID) for users designated as priority personnel.

[Redacted]

The university operators served as a source of information during this event. The group worked closely with personnel from University Relations and the Virginia Tech Police Department to ensure accurate and up-to-date information was relayed to callers. The group manager quickly recognized the need to increase staffing during the event but was unable to get personnel on site due to campus access restrictions.

The current process for providing the Virginia Tech Police Department with identification information of the calling party for emergency phone calls is occasionally slow and cumbersome. The migration from analog to ISDN trunking will have a positive impact in investigations of malicious calls where the calling number identification was not blocked or spoofed. However, the originating number is often blocked by the malicious caller. This situation requires interaction with the local service provider to provide the necessary information. The local service provider should be engaged to explore opportunities to improve the process.

Short Term Recommendations

- Continue to optimize the capacity-planning and resource-engineering practices of the campus telephone systems for improved performance in crisis situations.
- Convert analog direct-inward-dial (DID) trunks to integrated services digital network (ISDN) trunks to provide access to calling number information on all inbound trunk resources and to improve audio quality for inbound calls to campus. This long-term project had been underway for some time and was completed on April 20th, 2007.
- Leverage existing, remote access trunks as overflow resources for the primary, inbound trunk group. This long-planned project was completed on August 7th, 2007.
- Install a dedicated ISDN circuit for priority personnel to ensure they have access to the PSTN during crisis situations.
- Engage the local service provider to discuss their capacity-planning and resource-engineering strategies relative to crisis situations.
- Investigate the ability to provide an informational announcement to callers before connecting them to an operator to reduce repetitious information exchanges during crisis situations.
- Review Communications Network Services' (CNS) departmental emergency plan to ensure the department is positioned to utilize other departmental personnel resources as operators during crisis situations.
- Work with the Virginia Tech Police Department and the local service provider to ensure emergency trace requests are processed expeditiously.

Long Term Recommendations

- Replace the current telephone system with components designed to integrate telephony applications into an Internet Protocol-based architecture.

- Engage peer institutions to discuss policies and procedures relative to providing traditional telephone service in a university environment. Focus discussions on the technology, processes, policies, and strategies currently utilized to ensure effective landline communications during periods of extraordinarily high call volume. Develop an understanding of common issues and concerns by comparing continuity of operations, emergency preparedness, and disaster recovery initiatives. Facilitate ongoing information-sharing sessions with those institutions where future interactions would be mutually beneficial.
- Install the core network infrastructure required to support IP telephony. Develop an implementation strategy for the following telephony features:
  - Malicious call trace
  - Multi-level preemption with precedence
  - Virtual call centers
  - Extension mobility
- Develop a strategy for creating additional diversity with regard to the connectivity between the campus telephone system and the public switched telephone network (PSTN). Engage local telephone service providers to develop a more detailed understanding of capacity-planning and service-availability issues relative to connecting the Virginia Tech telephone system to the PSTN.

Appendix VIII: Video, Campus Cable Television, and Related Broadcast Systems Utilization and Performance

Purpose

The purpose of this report is to examine the existing video, campus cable television, and related systems serving the Virginia Tech campus and the surrounding area, to determine how these systems were utilized during the tragedy of April 16, and in the aftermath of the tragedy, and to determine what enhancements would strengthen Virginia Tech's emergency notifications capabilities in the future.

Summary

In the days following the April 16th incident, Video/Broadcast Services (VBS) and Communications Network Services (CNS) provided video support to the Virginia Tech community. A summary of services provided includes:

- Coordination and operational support for rescheduling canceled interactive videoconference classes and events
- Interactive videoconferencing support for a multi-site College of Engineering informational session
- TV studio production for satellite uplinks to live news shows
- Fiber-optic feeds and satellite uplinks of special events and commencement ceremonies
- Video support and recording of memorial services
- Video support and recording of selected commencement ceremonies

Neither the Campus Cable TV System nor the Interactive Videoconference System was employed as part of the campus alert issued on the morning of April 16th.

The Video Work Group reviewed six areas.

- Cable television as a means to disseminate alerts and emergency information
- The feasibility of using currently installed Crestron Control Systems to send alerts to appropriately equipped classrooms
- Using WUVT for emergency alerts and broadcasts
- Using Blackboard and Sakai/Scholar to push alerts
- Virginia Tech use of VDOT's 511 Virginia system to disseminate emergency information
- Use of low-power AM and/or FM transmitters in order to disseminate emergency information

Campus Cable Television as a means to disseminate alerts and emergency information

Cable television on campus is provided and managed by Communications Network Services. CATV/SMATV service is provided to all on-campus residence hall rooms (approximately 4,752 rooms); approximately 590 classrooms, offices and other miscellaneous locations; and 153 rooms at the Inn at Virginia Tech.

Cable TV programming is provided through a coaxial cable plant with a forward channel-carrying capacity of 450MHz. Six channels of this system (channels 2-6 and 35) are reserved for official use to support academic and informational applications. Channel 33 is reserved for full-time use of VTTV, the student-run television station, operating from studios located in Squires Student Center. Channel 35 is reserved for an informational scroll. WTOB, the Town of Blacksburg Access Channel, is also carried on the Campus Cable TV System. The remaining channels are primarily used to provide entertainment programming for student residents.

The entertainment programming is received and processed onto the cable plant from a central location (Head-End) at the CNS Teleport Facility. Local affiliate network channels are also received and processed in the same manner. A backup antenna system is available for emergency use to allow continued viewing of the Roanoke-based television stations in case of satellite reception problems or failure. We provide a public service and instructional channel to Comcast/Blacksburg Cable.

Routing and control functions for the five academic-use channels (Channels 2-6) and the informational scroll (Channel 35) are located in the CNS Video Network Operation Center (VNOC) in RB-14. Operations personnel have the ability to route video and audio programming to any or all of these channels simultaneously. The Channel 35 scroll is produced by computer and can be configured to deliver any text-based message on a continual basis. Audio from an FM receiver is normally configured to accompany this scroll. Other audio sources can be routed and included as desired. Channel 33 VTTV programming is controlled from this point to both the campus CATV/SMATV system and the public access interface maintained with Comcast/Blacksburg cable.

Channel 16 WTOB (Blacksburg Access Channel) is inserted in the Head-End and is received via a forward/reverse coaxial link with the Comcast hub site located in Salem, Virginia. We provide programming to Comcast through this link. Content of this service is controlled from the VNOC in RB-14. CNS works in conjunction with Comcast/Blacksburg Cable and the Town of Blacksburg to maintain a coaxial tie between the CATV system in town and the CATV/SMATV system on campus. This interface allows programming provided by Virginia Tech to be made available to Comcast cable subscribers residing in town as well as permitting CNS to provide the WTOB public access channel to campus residents, faculty, and staff. This interface tends to be a low priority for the town franchise holder.

Eighty percent (80%) of CATV equipment on campus is aged. The Head-End facility is not connected to an uninterrupted power source (UPS) or backup power generator system. If main power is lost, all CATV/SMATV functions are offline for the duration of the power outage. Operational AC and DC power for the CATV system is inserted at the Cassell Coliseum location.

Additional downstream power supplies are located in other CNS main campus switchrooms. The main trunk cabling infrastructure is not a ringed topology, and the CATV system could be disabled by a cable cut in a critical location.

All the 181 centrally scheduled classrooms have CATV drops. All the 181 centrally scheduled classrooms have either TV sets or data projectors capable of displaying the Campus Cable TV programming. Approximately 110 (60%) of those classrooms are currently connected to a CATV service port and are capable of viewing the cable TV

programming. The remaining centrally scheduled classrooms require additional in-room cabling and/or equipment to permit connection to the CATV system.

Observations

- The Campus Cable TV System was not employed as part of the campus alert issued on the morning of April 16th.

Conclusions

- The Campus Cable TV System has potential to serve as one mechanism to disseminate alerts and information to the campus community during an emergency.

Short Term Recommendations

- Add a CATV Emergency Alert System (EAS) for use on campus
- Add FM receivers to allow the insertion of both WVTF and WUVT onto the Campus CATV information and instructional channels

Long Term Recommendations

- Integrate a CATV EAS with other campus alert mechanisms
- Deploy in-room cabling and equipment required to connect the 71 centrally scheduled classrooms not currently connected to the CATV system or capable of viewing cable TV programming
- Work with the colleges to deploy similar systems in all classrooms not centrally scheduled
- Deploy cable drops and televisions in other key locations
- Replace the current coaxial-based cable system with a digital IP-based CATV system provisioned over the university's highly reliable and diverse data network

Using currently installed Classroom Crestron Control Systems to send alerts to appropriately equipped classrooms.

Each of the Crestron Control Systems consists of a touchscreen that connects to the multimedia devices and controls audio, video, and computer displays in the classroom.

Currently there are 181 classrooms on campus managed by the University Registrar. Fifty-six of these classrooms are equipped with Crestron systems. In addition, four videoconference classrooms are equipped with Crestron systems. Ultimately, the goal is to have every centrally managed campus classroom Crestron-equipped.

Current Crestron units can create audio tones but do not have full audio capability. The Crestron touchscreen panels can display a flashing icon and/or text message but could not handle live audio and video. The Crestron Control Systems operate on building electrical power.

Crestron's RoomView software can control and monitor all Crestron-equipped rooms. Crestron's RoomView software runs on a non-redundant central server. Crestron's RoomView software requires campus data network connectivity to control and monitor each Crestron-equipped classroom.

Observations

- The classroom Crestron Control Systems were not employed as part of the campus alert issued on the morning of April 16th.

Conclusions

- The Crestron Control systems have potential to serve as one mechanism to disseminate alerts and information to the campus community during an emergency.

Short Term Recommendations

- Enhance the current system to enable sending an audible alarm, flashing icon, and/or a text message to classroom Crestron Control systems
- implement server redundancy for the Crestron Control software

Long Term Recommendations

- Equip every classroom with a Crestron Control system
- Provide conditioned power for all Crestron Systems
- Investigate the feasibility of deploying enhanced Crestron systems capable of supporting two-way audio/video

Using WUVT Radio for emergency alerts and broadcasts

WUVT is an FCC-licensed noncommercial radio station broadcasting at 3.5 kilowatts to Blacksburg, the Virginia Tech campus, and the surrounding areas, including Montgomery County, Christiansburg, Radford, Floyd, Giles County, Salem, Pulaski, and Wytheville. WUVT's mission is to promote education, understanding, and diversity of music while serving the community as an independent, not-for-profit, student-run radio station. WUVT's goal is to provide diverse, eclectic, and educational programming. While the station staff consists mostly of student members and unpaid volunteers, community involvement is strongly encouraged.

WUVT is available as a public service to the community and airs public service announcements twice an hour, every hour, for university and not-for-profit community organizations. The typical WUVT audience is a small portion of the overall campus community.

In September 2005, WUVT submitted a proposal to replace their aging and increasingly unreliable transmitter with one that is HD Radio-capable. The proposal included an analysis and justification of several potential sites to which the new transmitter could be relocated. Based on their site analysis and budget projections, WUVT recommended a [Redacted] site as the best option.

The 22-year-old Broadcast Electronics transmitter was repaired and the station returned to full power on April 28, 2007.

Observations

- WUVT was not utilized as part of the campus alert issued on the morning of April 16th.

Conclusions

- WUVT has potential to be used as one mechanism to disseminate alerts and information to the campus community during an emergency.

Short Term Recommendations

- The university should negotiate policies and procedures for the emergency use of WUVT to issue campus alerts and emergency information to the campus community
- Carry WUVT's audio signal on one or more of the Campus Cable TV instructional channels

Long Term Recommendations

- Expand WUVT's coverage area by relocating the transmitter to [Redacted]
- Integrate the WUVT Emergency Alert System (EAS) with other campus alert mechanisms

Using Blackboard and Sakai/Scholar to push emergency alerts to faculty and students

Blackboard
The Blackboard learning system is a mission-critical, enterprise-level application for instructors, researchers, and students. Today, over 75% of the university's undergraduate courses use the Blackboard learning management system. The majority of Blackboard use supports on-campus courses. Blackboard is also used to support programs not necessarily tied to the standard Virginia Tech academic calendar or located on the Virginia Tech campus in Blacksburg.

Scholar
In 2004, Virginia Tech joined a consortium of universities from around the world to provide design, development, quality assurance, training, and leadership for an integrated, easy-to-use, robust content management system known as Sakai. Scholar is Virginia Tech's branding of Sakai and can be used for course websites, research collaboration, committee work, and managing electronic portfolios. Scholar's dominant uses are research and committee work both internal and external to the university.

Based on current use statistics, there are 1500-3000 users per hour between 8AM and 1AM. Blackboard and Scholar are also used by continuing education as well as domestic and international distance students who would not necessarily be affected by a Blacksburg-specific event.

Observations

- Neither Blackboard nor Scholar was utilized as part of the campus alert issued on the morning of April 16th.

Conclusions

- Blackboard and Scholar have potential to serve as mechanisms to disseminate alerts and information to the campus community during an emergency.

Long Term Recommendation

- Intergrate Blackboard and Scholar with other campus alert mechanisms

Use of VDOT's 511 Virginia system to disseminate emergency information

511 Virginia is a statewide web, phone, and message board service that disseminates traffic, weather, and travel information throughout the Commonwealth of Virginia. The service is sponsored and managed by the Virginia Department of Transportation (VDOT). The 511 Virginia service is available 24 hours a day and currently offers information for 98 roads in Virginia, including every mile of Virginia's interstates.

To access travel-related information, travelers dial 511 from any landline or mobile telephone. The telephone system is voice-activated and easy to use. Callers simply speak the menu items of interest to them to receive information. In addition, travelers can visit the 511 Virginia website. The website contains even more information than the telephone system, giving users access to 400 webcams, information about points of interest, driving directions, and interactive maps that display possible travel delays.

VDOT personnel offered the use of the low-power AM radio transmitters for Virginia Tech emergency notification with the condition of agency approval. They also offered the use of the 511 Virginia-system electronic, emergency notification signage as a method to direct travelers to tune to the AM radio transmitters. VDOT officials are available to meet with Virginia Tech to establish the procedure allowing Virginia Tech access to these services.

Observations

- The VDOT 511 Virginia system was not utilized as part of the campus alert issued on the morning of April 16th.

Conclusions

- Use of the VDOT 511 Virginia system would be more effective in notifying the general public than the Virginia Tech community. As such, it may be a useful means of communication for certain types of emergencies.

Short Term Recommendation

- Begin discussions with VDOT to determine the feasibility of using the 511 Virginia system to alert travelers to a Virginia Tech emergency

Long Term Recommendations

- Investigate using the 511 Virginia system to direct travelers to tune to WUVT for additional information
- Investigate the placement of additional message boards in the Blacksburg/New River Valley region

Use of low-power AM and/or FM transmitters to disseminate emergency information

Unlicensed operation on the AM and FM radio broadcast bands is permitted for some extremely low-powered devices covered under Part 15 of the FCC's rules. These

devices are limited to an effective service range of approximately 200 feet (61 meters). These devices must accept interference caused by any other operation which may further limit the effective service range.

Observations

- Low-power AM/FM radio broadcast service was not utilized as part of the campus alert issued on the morning of April 16th.

Conclusions

- Low-power AM/FM radio broadcast service is not utilized in the Blacksburg area.

Short Term Recommendation

- Work with local agencies to determine the feasibility of using low-power AM/FM transmitters

Appendix IX: Information Technology Support Services

Purpose

The purpose of this report is to examine the existing Information Technology (IT) Support Services systems serving the Virginia Tech campus, surrounding area, and extended community, to determine how these systems performed during the tragedy of April 16, and in the aftermath of the tragedy, with special attention to the performance of the operations, call center, and help desk functions and determine what enhancements might strengthen the services provided in the future.

Summary

- Reported user problems were within the bounds of normal operations.

General Description

IT Support Services is comprised of two groups--the Virginia Tech Operations Center (VTOC) and University Computing Support (UCS). These groups work in tandem to provide support for the university's centrally-administered Information Technology services.

Virginia Tech Operations Center (VTOC)

The VTOC provides a single point of contact for support of the university's central IT services. The Operations Center, located in the Corporate Research Center, serves the campus as well as other Virginia Tech locations around the commonwealth. The VTOC merges traditional call center and computing help desk functions with network operations, video operations, and systems support in an integrated operations center. The VTOC provides support twenty-four hours a day, seven days a week to meet the needs of the university computing and network environment by responding to trouble calls or web-submitted inquiries from faculty, staff, alumni, retirees, parents, and students.

University Computing Support (UCS)

UCS provides end user technical support for many of the information technology services offered to students, faculty, staff, and other Virginia Tech affiliates. UCS operates a traditional IT help desk, responding to trouble reports escalated by the VTOC including those requiring a higher level of support or interaction with the end user for resolution. UCS also provides walk-in service and on-site executive support services.

Observations

Immediately following the events of April 16th, the VTOC functioned normally with call volume at or below average levels. The volume of trouble tickets processed by the VTOC for the week of April 16th fell by approximately 20% compared to the prior week. The decreased ticket volume can be attributed to the fact that many students, faculty, and staff members were not on campus during most of the week.

Despite the lower ticket volume at the VTOC, several units with which the VTOC regularly interacts were overloaded with calls. The VTOC was asked not to transfer calls for Alumni Relations, the Graduate School, the University Registrar, Undergraduate Admissions, and the Bursar. These calls are normally transferred when callers request assistance with items the VTOC cannot resolve including account problems, incorrect personal data, or student life issues.

Trouble tickets escalated from the VTOC form the primary input for work activities in UCS. As a result of the decrease in VTOC ticket volume, UCS also experienced a proportional decrease in help desk activities.

UCS staff assigned to on-site executive support tasks provided assistance with mobile devices for two university officials throughout the week of April 16th. Student staff normally situated at Torgersen Hall expressed a desire to continue working and were relocated to the VTOC for the week.

Conclusions

The performance of the operations, call center, and help desk functions was within the bounds of normal operations.

Calls to the IT Support Services areas declined.

Normal operating functions were replaced by support needs of other groups from within and from outside Information Technology. This work included the coordination of CNS group efforts in the field, emergency installation of telephone and data services, and a general point of contact for the dissemination of information.

Short Term Recommendations

- The university should regularly review and, as needed, update the process for distributing emergency response information to initial points of contact such as the university switchboard, call centers, and help desks.
- The university should assess the need to provide security to extended areas of campus–including university offices located in the Corporate Research Center--in an emergency situation.
- The university should provide training and detailed information on the campus building layout as it relates to structures north/south/east/west of the drill field. This information is needed when the university enacts the evacuation process.

Long Term Recommendations

- Evaluate leveraging the VTOC and UCS staff expertise in call center operations to help answer calls normally delivered to other call centers during times of emergency.

Appendix X: Data Preservation

[Redacted]

Short Term Recommendations

- Formulate and present a long-term data preservation methodology to university management
- Continue to move toward disk-to-disk backup. This migration was planned and implementation was in initial phases when the event occurred.
- Continue to encourage movement of users to centrally managed e-mail, storage, and backup facilities
- Establish a task force to study the issue of university-owned and/or controlled data repositories as they relate to ownership of information. Define what is private and personal information versus what is university or public information as required by policy, state, or federal laws

Long Term Recommendations

- Establish institution-wide policies and procedures related to data preservation.

[Redacted]

Appendix XI: Data Retrieval

Purpose

The purpose of this report is to discuss Information Technology's actions to gather, analyze, report, and provide data to university management and to law enforcement in response to the events of April16, 2007. Data retrieval actions covered in this report were performed by various organizations within Information Technology including Network Infrastructure and Services, Enterprise Systems, and the Office of the Vice President for Information Technology.

Summary

- Information retrieval work supported emergency response efforts, law enforcement investigations, and victim assistance efforts.
- Information was provided to support emergency response efforts in the following areas:
  - person location information
  - counseling
  - donation management
  - communications with the university community
  - continuation of university operations
- Employee and student location information for individuals who may have been in Norris Hall was provided to law enforcement from various sources.
- Information was provided to support law enforcement investigations relative to the events of April 16th. Information included telephone call detail record information, copies of voicemail, e-mail records and analysis of e-mail logs, network traffic information, and USPS mail.
- The events of April 16th triggered multiple threats to the university occurring over the weeks following the event. Information was provided to support law enforcement investigations relative to those threats. Information included telephone call detail record information and copies of voicemail.
- In many cases, families of the deceased victims requested any digital information (digital files) created by the victims and held on university systems. The three primary sources of digital files were the e-mail system, the Filebox service, and the ePortfolio program. Any digital information available from the three sources was provided to the Dean of Students' office or to the university representative supporting the victim's family.

General Description

Numerous Information Technology groups leveraged a wide range of data sources to provide data and analysis for the purposes of emergency response, law enforcement investigation, and victim assistance. Information was provided to families of the victims (via the Dean of Students office or university family representative), various law enforcement agencies, data stewards, and university management. The primary sources of information included Banner administrative systems, telecommunications systems, e-mail, Filebox, and ePortfolio (VTeP).

Enterprise Information Systems

University student and employee information is collected and managed using the Sungard Higher Education Banner system in conjunction with enhancements and system additions developed by Virginia Tech. For students, the system includes personal identification information, housing assignments for students living in residence halls, academic history, class schedules, and financial records. For employees, the system contains personal identification information, current employment records, and employment history. The database includes information for current faculty, staff, and students as well as historical records. In addition, the internally developed Enterprise Directory, which is primarily based upon information derived from the Banner system, is used to manage authentication and authorization to university systems.

The capture, maintenance, and dissemination of university enterprise data using the Banner system is managed by appropriate administrative and academic departments under the oversight of data stewards, including the University Registrar for student data and Human Resources for employee data. The data stewards address data integrity, appropriate data access and usage, and regulatory compliance for information processes. Personal information for students and employees is primarily provided and maintained by the individual student or employee through the use of web interface tools. In some cases, information from paper files was used on April 16th to supplement data available in Banner.

Telecommunications Information

Management Information Systems

Telecommunications service information is managed in ATLAS, an internally developed Oracle-based information system. Building and room location is available for all telephone and Ethernet service. Primary user (employee name) information is stored for all departmental telephone services and some departmental Ethernet services.

Telephone call detail record information is also stored in ATLAS. Call detail information for outgoing telephone calls for the last 11 years is stored and easily accessible for reporting purposes. Internal calls (those from one Virginia Tech telephone extension to another) have been collected and stored on an as-needed basis for traffic engineering analysis. Soon after the events of April 16th, internal call collection for all Virginia Tech telephone numbers was activated as was call collection for all incoming calls in an effort to maximize the ability to trace calls. Call detail information is generally available via database access within an hour of call completion and always within 24 hours of call completion.

Emergency Call Traces

Emergency call traces are performed at the request of law enforcement in response to threatening or harassing telephone calls to Virginia Tech telephone numbers. The procedure for tracing emergency or malicious telephone calls typically involves interaction between several entities:

- Targeted individual (the person who received the phone calls)
- Virginia Tech Police Department
- Communications Network Services (CNS)

- Telephone service provider (for example, Verizon or AT&T)

The targeted individual typically reports the incident directly to the Virginia Tech Police Department providing the called telephone number and the date/time of the incident as source information. The Virginia Tech Police Department, in turn, engages CNS with the source information for a preliminary assessment.

CNS engineers have real-time access to completed call information via an internally developed Emergency Call Trace application and Adtran Atlas (not to be confused with the ATLAS information system) devices.

Adtran Atlas devices are used as intermediary, integrated services digital network (ISDN) switches with connectivity to the public switched telephone network (PSTN) and the Virginia Tech telephone system. These devices are utilized primarily for their ability to convert ISDN signaling from the PSTN to channel associated signaling (CAS) from the Virginia Tech telephone system. Utilizing the Atlas devices enables the university to use ISDN circuits for all incoming connectivity from the PSTN. ISDN circuits provide the capability for caller ID information to be delivered for incoming calls to university telephone numbers. The Atlas devices log all inbound and outbound calls providing an audit trail for malicious or suspicious calls.

If the originating caller's telephone number is available via the Emergency Call Trace application or Adtran Atlas transaction logs, CNS provides that information to the Virginia Tech Police Department for further investigation. If the caller ID has been blocked or spoofed, CNS and/or the Virginia Tech Police Department engage the external telephone service provider.

Caller ID spoofing is the practice of causing the telephone system to display a number on the recipient's caller ID display and the telephone system's transaction logs that is not the actual number of the originating caller. Caller ID spoofing can be facilitated by web-based telephone service providers who initiate calls on behalf of their subscribers allowing the subscriber to specify the originating telephone number, the destination telephone number, and the caller ID.

On June 27, 2007, the United States Senate Committee on Commerce, Science, and Transportation passed S.704, a bill that would make it a crime to spoof caller ID. Dubbed the "Truth in Caller ID Act of 2007," the bill would outlaw causing "any caller identification service to transmit misleading or inaccurate caller identification information" via "any telecommunications service or IP-enabled voice service." Law enforcement is exempted from the proposed rule.

Network Management Data

Information collected to support management and operation of the data network is sometimes used to assist in law enforcement investigations. The sources of information include the following:

- Logs from authentication systems controlling access to the university's Virtual Private Network (VPN), modem pool, and wireless networks. These logs include the userid used, session duration, and some address information.
- The IP registry shows the department or entity a particular IP address has been assigned to and the associated contact person.

- Data polled from Ethernet hubs and routers showing bindings between Ethernet addresses and IP addresses
- Cable plant data containing location information for all wired connections
- Flow information showing IP addresses and data volume
- Port statistics showing data volumes

All information collected and stored is used for the operation and management of the network. Its usefulness to law enforcement varies based on which systems were involved in a particular incident and how soon after the incident the information is requested. Network activities involve numerous data exchanges with numerous hosts, and many of the endpoints are mobile.

The general nature of network communications makes the binding between the available information (usually an IP address and timestamp) and the responsible individual fairly weak.

None of the network management information routinely collected includes the data contents--only header data (cf. envelope). In extremely rare cases, actual data contents are collected in response to court orders.

NetFlow log data are statistical summaries of flows (connections) that have passed a particular point in the network. The data content of the connection is not recorded. The logs do record the technical details of how the connection was established, when it happened, how long it lasted, and how much information was sent. NetFlow data are only collected at specific points in the network where they are needed for capacity planning and network management. It is important to note that the network is a large, distributed fabric. There is no single place through which all network traffic flows. At Virginia Tech, NetFlow data is collected primarily where network traffic enters and leaves the campus network and between campus and the primary servers in our data center. The average volume of NetFlow data is about 15-20 gigabytes per day. The logs are generally overwritten every five days.

[Redacted]

Personal Digital Information

The personal digital information covered by this report includes e-mail held on the university's e-mail server; files stored in an individual's digital Filebox; and files placed in a personal ePortfolio account.

All current Virginia Tech students, staff, and faculty are provided with an e-mail address. The university maintains a central e-mail server for all students, faculty, and staff. A Microsoft Exchange server is another option available only to faculty and staff.

Filebox is a web publishing and file storage service provided free of charge for all current Virginia Tech faculty, staff, and students. Filebox can be used to create a homepage for an individual or group, share files with friends and coworkers, transfer files, and backup important data. The default quota (space limitation) for Filebox is currently 30 MB.

ePortfolio is an online, personal information management system designed to give students, faculty, and staff the ability to create and distribute their educational records

and other supporting documents. The ePortfolio system provides a dynamic and efficient mechanism for collecting, integrating, and sharing a wide variety of academic, career, and personal information.

E-mail Logs

E-mail logs are stored for 18 months and contain every e-mail transaction (sending or receiving an e-mail message) that was routed through the Virginia Tech servers including:

- Any e-mail *to* something@vt.edu from anywhere in the world is received and logged on that system
- Any e-mail *from* a user, whether they use a valid vt.edu address or another address (e.g. they list their return address as their hotmail address), sent using the Virginia Tech e-mail servers is logged
- Any e-mail sent using the Virginia Tech webmail service is logged
- E-mail sent using another organization's e-mail server is not logged because Virginia Tech didn't process it. A user could, for instance, while at home, use their parents' computer, configured to use their cable company's mail server, to send e-mail with a return address of "vt.edu," and there would be no log record for this transaction. (The log record would be at the cable company's e-mail center, but Virginia Tech would normally have no knowledge of its existence.) However, any replies sent to that vt.edu e-mail address would be logged so the existence of one of those notes could be inferred.

University Mail

Mail Services collects and distributes letters and packages for university departments and residence hall students.

Virginia Tech Police Access to Information

The Virginia Tech Police Department has access to Hokie Passport, Parking, and some Banner information.

In Banner, authorized Virginia Tech Police personnel have the ability to search for class schedule information for a specific student. They do not have the ability to search for all classes and students in a particular building at a particular time. They do not have the ability to search for all employees working in a specific building at a given time.

Virginia Tech Police noted that accessing three systems separately is less effective than having a single, consolidated interface customized for their specific needs.

Information Release Authorization

Requests for Banner information and the related authorization for those requests are handled by the data stewards responsible for the particular information area. When data stewards need programming or data analysis, they engage Enterprise Systems to retrieve the information. Information is provided to data stewards for delivery to the original requestor of that information.

Requests for non-Banner information are made to management within Information Technology who work with University Legal Counsel to determine the appropriateness of the request and the proper course of action.

Observations

For purposes of this report, observations are classified in three categories-- Emergency Response, Law Enforcement Investigation, and Victim Assistance.

Emergency Response

Personal Locator Information

Initially on April 16th and 17th, the efforts of Enterprise Systems staff were focused on determining who was in Norris Hall by analyzing class schedules, employee office addresses, and employee mail codes. Spreadsheets of this information were produced and provided to the Virginia Tech Police.

Another source of personal location information was telecommunications service information. On the afternoon of April 16th, telecommunications user location information for employees in Norris Hall was provided to the Office of the Executive Vice President at the request of law enforcement. The information included employee names and room number locations for users of telephone and Ethernet services in Norris Hall.

Based on interviews with Virginia Tech Police, another source of location information used included electronic card access reports and photo IDs. The Virginia Tech Police worked directly with the Hokie Passport office to obtain this information.

Emergency Contact Information

Reports and queries were created to ascertain as much emergency contact information for victims as possible using any available emergency contact data and any available address listings.

Counseling Support

A number of queries were produced by Enterprise Systems for the Cook Counseling Center to provide information about the victims. Prior to the resumption of classes, a cross-compilation of the class schedules of all victims was generated to facilitate providing a counselor for the first meetings of each of these classes.

Donation Management Support

Almost immediately following the tragedy, the university began receiving donations. Enterprise Systems staff, working with University Development, adapted the on-line giving web pages to facilitate receiving these gifts. Subsequently, as victims' family information has been determined, Enterprise Systems staff, on behalf of University Development, has worked to modify development systems and processes. These efforts are intended to ensure communications to the families always reflect Virginia Tech's compassion for them and to make sure the university does not inadvertently send general, mass communications to any relatives of the victims.

Continuing Operations

A significant aspect of the processing and response activities of Enterprise Systems was providing data to enable completion of the spring semester. This work initially involved determining what classes would need to move from Norris Hall for the remainder of the spring semester and for subsequent semesters. Once that work was completed, Enterprise Systems facilitated the analysis and assignment of alternative classroom

locations. Data was provided to assist in the relocation of classes and in the communication of the changes to affected students and faculty. Implementing the amended academic policies for the spring semester also required a number of special reports for the University Registrar's office and the Office of the Provost as well as significant system modifications to accommodate end-of-term processing for the semester.

Privacy

Immediately following the tragedy, it was recognized that information concerning victims should be restricted from inclusion in the public directory. The University Registrar's office was asked to mark the student records as "confidential" in Banner to insure the information would not be publicly accessible from the Enterprise Directory.

Call Detail

Per requests from university management, near real-time call detail record information was provided for particular telephone numbers within the requesting department.

Law Enforcement Investigation

Telephone Call Detail Records

Telephone call detail records were provided to law enforcement officials in response to a Grand Jury subpoena. Call detail records included in the response covered the period from August 19, 2006 through April 16, 2007.

Analysis to confirm the availability of telephone call detail records for all victims for an expanded timeframe was also completed in preparation for additional legal requests. Those requests were not served; therefore, the additional information was not shared.

Victim Voicemail Records

Copies of existing voicemail for requested telephone numbers were provided to law enforcement officials in response to a Grand Jury subpoena.

Threatening Calls

Over a period of several weeks following April 16th, threatening calls were reported to the Virginia Tech Police, who, in turn, engaged CNS engineers to perform emergency call traces. In response to these requests, CNS provided copies of call detail records and copies of available related voicemail to law enforcement. Caller ID information for all the threatening calls was either spoofed or blocked. Therefore, law enforcement needed to forward the information provided by CNS to the telephone service provider to get the actual calling number.

Network Trace

Pursuant to a subpoena, a network trace was performed for an IP address under investigation.

E-mail Records

Pursuant to a court order, certain e-mail still stored on the Virginia Tech e-mail server was provided to law enforcement.

Pursuant to a court order, analysis was completed on e-mail log files. A raw listing of date/time, sender, recipient, and a listing of the frequency of each contact were generated.

University Mail

With an authorized release, Mail Services provided mail and package notices to law enforcement.

Victim Assistance

In many cases, families of the deceased victims requested any digital information (digital files) created by the victims and held on university systems. The personal digital information available varied by individual.

Each individual had an e-mail account. However, the configuration of the account determined whether there was e-mail residing on the central e-mail servers. In a few cases, e-mail had either been downloaded to the individual's computer just prior to the incident or it was forwarded to another e-mail account (i.e. Google e-mail account). In these cases, there was little or no e-mail on the central server. Retrieving e-mail held on the university central server is time-sensitive since university procedure calls for the deletion of e-mail remaining on the university servers if it is older than 30 days. In most instances, there was e-mail in the account which was downloaded to a compact disk (CD). The content of the e-mail was not reviewed during the downloading process.

There were eight deceased students who used the Filebox service. The contents in each victim's Filebox were downloaded to a CD. The content of the individual Filebox was not reviewed during the downloading process.

There were five deceased students who had opted to open an ePortfolio account. The contents of these accounts were downloaded to a CD. The content of the ePortfolio was not reviewed during the downloading process.

The Dean of Students office was informed about the different types of digital information so university representatives who were assisting the victims' families could inform the families about the kinds of information that might be available. When a request for the victim's digital information was received from the university representative or the Dean of Students office, the appropriate CDs were prepared. The CDs were turned over to the appropriate university representative assisting the victim's family or to the Dean of Students office to be delivered to the appropriate family member.

In addition, there were several instances where the next-of-kin for a deceased faculty member needed access to their spouse's e-mail account(s.) These faculty accounts remained active to allow for communications with the surviving spouses or, in some cases, the settling of estates.

Conclusions

- Information Technology (IT) was able to effectively support a myriad of immediate and evolving emergency response, law enforcement, and victim assistance data needs during and following April 16th. This ability was directly attributable to the following:

  - Having information systems containing student, employee, and system data readily available for analysis, reporting, and immediate implementation of critical process changes.
  - Having Information Technology staff with proven expertise in understanding the data and systems and their applicability to university processes. These individuals were able to quickly assess data requirements.
  - Having a well-established, close, working partnership between university data stewards, university management, IT data analysts, system administrators, and engineers. The relationship facilitated effective interpretation of the data requests.
- Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA) Compliance: One of the challenges immediately encountered was to insure compliance with FERPA and HIPAA requirements while still providing all possible assistance to emergency response personnel. The unfathomable circumstances created questions concerning interpretation of the regulations, such as the applicability of FERPA in the event of a student's death. Maintaining vigilant attention to the restrictions of FERPA and HIPAA added significant complexity to the urgent data needs of April 16th and the activities of the days that followed.
- Inadequate Emergency Contact Information: Another data issue of immediate concern was the lack of emergency contact information, particularly for students. Specific emergency contact information was found to be missing or unreliable for most students. In addition, parent information and home addresses were frequently not available. The student information system is set up to record these elements. However, this information is provided by students on a voluntary basis, and most had chosen not to enter it. In some cases, paper records for students were referenced in an attempt to find contact information.
- Location Information: An additional data challenge was determining who might have been in Norris Hall. Class rosters for classes scheduled in Norris were available as a starting point for locating students. But students could also be in Norris Hall for a variety of other reasons—for example, student employees or those using research labs. Determining which employees were working within Norris was difficult to verify for all employee types such as wage staff, adjunct faculty, etc. Various lists were generated using office mailing addresses, telephone and Ethernet locations, and class assignments, but none of these provided an all-inclusive resource.
- Electronic Card Access Reports and Photo IDs: Location and identity information is critical to emergency responders. Virginia Tech Police worked with the Hokie Passport office to facilitate access to this information.
- Building Usage: Determining an overall view of the activities and functions assigned to Norris Hall required correlating information concerning building functions and occupancy across various systems in an effort to determine employee usage, academic usage, lab functions, health and safety requirements, and overall building functions. While the cooperative and dedicated commitment of the various offices involved enabled this information to be gathered, having a more integrated view of the data would have greatly facilitated the process.
- Supporting Diverse Constituencies: Across many of the response activities, one overarching difficulty from a data perspective was insuring that the diversity of constituencies the university serves was appropriately considered. Whether the context was inclusion of adjunct faculty in e-mail listserv communications or the

office locations of student employees, an important aspect of each question was always defining and managing specific, unique groups of constituents. While this difficulty was addressed on a request-by-request basis, an integrated, enterprise-centric identity management system would have reduced some of the complexity of the process.

- There is a desire by families to retrieve digital information created or stored by deceased students. This wish is not unique to victims of April 16, 2007. Some digital information is perishable--specifically e-mail being held on the university central servers which may, as a result of normal operating procedures, be deleted after approximately 30 days.
- Ensuring the digital information is provided to the appropriate individual is a major concern. The university representatives assisting the family members were very valuable in identifying those who wanted the digital information and also ensuring it was turned over to the correct family member.
- Law enforcement and other first responders lack an accurate and accessible information source for person location information.
- Call trace functionality provides important information, but often the telephone service provider must also be engaged to complete investigations.

Short Term Recommendations

- Develop a report for inclusion on the Hokie SPA to provide information on instructors/students by building. This development is already in progress.
- Develop strategies, policies, procedures, and processes for promoting availability of emergency contact information for students and employees.
- Implement an operating policy to ensure that as soon as the university is notified of the death of a student, faculty or staff member, digital files the individual may have held on the e-mail servers, Filebox, ePortfolio, or any future storage services should be backed up in case the information is needed. The digital information should be placed on CDs when the official request for it is received. The content of these files must not be reviewed in the process of retrieving and copying the information.
- Continue to use a university representative to assist a victim's family members. This procedure proved to be a valuable process for determining a family's desire for any digital information and ensuring these files were provided to the proper individuals.

Long Term Recommendations

- Develop a consolidated and comprehensive personal locator information system while considering personal privacy and security. Much of this information already exists in disparate information systems such as Banner, Hokie Passport, and telecommunications systems. Existing information such as name, class schedule, emergency contact information, electronic card access logs, photo id, office address, and telecommunication service information could be consolidated into a data warehouse application. Another approach could be to make this information available to a personal locator application via Web Services interfaces to existing information systems.
- Existing personal locator information should be enhanced to include information on lab usage and location information for employee types such as wage and adjunct faculty.

- As telecommunications and pervasive computing systems evolve to include presence information, those sources of information could be made available as well.
- The system should leverage geographic information system (GIS) and computer-aided design (CAD) information as well to improve location based query functionality.
- Use identity management systems as a mechanism for more effectively managing diverse, campus constituent services and populations.
- Develop a consolidated, customized user interface for Virginia Tech Police to access appropriate university information.

Appendix XII: Managing Personal Information

Purpose

The purpose of this report is to identify how Virginia Tech manages personal information, to review how that information might have facilitated the university's response to the April 16th tragedy, and to determine what enhancements could be made to improve the management of personal information in the future. Personal information about students, faculty, staff, and other affiliates considered in this report includes the following:

- Personal identifying information; e.g., name, Virginia Tech identification number, biometric information
- Locator information; e.g., residential address
- Communications information; e.g., e-mail address, telephone number
- Emergency contact information; e.g., name, address, and telephone number of emergency contact

Summary

The originating, authoritative sources for Virginia Tech personal information are the SunGard Higher Education Banner system, the Enterprise Directory, and the subscription component of the VT Alerts system. Banner, the Enterprise Directory, and VT Alerts Automated Notification System are housed on university computers, maintained by Information Technology. There are currently no system processes requiring an individual to update his or her personal information once it is entered in one of these systems.

- Education and training are needed to encourage people to provide accurate personal information
- Students and employees could be required, or given the opportunity, to update personal information on a recurring schedule
- One option for promoting the regular update of personal information might be combining update requests with technology security awareness processes currently under consideration such as the renewal of the Virginia Tech personal identifier (PID) and password
- The university does not currently maintain any biometric identification information in any centrally managed repository. However, the Hokie Passport office maintains photos of students and employees; and some building spaces are secured using fingerprint readers.
- Performing additional integrity checks will improve the accuracy of the personal information maintained in the source systems

General Description

The SunGard Higher Education Banner system is the authoritative source for the majority of personal information for students and employees at Virginia Tech. Banner contains personal identifying information, locator information, and emergency contacts for students and employees. Student information is initially entered into Banner through the admissions and financial aid processes. Employee information is created as part of the hiring process. Students and employees may update portions of their personal information after they are accepted or hired. Some of the information may only be updated by the appropriate university office.

The Enterprise Directory is the authoritative source for the Personal Identifier (PID) and password. Students and employees create their own PID and password login credentials. A Virginia Tech default e-mail address is automatically generated for students and employees at PID-creation time. The Enterprise Directory is also the authoritative source of information for sponsored persons such as participants in short-term programs who are on campus only temporarily. Information Resource Management enters their personal identifying information, creates their PIDs, and sets an initial password the user must change within 24 hours.

Electronic communications contact information is entered in the VT Alerts Automated Notification system by eligible students, employees, and Virginia Tech affiliates. Information in the VT Alerts system is maintained by the owner of the information. Personal identifying information is not stored in VT Alerts. Instead, the contact information in VT Alerts is tied to a person's record in the Enterprise Directory by the Universal Identifier (UID), which is a unique, automatically generated number.

Observations

Over the last several years, the university has become less dependent on addresses and phone numbers as part of the identification process. Reasons for this change include the following:

- Student billing and payment is now provided online
- Grades are released to students online. Grade mailers are not sent.
- Benefits for employees are electronically managed by the state
- Employees have adopted an electronic pay stub
- Electronic W2s were piloted for the 2006 tax year and will be available to all employees for the 2007 tax year
- For students, once admissions and orientation activities have been completed, addresses or phone numbers are not used in any subsequent, routine, academic or business processes.

Upon entry of addresses and phone numbers, Banner provides some basic validation of the city/state/zip code combination. However, the address itself is not currently checked. Additional software could be integrated into Banner to check for a valid address. However, even this software would not be able to determine if this was, in fact, a legitimate address for that specific individual.

Employee work addresses are also of doubtful reliability. Many individuals do not actually work where they receive their mail or where they indicate their office is located. In addition, maintaining up-to-date employee address information is difficult.

In evaluating contact information for the various members of the campus community, other areas of concern are the many affiliates, workers, friends, and community members who visit the campus daily. The normal day-to-day operations of the university inherently bring many people to campus for whom we do not have identifying or contact information.

For individuals who have been given sponsored PIDs in the Enterprise Directory, personal identifying information is entered at the time the sponsored PID is created. But there is no emergency contact information entered or provided for these individuals.

Parts of VT Alerts not requiring subscription are available to the general population. The subscription component of VT Alerts is restricted to individuals with a Virginia Tech affiliation who have a significant likelihood of being on a Virginia Tech campus.

Short Term Recommendations

- Create a data policy group to make decisions regarding use, maintenance, and management of personal information.
- Continue to make students and employees aware of the VT Alerts Automated Notification System and the importance of providing accurate information to the VT Alerts subscription service.
- Educate students and employees about the importance of providing accurate personal information.
- Identify additional ways to make emergency notices and information available to those people who are on campus but might not be reached by the VT Alerts Automated Notification Systems.
- Provide students and employees with information about the need to manage sensitive personal identifying information.
- Provide students and employees with information about how Virginia Tech manages sensitive personal information.

Long Term Recommendations

- Create a university data stewardship council, selected from responsible positions among data stewards and data users, to review and coordinate implementation of data policies and recommendations.
- Undertake an effort to determine the types of emergency contact and locator information needed for faculty, staff, and students.
- Evaluate the need for emergency contact and locator information for individuals coming to campus for only a short time. Based on the finding, develop an implementation plan.
- Perform additional integrity checks on data entered into Banner, the Enterprise Directory, and the VT Alerts Automated Notification System.
- Use various online processes to present opportunities for people to update their personal information.
- Review data stewardship roles and communicate those roles to the university community.
- Classify university data according to Policy 7100, the Administrative Data Management and Access Policy.
- Investigate issues surrounding biometric identification including the associated privacy and security implications
- Create an enhanced, standardized, notification process for any potentially serious exposure of personal identifying information.

Appendix XIII: Response Centers

Purpose

The purpose of this report is to review response centers, both existing and those deployed as a result of the events of April 16, 2007, and document timelines (as applicable) for each. The report evaluates the performance (level of success) of the centers and makes recommendations for improving the process for establishing them and enhancing the response level in an emergency situation.

Summary

Following the morning events of April 16th, the need for various types of response centers became immediately apparent. These centers can be categorized into six types:

- Parents and families of all victims: A primary need was to have individuals available to answer questions from families of the victims and to provide information to them.
- Public relations: Provide a centralized off-campus location for all media to gather.
- Law enforcement: Provide an on-campus location for coordination of all law enforcement activities.
- Counseling: Provide counseling to faculty, staff, and students who needed help in coping with the situation.
- Assistance: During a situation such as this, some individuals want to help in various ways (i.e. volunteering, donations, service, technology).
- Emergency Response: Healthcare and other agencies that need to respond immediately.

General Description

During the days and weeks immediately following April 16th, the need for various call/command/response centers was recognized. These centers needed to be strategically located and well-equipped with telephones, data connections, computers, and people to staff them. The staff needed to have the necessary information to answer questions. They needed to be fed. The computers needed the appropriate software loaded and the appropriate level of security installed.

Information Technology (IT) played a major role in providing for and supporting these needs. Many individuals involved in coordinating the set-up of a center provided positive feedback about Information Technology's rapid response and ability to establish a center, within hours, with no advance notice.

Some of the services provided by Information Technology included:

- installing telephone lines within a few hours of a request
- installing fax lines
- installing network hubs to facilitate wireless access
- providing and setting up computers
- providing and setting up printers, shredders, and fax machines
- installing cable television connections
- providing and setting up televisions

- working with Risk Management and Purchasing departments to bypass the normal order processing procedures in order to make emergency purchases

Groups involved within Information Technology included:

- Switch Engineering
- Field Engineering
- Order and Provisioning
- Systems Development and Administration
- Video/Broadcast Services
- Information Technology Acquisitions
- Business Operations

Observations

Response/Command Centers:

Virginia Tech Parent Information Response Center

Shortly after the events occurred on April 16th, the Office of the Dean of Students (DOS) recognized the need to establish a center to answer and respond to calls from parents, families, and friends. An "800 number" and significant space were needed for the center and were not available in the DOS office. They quickly identified the Virginia Tech Student Calling Center, located at the University Mall, as a possible location for such a call center. Follow-up discussions with University Development revealed telephones were not located at every station, and the phones were not set up to receive incoming calls. Discussions with Communications Network Services (CNS) about changing the calling capabilities on these phones revealed that a response center in RB14-109 was already configured with the services (telephones, data connections, and computers at individual stations) needed by the DOS and available for their use.

By 5:00P.M. on April 16th, the call center was established in RB14-109. University employees, employees from the Virginia Department of Emergency Management, and local volunteers manned the telephones. This center operated 24 hours a day.

Initially, many of the individuals who answered the call center telephones did not have the information needed to answer questions posed by the callers. Because of the call center location, many CNS employees attempted to provide information to support this group.

Arrangements had not been made to provide food for the call center personnel. CNS provided food and drinks for the workers there.

This call center received calls from individuals who did not speak English.

Public Information Office

The Public Information Office (PIO) had to be located in Burruss Hall, close to both the President's office and to University Relations.

Within two hours, Information Technology was able to respond and provided all requested devices and connections. There was no reason or need to go to any source outside the university.

Preparations for this center included the installation of telephones, data connections, and a video connection. Information Technology also provided laptop computers, a printer, and a fax machine.

University Relations

A center was established in the Alumni Center Board Room, located in The Inn at Virginia Tech, to assist University Relations with media inquiries. University Relations was not able to handle all the calls coming into their main telephone number, located in 318 Burruss Hall. This telephone number was forwarded to a group of 12 phones installed by CNS in the Board Room. CNS also provided, installed, and configured a fax machine, printer, and laptop computers. The advantage of providing space for the press at The Inn was the available space in conference rooms in which they could set up.

Student Assistance

This center was initially established in the Solitude Room at The Inn at Virginia Tech. It was designated as a place for mental health groups to meet and coordinate their activities. Phones and personal computers were provided. The need to be located on campus resulted in this center moving to the Squires Commonwealth Ballroom. Eventually, the group moved to smaller rooms in Squires. Information Technology established network and telephone connections for this center and provided computers, a fax machine, and printer.

Command Posts for VTPD, State Police, FBI, ATF

Command posts were established in Burruss Hall, Lane Stadium, and the airport. All needed network connections, phones, faxes, and printers were provided. Command posts on and off campus were used.

Alumni Development

A command center was set up in RB14-109 in response to Dr. Steger's appearance on "Meet the Press" and in preparation for a response expected from Oprah Winfrey mentioning Virginia Tech on her program. The latter never happened but having almost immediate access to these necessary support areas was critically important during the recovery period.

College Command Centers

The College of Engineering used 260 Durham Hall as their command center. Three areas provided the Dean of Engineering with critical support: CNS, Moving and Hauling (to move the Dean's office and Engineering Science and Mechanics faculty and staff), and the Virginia Tech Police Department (to keep them informed). Having almost immediate access to these necessary support areas worked well for them during the recovery period.

University Switchboard

The university switchboard functioned normally. However, during the week of April 16th, the quantity of calls normally processed tripled in number.

Call totals, including those from the previous and following weeks, are shown below for comparison purposes.

DATE	CALLS
4/9/07- 4/15/07	3224
4/16/07 - 4/21/07	9878
4/23/07 - 4/29/07	3183

The university switchboard began receiving calls requesting information almost immediately after the event.. The operators did not have all the information needed to respond to the callers. Standard language and approved information updates from various university offices would have decreased the time required to handle calls and ensured consistent, approved information was relayed to callers.

Montgomery Regional Hospital

The director of Staff Development/Emergency Management for Montgomery Regional Hospital (MRH) indicated they became aware of the events of April 16th via informal methods, such as media reports and police scanners. At this point, they implemented their emergency response plan. Montgomery Regional Hospital received calls from employees of other regional hospitals who were trying to obtain additional information.

Other Support

In addition to its role in establishing response centers, Information Technology played a critical role in moving academic departments (Dean of Engineering and Engineering Science and Mechanics) from Norris Hall to other buildings. Telephone and data connections were installed. Computers were provided, set-up, and needed software installed. Much of this work was performed on the Sunday afternoon and evening prior to classes reconvening on Monday morning, April 23rd.

Conclusions

- Call/command/response centers must be established as quickly as possible.A predefined list of available call centers, along with a list of known personnel resources to answer the telephones, would facilitate the expeditious set-up of these centers.
- During the days and weeks immediately following April 16th, Information Technology worked with administrators across the university to quickly respond to their requests for assistance in establishing call/response centers.

Short Term Recommendations

- Establish a team to develop an overall plan for call/response/command centers. The plan should address the following:
  - Developing a list of rooms easily able to be converted to call/response/command centers. Rooms should be geographically dispersed around campus and include off-campus locations.
  - Installing phone connections to allow both incoming and outgoing calls
  - Staging phones close to the proposed center locations, ready for deployment
  - Installing Ethernet portals and video connections
  - Identifying computers available for use in a call/response/command center. Sources include the laptop loan program operated by Information Technology Acquisitions (ITA) and university computer labs. Identify labs able to serve as

call centers or from which computers can be "borrowed." ITA also has a relationship with hardware vendors allowing computers to be purchased or borrowed very quickly.
    - Identifying software to be loaded on each computer for use in an emergency situation. Address security as part of the setup.
    - Compiling a list of system administrators, along with their contact information, who could be reached to set up computers and load software
    - Equipping every center with operating supplies (e.g. white board, phone books, etc.)
    - Equip every center with a fax machine and printer
- Maintain two "800 numbers' in reserve for use in emergency situations. Ensure the Continuity of Operations Plan (COOP) for the university notes the availability of these numbers.
- Develop a script of Frequently Asked Questions (FAQs) for use by those answering the phones. These questions should include those applicable to any situation and those that are situation-specific.
- Develop a resource list (with contact information) of individuals who speak languages other than English
- Develop a procedure with instructions for the handling of malicious calls.
- Engage the International Association of Campus Law Enforcement (IACLEA) to consult with Virginia Tech about the establishment of command centers
- Provide timely information updates to all university call centers that interface with the public and with university employees

Long Term Recommendations

- Implement a unified response center for all responding and emergency teams.
- Develop a plan for establishing emergency call, response, and command centers for critical support areas.
- Conduct drills to test emergency call/response/ command centers deployment.

Exhibit A: Response Center Details

VT Parent/Family Information Line

Sponsoring Entity: Dean of Students
Location: RB14 Classroom 109
Purpose: Point of contact for families of victims.

1. 4/16 (10:05 a.m.): Associate Vice President for Network Infrastructure and Services was asked to activate the call center. Phones were staged in this area. Service was already active.
2. 4/16 (5:00 p.m.): Decision was made to use as the location for Virginia Tech Parent/Family Information Line
3. Arrangements were made for 12 telephones to support the inbound toll-free number. Three additional telephones were reserved for media calls. These lines were not used and were later allocated to the Virginia Tech Parent/Family Information Line. Calls from Dean of Students Office, were also forwarded to RB14-109.
4. Systems Development and Administration staff arranged computer access for volunteers. The location is a classroom, so computers were already installed and ready for use.
5. CNS continued to support University Development by answering questions and providing food.
6. Staffed by volunteers until midnight and Department of Emergency Management staff from midnight until noon 4/17
7. 4/18: New toll-free telephone phone number, established by Virginia Information Technologies Agency (VITA).
8. 4/26: No longer used by Dean of Students

Note: University Development became involved because they were originally contacted by the Dean of Students requesting use of their Student Call Center, located in University Mall, for the Virginia Tech Parent/Family Information Line.

University Development Response Center

Sponsoring Entity: University Development
Location: RB14 Classroom 109
Purpose: Prepared to accept donations in response to media events.

1. 4/22: President Steger appeared on “Meet the Press.” Room was staffed to answer calls.
2. 4/29-30: Staffed to respond to possible calls from “Oprah” fans. Oprah was supposed to mention the incident on her show.
3. 5/1: No longer used by University Development

Public Information Office

Sponsoring Entity: University Relations
Location: 318 Burruss Hall
Purpose: Coordinated a consistent dissemination of information. The phone bank was originally established in the Holtzman Alumni Center. University Relations soon realized this center needed to be closer to the University Relations office and to President Steger Center was moved to 318 Burruss.

1. 4/19: Move phones for offices occupying 318 Burruss to 400 Burruss. Installed six phones and one video connection, 18 data (hub), one analog line, and television service.
2. 4/20: printer, fax, three laptop computers installed by System Development and Administration (from Holtzman). Other laptops provided by Information Technology Acquisitions were also moved from Holtzman to Burruss 318.An Automatic Call Distribution (ACD) system and two call processing boxes were provided to forward their main number, and process the calls being received. Calls were distributed by time of day. During normal working hours, calls were sent to the phone bank for handling. During non-working hours, calls were answered by call processing boxes with an announcement indicating the center was closed and when it would re-open.
3. 4/24 Installed one phone and one network connection. Changed the lines able to be answered/used on two phones
4. 4/27: Center removed. Restored telephone service in 318 Burruss. University Relations number, was restored in 314 Burruss Hall. As of 6/26/07, it is still answered by a temporary staff member.

Command Post FBI/ATF/State Police

Sponsoring Entity: Virginia Tech Police Department
Location: [Redacted]
Purpose: To provide centralized location for the FBI, ATF, and State Police to operate [Redacted]

Command Post Virginia Tech Police Department

Sponsoring Entity: Virginia Tech Police Department
Location: [Redacted]
Purpose: Provide an emergency response and incident command post

1. 6/14: Installed an Ethernet connection and telephone. An additional four portals are available for use in this room, once activated.

Secret Service

Sponsoring Entity: Virginia Tech Police Department
Location: [Redacted]
Purpose: Provide communications support for Secret Service in preparation for President Bush's visit.
[Redacted]

Emergency Resource Response Group

Location: 400 Burruss Hall, Solitude Room at The Inn, RB14-115

1. 4/18: 400 Burruss: Set up phone
2. Initial meeting held in Solitude Room at The Inn
3. 4/19: Began holding meeting in RB14-115 (meetings 4/19, 20, 23, 26)

Student Assistance Center

Sponsoring Entity: Student Affairs, Cook Counseling
Purpose: To provide counseling services.

- Solitude Room: Provided a centralized location for community services groups to meet
- Squires Commonwealth Ballroom: Counseling services for students
- Brush Mountain Room: Counseling services for faculty, staff, students
- West Side Lane Stadium: This area was used as a meeting point for mental health volunteers who attended classes the first week they resumed after the events of 4/16
- Squires 202 and 218

Location: Solitude Room at The Inn, Squires Commonwealth Ballroom, Squires 202 and 218, West Side Lane Stadium, 5th floor Press Room

1. 4/18: Solitude Room: Provided and set up three computers, a printer, and an Ethernet hub for network connections. The Inn provided the phones
2. 4/20: Move to Squires Commonwealth Ballroom. Four phones were installed in Squires
3. 4/25: Partially moved to Squires 202 and 218: Phones, three computers, fax, and printer moved.
4. 4/25: Remainder moved from Squires Ballroom to West Side Lane Stadium, 5th floor Press Room. Five telephones and fax.
5. 4/27: Squires 202 and 218 closed. Phones, hub, and computers picked up.

University Relations - Alumni Center Board Room

Sponsoring Entity: University Relations
Location: Holtzman Alumni Center Board Room
Purpose: To assist University Relations with media inquiries. University Relations was not able to handle the many calls coming into their 318 Burruss Hall location.

1. 4/17 (11:00) Requested installation of a group of phones staffed by university personnel to assist University Relations with media inquiries. Forwarded Office of University Relations telephone number to the Board Room.
2. Staged equipment and fulfilled request for a call center with 12 phones
3. Noon: Deployed a fax machine, a printer, and two laptops to the Board Room of the Alumni Center to assist University Relations with media inquiries. Assisted Information Technology Acquisitions with the configuration and activation of six additional laptops. Set up televisions.
4. 4/25: Left Holtzman. Reduced the number of phones and moved them to 318 Burruss Hall.

Triage Area

Sponsoring Entity: Virginia Tech Police Department (Virginia Tech Rescue Squad)
Location: [Redacted]
Purpose: Provide a temporary command center to respond to the rapidly occurring events.

1. 4/16 (11:15 a.m.): Call to install phone.

Virginia Tech Police Department Trailer

Sponsoring Entity: Virginia Tech Police Department
Location: [Redacted]

1. 4/16: One phone installed.

Command Post Montgomery County Sheriff

Sponsoring Entity: Virginia Tech Police Department
Location: [Redacted]
[Redacted]

Massengill Panel Liaison – Governor's Review Commission

Sponsoring Entity: President's Office
Location: RB7 Suite 1100
Purpose: To serve as the university's liaison with the Massengill Panel. Lenwood McCoy will clear and coordinate all responses to requests for information relative to the events of April 16th, including those originating from individuals or groups other than the Panel.

1. 4/30: Installed four phones and six data connections

Appendix XIV: Cyber-Security

Purpose

The purpose of this report is to examine the security of many of the information technology services at Virginia Tech and to determine how these systems performed during the tragedy of April 16th. The report will also attempt to determine, in the aftermath of the tragedy, what enhancements might improve the security of these services. Services included in this report are as follows:

- Data Communications
- Web Communications
- Radio Systems
- Cellular Service and 911
- External Networks
- Traditional Telephone Services
- Video Services, including Cable TV
- Response Centers
- Data Preservation
- Data Retrieval

Summary

- There were no known information security breaches at Virginia Tech due to the events of April 16th. However, if a major security exploit had been launched during that period, it is likely the open-network environment instituted in order to allow guest access would have contributed to significant network and computer security problems.
- E-mail and instant messaging communications systems performed well. Utilizing resources from a high-speed research network enabled the data network to handle the increased load generated by the events of April 16th. The main webpage (www.vt.edu) was "slimmed down," and servers were reconfigured in order to handle the increased activity on that site.
- Fortunately, there were no failures on some of the older equipment. Repairing aging systems might have been difficult and potentially could have caused critical services to be unavailable.
- Better interoperability between radio systems would be valuable to emergency response personnel. Radio and cellular systems need to operate better inside some buildings.
- Personal data and university-owned data was utilized, retrieved, and preserved in a manner that protected personal privacy and the integrity of the data.

General Description

The three basic elements of security are confidentiality, integrity, and availability. Security is an integral part of the planning process for Virginia Tech's Information Technology infrastructure. While there were no known security breaches due to the events on and surrounding April 16, 2007, the need for confidentiality, integrity, and availability of services was never higher than during this time. In order to ensure our preparedness for future emergencies, it is important to assess the effectiveness of each area under review relative to the three basic elements of security.

Observations

Data Communications

As documented in the Data Communications Utilization and Performance report, the data network provided adequate service to support information distribution and applications related to the response to the events on April 16th. As the traffic on the network increased past 70 percent, measures were taken to increase network capacity. By utilizing the Mid-Atlantic Terascale Partnership (MATP), the university's network engineers were able to rapidly increase network capacity using resources normally dedicated to research activities.

Although the university's core and distribution networks experienced no significant problems during the April 16th time frame, aging network equipment increases the risk of network failure at any time. That risk increases as network load peaks, and the need for a reliable service becomes more critical during an emergency situation.

The requirement for authentication on the wireless network was eliminated in order to provide wireless access to non-Virginia Tech affiliates such as emergency responders. The removal of authentication opens the network to increased abuse and limits our ability to trace abuses to a specific individual. Existing computers on the Virginia Tech network may be exposed to vulnerabilities introduced by guest computers, and guest computers, usually "protected" by a corporate firewall on their home networks, may be exposed to new vulnerabilities. The Data Communications Utilization and Performance report emphasizes the need for a better solution to allow guest access to the wireless network.

The ability to employ a private, encrypted, instant messaging system such as the one deployed at Virginia Tech was valuable during the April 16th events. The university's e-mail systems and Information Technology's internal wiki (http://en.wikipedia.org/wiki/Wiki) were also effectively utilized. There seemed to be little concern about the authenticity of the e-mail messages sent by University Relations. However, some method of digitally signing or otherwise authenticating the sender of such messages should be considered in the future.

Web Communications

Problems with availability of centrally hosted web services occurred due to the high demands placed on the Virginia Tech homepage, www.vt.edu. To mitigate the problems, the complexity of the content on the homepage was reduced. However, access to other informational pages was also impacted by the heavy load on the web hosting server. The ultimate resolution was to increase capacity for the web hosting server. This increase was accomplished by using load balancing to allow additional hardware to be added to multiple server pools. The memorial website created as a result of the tragedy was heavily used. Eventually it was moved to be hosted externally.

Radio Systems

Radio systems offer a reliable, but insecure, means of communication. Although security was not a major concern relative to the radio systems used on April 16th, several issues merit consideration in any upgrade or replacement plans.

The lack of interoperability between systems used by the different agencies could cause delays putting people at risk. Interoperability is an issue to be addressed. Backup radios should also be available.

Although not identified as a major issue, the open nature of radio communications allows anyone with the proper receiver to listen to narrowband FM, public safety radios. There is no authentication of the station with which a person is communicating.

Many agencies had difficulty with signal loss inside buildings on campus. Again, this problem was not viewed as a major issue, but it should be addressed when implementing future systems. While not an issue during the April 16th events, vulnerabilities to jamming and interference should be considered in the design of future systems.

Cellular Service and 911

The existing cellular and 911 services experienced no major security-related issues except for reduced service availability due to the overall increase in volume of calls. Multiple service providers brought in Cell on Light Truck (COLT) units to add capacity to the cellular networks. No security issues were identified with the 911 services, but inefficient service could impact an agency's ability to respond. Work is underway by Blacksburg Police, Montgomery County Sheriff's Office, and Christiansburg Police to terminate transferred calls on the university's dedicated 911 lines instead of Virginia Tech Police Department administrative lines. The need to enhance indoor cellular coverage was recognized.

External Networks

See the reference to the Mid-Atlantic Terascale Partnership (MATP) in the Data Communications Utilization and Performance report.

Traditional Telephone Services

The current wireline telephone service at Virginia Tech requires physical access to the telephone handset in order to listen to or deliver a call. Therefore, the current system has minimal security vulnerabilities affecting confidentiality or integrity of the transmitted message. However, the age of the current system could result in some availability issues because an aging system is more difficult to maintain than a current one. Vendor support personnel are less familiar with older systems and parts are hard to obtain. The old system may fail in unexpected ways, making it more difficult to ensure uninterrupted service.

As new voice systems based upon packets are evaluated, the same security concerns we have for our current IP-based data network will need to be addressed for IP-based telephony technology. Encryption, reliable packet delivery, intrusion detection and prevention, etc., will be required in any new system deployed at Virginia Tech.

Video Services, including Cable TV

The Campus Cable System and Interactive Videoconference Systems were not used to send emergency alerts on April 16th, so no security issues were identified. If the existing systems were augmented and enhanced, they could be used in the future as part of an integrated campus emergency alert system. At that time, the integrity and availability of the current systems should be assessed. Best practices for maintaining backups and archives of broadcasts may become more important if the use of these systems grows.

If an infrastructure for building surveillance is created using video and audio services, privacy issues must be considered, with careful attention to state and federal regulations. Access to logs and tapes will need to be restricted and appropriate procedures to permit authorized access will be required.

Response Centers

No security issues were identified relative to the provision of response/command centers needed due to the April 16th tragedy. The fact that computers were provided to many people during this time calls attention to the need to secure those computers before they are connected to the network.

Data Preservation

All centrally-maintained production servers are backed up to tape media daily. Normally, a backup tape is retained for some period of time and then expired or reused according to a tape rotation schedule. In order to preserve information relative to the events surrounding April 16th, backup tapes for Banner, communications, courseware, e-mail, Enterprise Directory, Filebox, Network Attached Storage, Storage Area Network, web hosting, and departmental servers using the central backup service were taken out of rotation and not expired. The preserved backup tapes are securely stored in an off-site storage vault and can only be accessed by authorized personnel.

For selected individuals identified by university, state, or federal authorities, copies of the e-mail content, Filebox content, ePortfolio content, and voicemail recordings were preserved on compact disk (CD) or digital video disk (DVD.) Working closely with law enforcement officers, the content was preserved in a secure manner, ensuring the integrity and privacy of the data. In addition to this content, copies of Enterprise Directory logs and Network Flow data for certain days in April 2007 were preserved on CD and DVD. The CDs and DVDs not given to authorities are stored in a secure area with extremely limited, restricted access.

Images are being created of certain personal workstation (laptop or desktop) computer hard drives to fulfill data preservation requirements. The process for making the images preserves the integrity of the data and the privacy of the individual. After being created, the hard drive images are being stored in an encrypted form on the Network Attached Storage server for long-term preservation and access by authorized parties.

The data being copied and/or preserved was securely handled in accordance with university policy and state and federal legislative and regulatory requirements. Any transmission over the network was done using encrypted channels (secure FTP). Data preservation and collection was done under the oversight of a working group that included attorneys from the Office of the University General Counsel, management in Network Infrastructure and Services, and a private consulting firm specializing in data retention requirements and procedures.

Data Retrieval

Information Technology retrieved data and records in order to support emergency response efforts, law enforcement investigations, and to assist the families of victims of the April 16th tragedy. Information included telephone call detail records, copies of voicemail, locator and contact information, e-mail logs, and network traffic information, as well as content from e-mail, Filebox, and ePortfolio. Normal logging operations record

header information to show data exchanges between various hosts and, in the case of e-mail, senders and recipients. The logs do not contain message content.

The retrieval and release of information from the SunGard Higher Education Banner system was authorized by the data steward responsible for the particular information area. Non-Banner information was retrieved and released under the direction of Office of the University General Counsel. The University Registrar's office marked deceased student records as "confidential" to prevent their public display in the university's searchable, online directory.

Information Technology responded to requests from the Dean of Students office for content from deceased students' e-mail, Fileboxes, and ePortfolios by downloading the content to a CD. The content was not reviewed during the downloading process. The CDs were turned over to the Dean of Students office or to the appropriate university representative assisting the victim's family.

Conclusions

- Service availability (data, wireline, and cellular networks, web hosting) can become a problem when usage peaks. The ability to quickly add capacity during an emergency is extremely valuable.
- Redundant equipment for critical services should be located outside Blacksburg.
- Cellular and radio service is less than optimal inside some buildings.
- The ability to quickly deploy emergency equipment (computers, radios, cell phones, batteries) is needed.
- Aging equipment and systems (network, radios, wireline technology, computers) put the university at risk because old equipment is difficult to maintain and more challenging to restore when it fails.
- Access to personal information and digital content stored in university systems is crucial to the university's ability to respond to an emergency situation. Procedures used in response to the events surrounding April 16th were secure; but processes for updating, protecting, retrieving, and preserving personal information and content can be enhanced with additional policies, standards, and procedures.

Short Term Recommendations

- Improve the provisioning process for wireless guest service during emergency situations.
- Ensure critical services have the capacity to handle peak loads such as those occurring during emergency situations.
- Continue to enhance off-site redundancy for critical services.
- Educate students and employees on the importance of providing accurate personal information.
- Provide students and employees with information and standards on how to manage sensitive personal identifying information.

Long Term Recommendations

- Develop a secure method to allow non-Virginia Tech affiliates to access the Virginia Tech network in an emergency. Ensure the network access provided for guests:

  - supports the ability to identify a resource with an ongoing problem in order to isolate it from the network or require the owner to secure the resource. (See University Policy 7010, Policy for Securing Technology Resources and Services).
  - can be enabled quickly during an emergency.
- Upgrade aging equipment to reliably support services that must be available during an emergency situation.
- Build redundancy into critical new systems and services.
- Improve interoperability of radio communications used by emergency personnel in multiple agencies.
- Improve operation of radios and cell phones inside buildings to increase availability of those services. Where radio and cell phone service is poor, using the university's wireless network could be a solution, as long as secure guest access to the wireless data network is provided.
- Evaluate the need for encrypted communications technologies for law enforcement officers.
- Establish institutional policies and procedures for data protection, preservation, and retrieval to maintain the security of the data and the privacy of the individual.
- Establish a university data stewardship council, with members selected from responsible positions among data stewards and data users, to review and coordinate implementation of data policies and recommendations. Classifying data according to University Policy 7100, Administrative Data Management and Access Policy, will facilitate the work of this council.
- Implement an identity management system to more effectively manage the university's diverse campus constituent services and populations.

Exhibit A: References

Conversations with members of and materials submitted by the following report working groups:

- Data Communications Utilization and Performance
- Web Communications Utilization and Performance
- Radio Communication Systems Utilization and Performance
- 911 Systems Utilization and Performance
- Cellular Service Utilization and Performance
- Traditional Telephone Service Utilization and Performance
- Video, Campus Cable Television, and Related Broadcast Systems Utilization and Performance
- Response Centers
- Data Preservation
- Data Retrieval
- Managing Personal Information

Appendix XV: VT Alerts Automated Notification System

Purpose

The purpose of this report is to discuss the review process and selection criteria for the VT Alerts Automated Notification System, implementation decisions and recommendations, the relationship with VT Alerts, and the current subscription status.

Summary

- As part of the review of advanced messaging options, and as a result of the incident that occurred on the first day of classes in fall semester 2006 (August 21, 2006), a group was formed to review and analyze various vendor-provided, automated event notification systems.
- The purpose of these systems is to provide hosted services to send emergency messages, or other communications, to cellular telephones (or other wireless devices) through SMS (Short Message Service; so-called text messaging), through e-mail, or to regular landline telephones.
- Membership in this review group included staff from the following groups:
  - Student Programs
  - University Relations
  - Virginia Tech Police Department
  - Communications Network Services (CNS) Systems Engineering
  - CNS Research and Development
  - University Computing Support (UCS)
  - Secure Enterprise Technology Initiative (SETI)
  - Collaborative Technology Unit (CTU)
  - Learning Technologies
  - Network Infrastructure and Services (NI&S) Systems Support
- Two vendor products were demonstrated prior to April 16, 2007, and three after that date.
- The review committee unanimously selected 3n (National Notification Network) Online, and the product was purchased using emergency procurement procedures. The contract with the vendor was signed on May 16, 2007. The desired feature list for an emergency notification system, prepared by this committee, is included in Exhibit A of this report.
- The system was ready to accept subscriptions on July 2, 2007.
- By the end of the first day (July 2nd), over 2,000 students, faculty, and staff had subscribed. This number increased to over 4,000 by the end of the first week (July 6th).
- As of August 9, 2007, the VT Alerts Automated Notification System had 10,922 subscribers. Seventy-eight percent of the subscribers are students, 21% are staff, and 14% are faculty. (Some faculty/staff are also students.)

General Description

VT Alerts

Prior to the implementation of an automated event notification system, University Relations used seven methods of communicating urgent messages. All of these methods were used on April 16th:

- Broadcast e-mail to @vt.edu addresses (via LISTSERV)
- Broadcast voicemail to campus phones (offices and residence halls)
- Recorded message on the WeatherLine/Hotline (540/231-6668)
- VT.edu (www.VT.edu) and the Virginia Tech News website
- University switchboard
- Public media (TV, radio, news websites)
- Siren System

The general public has access to all of the above methods.

Virginia Tech students, faculty, and staff can now subscribe to an automated event notification system that will notify them of an emergency situation. Each subscriber can select up to three different ways to be contacted. These contact methods include the following:

- Text message (SMS) to mobile devices
- Instant message (AOL, MSN, ICQ, and Yahoo)
- E-mail (including non-VT addresses)
- Phone call to office
- Phone call to residence
- Phone call to mobile number
- Phone call to another destination

All of the above methods of urgent and emergency communications have been branded as “VT Alerts”. The system requiring subscription is referred to as “VT Alerts Automated Notification System. “

Implementation

Implementation decisions for the VT Alerts Automated Notification system include:

- All subscriber data will be collected and stored locally. This data will be uploaded to the vendor and used by the vendor system to send notifications. All additions, deletions, and changes to subscriber contact data will be reflected locally and on the vendor’s system. This implementation not only provides redundancy (data stored in two dispersed geographical locations) but also removes vendor dependencies. No information able to be used to identify any individual is passed to the vendor’s system.
- Each subscriber will be responsible for entering and maintaining his/her own contact information. Data will not be extracted from other systems; data will not be provided to other systems. The subscriber, not the university, has the responsibility for providing, and maintaining, accurate and valid contact information. A subscriber can update his/her contact information online at any time.
- Contact information provided by a subscriber will not be used for any purpose other than emergency contacts. Should future decisions be made to use this

information for any other purpose, the subscriber will be notified, in advance, and provided with appropriate options.
- This is an "opt-in" system. Each student, faculty, and staff member makes the decision to subscribe or not subscribe. A very aggressive public relations effort has been undertaken to inform students, faculty, and staff about the system.

Use

University Relations has developed a model for using the system that includes defining four scenario levels. Each level corresponds to emergencies of different types and seriousness beginning with Level 0 (the least serious) and progressing to Level 3 (the most serious). Modes of communication are suggested for each level, but use of each will be dictated by the specifics of the event. The scenario levels align with the university's Emergency Response Plan. (See VT Alerts – Virginia Tech's emergency notification service) The VT Alerts Notification System could be used for Level 2 and Level 3 events.

During an emergency, each subscriber will be contacted via their designated contact methods using the contact information they provided. Attempts to contact the subscriber will continue until either an acknowledgement is received by the subscriber or until a predefined number of unacknowledged attempts are made.

Observations

- Over 4,000 members subscribed during the first week the system was available, and subscriptions are increasing at a steady pace.

Conclusions

- VT Alerts, along with other notification methods being implemented, will help ensure a maximum number of people are promptly notified of an emergency situation.
- We, as a university, cannot force students and employees to be safe, but we do want to ensure they are aware of the opportunities to increase their safety. The only way we can do this is to have a record in VT Alerts indicating each person has made a decision to either subscribe (opt-in) or not subscribe (opt-out).
- Information from other systems should not be used to populate VT Alerts, and information from VT Alerts should not be used to populate other systems. If the university takes the responsibility of populating VT Alerts with emergency contact information, they assume part of the responsibility of ensuring this data is correct. The implications of the university entering a piece of incorrect contact data could be significant. The subscriber should be solely responsible for ensuring his/her contact data is correct. In addition, as long as the system continues to be "stand-alone", the subscriber may be more comfortable entering contact information which they would not provide for other reasons. This process may increase the likelihood of a successful contact during an emergency.

Short Term Recommendations

- Require every eligible subscriber (faculty, staff, and students) to either opt-in or opt-out of VT Alerts Automated Notification System

- Work with the Virginia Tech Police Department to determine if individuals from outside Virginia Tech (law enforcement and first responders) should be included in the VT Alerts Automated Notification System.
- Identify other individuals, or groups of individuals, who are not students, faculty, or staff, but have a university-related business reason to be on a Virginia Tech campus. Decide if these individuals are eligible to subscribe to VT Alerts Automated Notification System.
- Expand the methods for making emergency notices and information available to those people who are on campus, but might not be reached by the VT Alerts notification systems.
- Continue to have personal information in VT Alerts Automated Notification System provided and maintained only by the subscriber.
- Provide kiosks throughout the campus and encourage their use for subscribing to VT Alerts Automated Notification System.

Long Term Recommendations

- Develop a single interface from which University Relations can create an urgent message (in both text and voice format) and choose methods for delivery, order, and timing. While messages from the VT Alerts Automated Notification System can be sent using one interface, other types of VT Alerts notifications require different interfaces.

Exhibit A: Desired Features of the VT Alerts Automated Notification System

During internal working group meetings, a desired list of features for an emergency notification system was developed for Virginia Tech. The features most important to Virginia Tech may differ from those for other colleges and universities. Some of the many variables considered for choosing the most effective system include the size of the campus population, geographic location, and campus distribution. After reviewing the 3n product and discussing specific needs with 3n representatives after April 16, 2007, Virginia Tech determined the 3n product should meet the specific needs identified. The system features identified by the internal working group are as follows:

- Successful system would provide:
  - Multi-modal communications;
    - text messaging (preferably using true Short Message Service [SMS] protocol)
    - instant messaging (IM)
    - e-mail
    - web posting
    - voice communication to cellular or landline-based extensions (including ability to fax)
  - Flexibility in "registering" or "subscribing" users;
    - ability to preload based on existing directory data with both APIs and online mechanisms for batch or manual updates
  - Robust, but distributed, data centers, i.e. more than one location; ability to send alerts even if event impacts vendor's facility
  - Robust, but dispersed, messaging; concern is with saturation of communications channels ("too much, too soon" can quickly overwhelm cellular and landline telephony systems)
- The vendor would have to be flexible with terms of the contract, and be willing to collaborate on further development of the product's features to meet specific needs identified by Virginia Tech.

Appendix XVI: Telecommunications Working Group

Joseph C. Albert, Captain, Virginia Tech Police

Morgan W. Allen, Director, Systems Development and Administration, Network Infrastructure and Services

Phillip E. Benchoff, Senior Network Engineer, Network Infrastructure and Services

Earving L. Blythe, Vice President for Information Technology; Chair, Telecommunications Working Group

Charles Bostian, PhD., Alumni Distinguished Professor, Wireless@Virginia Tech; Electrical and Computing Engineering

Guy J. Cormier, PhD., Chief Information Officer, Virginia Bioinformatics Institute

Jeffrey M. Crowder, Program Director for NetworkVirginia, Mid Atlantic Terascale Partnership, VORTEX; Network Infrastructure and Services

Michael L. Dame, Director of Web Communications, University Relations

William C. Dougherty, II., Assistant Director for Systems Support, Network Infrastructure and Services

Mary B. Dunker, Director, Secure Enterprise Technology Initiatives; Enterprise Systems

W. Samuel Easterling, PhD., Ed., Professor and Assistant Department Head, The Via Department of Civil & Environmental Engineering

Richard G. Hach, Associate Director of Network Administration, Special Projects and Initiatives; Network Infrastructure and Services

Mark C. Harden, Manager, Video/Broadcast Services, Network Infrastructure and Services

Carl E. Harris, Director, Network Engineering and Operations, Network Infrastructure and Services

Larry Hincker, Associate Vice President, University Relations

Billy J. Hutson, Systems Architect, Network Infrastructure and Services

Judy L. Lilly, Associate Vice President, Network Infrastructure and Services; Co-Chair, Telecommunications Working Group

Randolph C. Marchany, Director, Security Lab, Information Technology Security Office

Mary Beth Nash, Associate University Legal Counsel, University General Counsel (Counsel to the Group)

John D. Nichols, Information Technology Manager, Network Infrastructure and Services

John F. Pollard, Director, Field Engineering and Service Operations, Network Infrastructure and Services

Jeffrey H. Reed, Phd., Willis G. Worcester Professor of Electrical and Computing Engineering; Director, Wireless@Virginia Tech; Bradley Department of Electrical and Computing Engineering

Patricia L. Rodgers, Director of Business Technologies, Network Infrastructure and Services

Jeb E. B. Stewart, Information Technology Chief of Staff and Director for Planning and Administration; Office of the Vice President for Information Technology

Brenda A. Van Gelder, Director, eCorridors Program; Office of the Vice President for Information Technology

Appendix XVII: Sub Working Group Members

Marvin Addison, Application Developer, Middleware; Secure Enterprise Technology Initiatives

Doug Atwater, Test Engineer, Test and Deployment; Secure Enterprise Technology Initiatives

Wanda Baber, Team Manager, Systems Engineering and Administration; Network Infrastructure and Services

Steve Beatty, Electronics Technician, Office of the University Registrar

Jeff Bevis, Director of Research and Development, Network Infrastructure and Services

Bill Blevins, Account Manager Senior, Communications Network Services

Betsy Blythe, Director of General Enterprise Applications, Information Warehouse and Access; Enterprise Systems

Jeffrey Brewster, Applications Programming Analyst, Integration and Portal Services; Enterprise Systems

Susan Brooker-Gross, Director for Policy and Communications, Office of the Information Technology Chief of Staff

George A. Cooper, Director, Business and Management Systems, Office of the Executive Vice President

Randy Crockett, Project Leader, Student and Financial Aid, Administrative Information Systems; Enterprise Systems

Jeff Dalton, Multimedia Producer Director Senior, Video/Broadcast Services; Network Infrastructure and Services

Wayne Donald, Information Technology Security Officer, Information Technology Security Office

Daniel Fisher, Project Manager, Middleware; Secure Enterprise Technology Initiatives

J. R. Fleeman, Test Engineer, Test and Deployment; Secure Enterprise Technology Initiatives

Henry Floyd, Project Management, Network Infrastructure and Services

Marvin Foushee, Associate Registrar, Office of the University Registrar

Deborah Fulton, Associate Vice President, Enterprise Systems

Karen Herrington, Director, Information Resource Management; Information Technology Security Office

Rosie Higdon, Director, Human Resources Technology Services and Employee Records; Human Resources Department

William Holbach, Coordinator, Assistive Technologies

Kimberly Homer, Test Team Manager, Test and Deployment; Secure Enterprise Technology Initiatives

Lee Anne Hoppe, Project Leader, Human Resources Information Systems; Human Resources Department

Vince Houston, Captain, Virginia Tech Police Department

Ron Jarrell, Team Manager, Systems Engineering and Administration; Network Infrastructure and Services

Raven Jennings, Customer Support Center Agent, University Computing Support; Network Infrastructure and Systems

Doug Jones, Field Engineering Manager, Communications Network Services

Vera Kidd, Associate Director for Administration and Business Services, Student Programs

Gail Kirby, Interim Director of Residence Life, Student Programs

Joyce Landreth, Assistant Director for Support, Virginia Tech Operations Center; Network Infrastructure and Services

Steve Lee, Research Engineer, Network Infrastructure and Services

Denise Linkenhoker, Program Support Technician**,** Virginia Tech Police Department

Barry Linkous, Telecommunications Engineer, Network Infrastructure and Services

David Martin, GIS-Cad Technician, Network Infrastructure and Services

Evelyn Martin, Assistant to Associate Vice President, Network Infrastructure and Services

Ken McCrery, Manager, Integration and Portal Services; Enterprise Systems

Deborah Morgan, Lieutenant, Virginia Tech Police Department

Christine Morrison, Project Management, Network Infrastructure and Services

J. Michael Moyer, Systems Engineer, Systems Engineering Administration; Network Infrastructure and Services

Mike Naff, Director, Administrative Information Systems; Enterprise Systems

Elaine Oliver, Web Designer, University Relations

Mark Owczarski, Director of News and Information, University Relations

William Plymale, Director, Research and Development; Learning Technologies

Tim Rhodes, Team Manager, Systems Engineering Administration; Network Infrastructure and Services

Kevin Rooney, Technical Lead, Information Resource Management; Information Technology Security Office

William Sanders, Director, Blacksburg Electronic Village; Network Infrastructure and Services

Joseph Schottman, Information Technologies Specialist, Video Broadcast Services; Network Infrastructure and Services

Anne Sheppard, Manager of Student Computing Programs, University Computing Support

Jitendra Shrestha, Web Designer, Integration and Portal Services; Enterprise Systems

Rick Sparks, Orientation Director, Dean of Students Office

Rob Sprague, Supervisor, Virginia Tech Operations Center; Network Infrastructure and Services

Doris Stock, Special Assistant to the Associate Vice President, Network Infrastructure and Services

Sam Tressel, Computer Systems Chief Engineer, Video/Broadcast Services; Network Infrastructure and Services

Diane Whitlock, Telecommunications Systems Planning, Communications Network Services

Doug Whorley, TV/Multimedia Systems Engineer, Video/Broadcast Services; Network Infrastructure and Services

Colin Wiseley, Audiovisual Systems Technician, Office of the University Registrar

Cindy Woods, Test Engineer, Test and Deployment; Secure Enterprise Technology Initiatives

Tom Wynn, Supervisor and Video Systems Engineer, Network Infrastructure and Services

Appendix XVIII: Contributors

Craig Allison, Sales, Two-Way Radio, Inc.

Steve Ayers, President and CIO, AnswerWorks, Inc.

Sherry Box, Communications Manager, Virginia Tech Transportation Institute

Bruce Bradbery, Captain, Police Services Division, Blacksburg Police Department

Eric Brown, Communications Research Engineer, Communications Network Services

Tom Carey, Custom Network Solutions Manager, Sprint Nextel

Steve Chiles, Network Operations Technician, Communications Network Services

Dan Cook, UNIX Systems Administrator, Communications Network Services

Martha Cox, Lead Communications Officer, Christiansburg Police Department

Kevin Davis, Technical Lead, Help Desk; University Computing Support; Network Infrastructure and Services

Jason Decker, Network Operations Technician, Communications Network Services

Jason Delacerna, Network Operations Technician, Communications Network Services

Jason Dominiczak, 1st Lieutenant, Vehi-Comm, Virginia Tech Rescue Squad

Faye Duncan, Communications Supervisor, Montgomery County Sheriff's Office

Shane Ellison, Data Warehouse Architect, Database Management Systems; Secure Enterprises

Russ Fenn, Applications Administrator, Database Management Systems; Secure Enterprises

Helen Franks, Major Account Manager, Sprint Nextel

Kim Gausepohl, Manager, Online Learning Systems, Educational Technologies, Virginia Tech

Sean Gillespie, Network Systems Specialist, Communications Network Services

Bruce Grimes, Senior Account Representative, Professional Communications

Phil Hale, Government Account Manager, Sprint Nextel

Diane Harding, Government Account Manager, Sprint Nextel

Henry Henderson, Owner, Professional Communications

John Homer, Systems Engineer, Systems Engineering and Administration; Network Infrastructure and Services

Wayne Howell, E-911 Communications Supervisor, Floyd County Sheriff's Office

Carol Hurley, Desktop Support, University Computing Support; Network Infrastructure and Services

Garry Jessup, Blacksburg Shop Manager, Two-Way Radio, Inc.

Matt Johnson, Captain, Virginia Tech Rescue Squad

Brian Jones, Network Engineering Manager, Communications Network Services

Steve Jones, Director of Technology, Town of Blacksburg

Ron Keller, Network Systems Specialist, Communications Network Services

Bruce Kemp, Computer Operations Technician Senior, Virginia Tech Operations Center; Network Infrastructure and Services

Sarah Kendall, Communications Officer, Montgomery County Sheriff's Office

John Krallman, Director of Information Technology Acquisitions, Office of the Information Technology Chief of Staff

Vickie Lambert, Sales Manager, Two-Way Radio, Inc.

Michael Lancaster, Smart Traffic Center Operations Manager, Virginia Department of Transportation

H. David Linkous, Director, Staff Development/Emergency Management, Montgomery Regional Hospital

Tom Lovejoy, Captain, Operations, Blacksburg Rescue

John Moore, Director, Educational Technologies, Virginia Tech

Jeff Newman, Project Manager, Two-Way Radio, Inc.

Tom O'Malley, Director-Network Engineering, Verizon Wireless

Dave Poff, Operations Manager, US Cellular

Mary Rachich, Customer Account Manager, Campus TeleVideo

Dave Ravas, RF Engineering Manager, AT&T Mobility

Dennis Reece, Internet Manager, Citizens Telephone Coop:

P.A. Sadowski, Major; Data Network Manager/Engineer, NC State Highway Patrol

Cory Schulfer, Applications Engineer, Extron Electronics

Mark Silvius, Graduate Research Assistant, Electrical and Computer Engineering, Virginia Tech

Keith Simmons, Senior Performance Engineer, Verizon Wireless

John (JD) Smith, Town of Blacksburg

Teresa Snavely, Operations Technician, Virginia Tech Operations Center; Network Infrastructure and Services

Kevin Sterne, Chief Engineer, WUVT 90.7 FM

Donald Stuart, Vice President, Two-Way Radio, Inc.

Danielle Thacker, Shift Lead, Virginia Tech Operations Center; Network Infrastructure and Services

Gene Thistle, Network Operations Technician, Virginia Tech Operations Center; Network Infrastructure and Services

Richard Todd, Senior Director, East Operations, US Cellular

Eddie Watson, Assistant Director, Educational Technologies, Virginia Tech

Anthony Wilson, Police Detective and Assistant Fire Chief, Blacksburg Police

Rob Young, Director-Network Engineering and Operations, AT&T Mobility

Appendix XIX: Glossary

10 GE	10 Gigabit per second Ethernet
511 Virginia	a statewide web, phone, and message board service that disseminates traffic, weather, and travel information throughout Virginia that is sponsored and managed by the Virginia Department of Transportation
711	The Federal Communications Commission adopted use of the 711 dialing code for access to Telecommunications Relay Services that permit persons with a hearing or speech disability to use the telephone system via a text telephone or other device to call persons with or without such disabilities
911	the emergency telephone number for the North American Numbering Plan
ADTRAN ATLAS	an integrated access device manufactured by ADTRAN that enables interconnecting and switching of telephone and ISDN lines/trunks, plus other functions
ALI	acronym for Automatic Location Identification, which is derived from a database generally maintained by the Incumbent Local Exchange Carrier (ILEC) under contract by a PSAP; each ILEC has their own standards for the formatting of the database; most ALI databases have a companion database known as the MSAG, Master Street Address Guide that describes the exact spelling of streets, street number ranges, and other address elements.
AM	Amplitude Modulation that is commonly used for radio broadcasting
ANI	acronym for Automatic Number Identification that is a system utilized by telephone companies to identify the directory number of a calling subscriber
ATLAS	Oracle database applications developed and used by Virginia Tech Communications Network Services
Banner	a collection of central administrative systems and data at Virginia Tech that encompass Alumni/Development, Human Resources, Finance, and Student and Financial Aid; Banner runs on the Oracle RDBMS; Banner is a product of SunGard--see www.sungardhe.com
BEV	the Blacksburg Electronic Village is an outreach project of Virginia Tech that serves the local community and others; BEV offers a wide variety of Internet-based services to Blacksburg area citizens, civic groups, and non-profit organizations--see www.bev.net
biometrics	the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits, such as from fingerprint, iris, face, and hand scans

Blackboard	a software learning system product used at Virginia Tech that is a mission-critical, enterprise-level application for instructors, researchers, and students. Over 75% of the university's undergraduate courses use the Blackboard learning management system.
BlueTooth	Bluetooth is an industrial specification for wireless personal area networks (PANs); it provides a way to connect and exchange information between devices such as mobile phones, laptops, PCs, printers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency
byte	abbreviation for binary term, a unit of storage capable of holding a single character of 8 binary digits
CAD	acronym used for Computer Aided Dispatch and for Computer Aided Design
CATV	originally "community antenna television," but is now more commonly known as "cable TV"
CD	a Compact Disk is an optical disc used to store digital data, originally developed for storing digital audio
central office	hub location for main telephone switch systems and for telephone wiring from subscribers
CLEC	Competitive Local Exchange Carrier
CNS	Virginia Tech Communications Network Services, a group within Network Infrastructure and Services
cognitive radio	a paradigm for wireless communication in which either a network or a wireless node changes its transmission or reception parameters to communicate efficiently without interfering with licensed or unlicensed users
COLA	a Web accessed application developed by Virginia Tech Communications Network Services that enables students to manage their telecommunications account, view statements, activate/deactivate services, and check balances
COLT	Cellular on Light Truck is a cellular, or mobile wireless base station on wheels
COW	Cellular on Wheels is a cellular, or mobile wireless base station on wheels.
Crestron Control	Crestron Electronics is a company that manufacturers high-end systems for home automation and conference room control; hardware developed by Crestron includes control processors, touch panels, keypads, lighting control systems, amplifiers, and audio servers; they manufacture remotes that connect to, and make use of their control systems in order to control other electronic and mechanical devices

cyber-security	security related to computer devices, data and communications
data warehouse	the main repository of an organization's historical data containing the raw content for management's decision support system
DBMS	Data Base Management Systems are computer and software systems that support storage of data and information
DHCP	Dynamic Host Configuration Protocol is used by networked computers to obtain temporary IP addresses and other configuration information from centralized DHCP servers
DID	Direct Inward Dial telephone trunks
dispatch center	a location where calls or issues are accepted and for which personnel may be contacted to respond
DNS	the Domain Name System (DNS) translates human-readable hostnames, such as www.vt.edu, to IP addresses the network uses for delivering the request or information; it also stores other information such as the list of mail exchange servers that accept email for a given domain
E911	Enhanced 911 or E911 service is a North American telephone network feature of the 911 emergency-calling system that automatically associates a physical address with the calling party's telephone number as required by the Wireless Communications and Public Safety Act of 1999; this is generally done by a form of reverse telephone directory that is supplied by the telephone company as a computer file, used to associate the caller's phone number with a physical street address that provides emergency responders with the location of the emergency without the person calling for help having to provide it
EAS	Emergency Alert System
ePortfolio	an online, personal information management system designed to give students, faculty, and staff the ability to create and distribute their educational records and other supporting documents
ERT	Emergency Response Team
Ethernet	a large, diverse family of frame-based computer networking technologies that operates at many speeds for local area networks
FAT	File Allocation Table is a partially patented file system developed by Microsoft for MS-DOS and was the primary file system for consumer versions of Microsoft Windows up to and including Windows Me
FAT32	a newer generation of FAT (File Allocation Table) with cluster counts held in a 32-bit field; typically used by computers running older Microsoft operating systems, including Windows 95/98/Me

filebox	a Virginia Tech service providing Internet-accessible file-storage space for documents, webpages, and similar items allowing university constituents to post information that is accessible to others
first responder	generally someone a from police, fire, or rescue organization
FM	Frequency Modulation
Frequency Bands used by police/fire/rescue	High HF (25-29.99 MHz); Low VHF (30-50 MHz); High VHF (150-174 MHz); Low UHF (450-470 MHz); UHF TV (470-512 MHz); 700 MHz (764-776 and 794-806 MHz); 800 MHz (806-869 MHz)
FTP	File Transfer Protocol used for intercomputer data transfers between clients and servers
Gbps	Gigabits per second, which is one billion bits per second
gigabyte	a unit of information or computer storage equal to 1000 bytes or 1024 bytes (1000 = one billion); when referring to RAM sizes and file sizes, it traditionally has a binary definition of 1024 bytes, and for every other use it means exactly 1000 bytes.
GIS	Geographic Information System
Hokie Passport	the official Identification Card for Virginia Polytechnic Institute and State University; it functions as a meal card as well as a building access key and bus pass.
Hokie SPA	a Web site portal for students, faculty, and staff that allows them to view academic, financial, and other pertinent information about their relationship with Virginia Tech
HPFS	the High Performance File System was created specifically for the IBM OS/2 operating system to improve upon the limitations of the FAT file system
IDE	Integrated Drive Electronics is a common term for the Advanced Technology Attachment (ATA) bus interface
IEEE 1394/Firewire	computer interface that supports up to 400 Mbps data transfers
ILEC	Incumbent Local Exchange Carrier
IM	acronym for instant messaging; a form of real-time communication between two or more people based on typed text conveyed via computers connected over a network such as the Internet
IP	Internet Protocol is a computer networking protocol used on the Internet
ISDN	Integrated Services Digital Network is a method of transmitting voice and data telephone call in a digital form, as opposed to analog
IT	Information Technology

Jabber	an open, secure, ad-free alternative to consumer instant messaging services like AIM, ICQ, MSN, and Yahoo; Jabber is a set of streaming XML protocols and technologies that enable any two entities on the Internet to exchange messages, presence, and other structured information in close to real time
kiosk	an electronic kiosk that houses a computer terminal that often employs custom kiosk software designed to function flawlessly while preventing users from accessing system functions
Knoppix	a Linux based computer operating system that boots and runs from a Compact Disk
LCD	a liquid crystal display is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector
legacy telephony systems	generally thought of as our past, or older generation, telephone systems that have been inherited
LISTSERV	an electronic mailing list software application
macro-cell	mobile wireless, or cellular, coverage areas are split up into cells to deal with line-of-sight signal loss and the number of active phones in an area; in cities, each cell site has a range of up to approximately ½ mile, while in rural areas, the range may be up to approximately 5 miles
MATP	Mid-Alantic Terascale Partnership is a consortium of research institutions in Virginia, Maryland, and Washington formed to to support research activities that require next-generation high-performance network connectivity
Mbps	digital data transmission speed in Megabits, or million bits, per second
modem pool	a bank of dial-up modems that support users dialing in with analog modems for computer and Internet data access
My VT	Web site, or portal, for accessing personal information associated with systems at Virginia Tech
NAS	Network Attached Storage
National LambdaRail	a nationwide high-speed communications network that is owned and controlled by the U.S. research community that moves data on light waves, or lambdas, over fiber-optic cable
NI&S	acronym for Virginia Tech Network Infrastructure and Services
NTFS	New Technology File System for computers running newer Microsoft operating system versions, including Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista

OpenVPN	an open source virtual private network (VPN) package for creating point-to-point encrypted tunnels between host computers
OSSI	in 2004 SunGard acquired Open Software Solutions Inc. (OSSI), then in June 2005, SunGard OSSI officially merged with SunGard HTE Inc., a wholly owned subsidiary of SunGard Data Systems, Inc; the Windows®-based OSSI product suite is a multi-jurisdictional system for police, sheriffs, fire, rescue, and EMS departments.
PBX	Private Branch Exchange, which is a private telephone system
PID	unique personal identification name, or user name, at Virginia Tech for accessing university computer and network systems
PSAP	acronym for Public Safety Answering Point, an agency in the United States, typically county or city controlled, responsible for answering 9-1-1 calls for emergency assistance from police, fire, and ambulance services
PSTN	Public Switched Telephone Network
RB14	Research Building XIV in the Corporate Research Park adjacent to the Virginia Tech campus in Blacksburg, VA
RSS	stands for "Really Simple Syndication," which is a family of web feed formats used to publish frequently updated content such as blog entries, news headlines or podcasts
Sakai/Scholar	a content management system called Scholar at Virginia Tech; Sakai is software that provides an online collaboration and learning environment; many users deploy it to support teaching and learning, ad hoc group collaboration, support for portfolios and research collaboration
SAN	Storage Area Network
SATA	Serial Advanced Technology Attachment interface for disk drives
SCSI	Small Computer System Interface is a set of standards for physically connecting and transferring data between computers and peripheral devices
servers	computers set up to provide services to user/client computer applications, such as for email and Web sites
SIRS	The State Interdepartmental Radio System (SIRS) is a low band frequency 39.54 MHz system developed in 1978 that is used statewide by local law enforcement to communicate between localities and the Virginia State Police
SMATV	Satellite Master Antenna Television system
SMS	Cellular, or mobile wireless, network Short Message Service

SSL	acronym for Secure Sockets Layer cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers
STARS	the Virginia Statewide Agencies Radio System (STARS) will be one of the first geographically statewide systems to employ digital trunked technology in the VHF 150 MHz band; it is an Integrated Voice and Data (IV&D) land mobile radio architecture, which uses the same mobile radio for both voice and law enforcement computer communications; STARS will include a Digital-Vehicular-Repeater-System (DVRS), which will translate the VHF signal used between the tower and vehicle, into a 700 MHz signal used for vehicle-to-portable communications; a single interface link will be provided to each of the counties and independent cities to bring interoperability at no cost to the jurisdiction, so that in a wide scale emergency, localities may be connected to each other in this manner, thus providing regional intercommunications
terabyte	a measurement term for data storage capacity defined as one trillion bytes
trunks	telephone lines between telephone switches
UCS	Virginia Tech's University Computing Support organization
UHF	Ultra high frequency; 300 MHz to 3 GHz
USB	Universal Serial Bus interface; USB 2 supports speeds up to 480 Mbps and USB 1.1 supports speeds up to 12 Mbps
VDOT	Virginia Department of Transportation
VHF	Very high frequency; 30 MHz to 300 MHz
voicemail	a system for recording voice telephone messages
VoIP	Voice over Internet Protocol
VORTEX	a broadband optical-fiber network that connects Virginia's universities to next-generation, high-performance networks
VPN	acronym for a virtual private network that is a communications channel tunneled through another network; one common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption; VPNs can be used to separate the traffic of different user communities over an underlying network with strong security features.
VT Alerts Automated Notification System	The VT Alerts Automated Notification System refers specifically to a set of contact methods to which students, faculty, and staff may subscribe

VTOC	Virginia Tech Operations Center that monitors and manages campus and other communications networks
VTPD	Virginia Tech Police Department
Wi-Fi	a wireless technology brand owned by the Wi-Fi Alliance intended to improve the interoperability of wireless local area network products based on the IEEE 802.11 standards
wireless hubs	wireless local area network access point device
WUVT	an FCC-licensed noncommercial radio station broadcasting at 3.5 kilowatts to Blacksburg, the Virginia Tech campus, and the surrounding areas

