ACUTA Audio Seminar

Emergency Notification at Virginia Tech

Information and Communications Infrastructure Issues

Tuesday, May 13, 2008

VirginiaTech
Invent the Future

Presenters

Mike Dame
Director of Web Communications
mdame@vt.edu

William Dougherty
Assistant Director Systems Support
william@vt.edu

Richard Hach
Associate Director Network Administration
rhach@vt.edu

Pat Rodgers
Director of Business Technologies
prodgers@vt.edu

VirginiaTech
Invent the Future

Seminar Topics

- Internal Review and Report
- Impact on Communications Infrastructure
- Web Communications
- Notification System
- Data Preservation and Collection
- Q & A

April 16 Internal Review: Information and Communications Infrastructure Group

4 Summary Findings

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:
- 4.1.2 Information Forensics
- 4.1.3 Routing of Cellular 911 Calls
- 4.1.4 Command and Call Centers
- 4.1.5 VT Alerts Emergency Notification System

4.2 Infrastructure Challenges (What Needs Work)

- 4.2.1 Cellular Phone Service
- 4.2.2 Public Switched Telephone Network
- 4.2.3 Emergency Responder Radio Communications

5 Tactical Recommendations

5.1 Data Communications Utilization and Performance
5.2 Web Communications Utilization and Performance
5.3 Systems Support Utilization and Performance
5.4 Radio Communications Systems Utilization and Performance
5.5 911 Systems Utilization and Performance
5.6 Cellular Service Utilization and Performance
5.7 Traditional Telephone Utilization and Performance
5.8 Video, Campus Cable Television, and Related Broadcast Systems Utilization and Performance
5.9 Information Technology Support Services
5.10 Data Preservation
5.11 Data Retrieval
5.12 Managing Personal Information
5.13 Response Centers
5.14 Cyber Security
5.15 VT Alerts Automated Notification System

Town of Blacksburg and Virginia Tech

- Blacksburg population about 41,000 people
- Between the Blue Ridge and Alleghany
- Virginia Tech about 26,000 students and 6,000 employees
- Internationally diverse, world-class research university
- Four distinct seasons, rural character
- Pedestrian oriented town
- "What a college is supposed to look like."

Communications Infrastructure Stress Factors

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

Network Performance

- PSTN generally engineered for the heaviest load offered to a network at a particular time of day/peak usage during a busy hour.
- Telecom networks whether wireless or wireline are designed to accommodate peak busy hours, not peak usage in the event of a disaster.
- Following the initial response, local provider networks became congested and blocked calls.
- 911 systems serving Virginia Tech, the Town and Counties enabled them to respond to students, faculty, staff and citizens and direct emergency service providers where they were needed.

Response by Private Carriers

- Cellular providers including AT&T, Sprint-Nextel, US Cellular and Verizon Wireless all dispatched technicians to add capacity to their networks.
- By April 17, Sprint-Nextel, US Cellular and Verizon Wireless each had “Cell on Light Truck” systems operating on campus
- Each provided emergency-use phones and accessories.

Infrastructure Facilities Duties

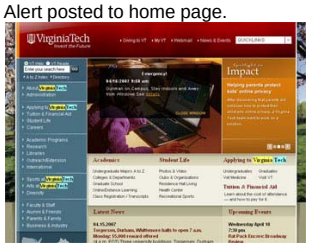
During the crisis, Virginia Tech IT faculty and staff were called upon to:

- Install telephone and data communications for
  - At least 9 geographically dispersed command centers
  - As well as media workrooms and counseling centers
- Perform network traffic balancing under unusual load
- Begin data collection and preservation activities
- Obtained location information
- Obtained class roster information

VirginiaTech Invent the Future

Web Communications How it started on 4/16

- **9:26 a.m.**
  Blast e-mail with subject line "Shooting on campus" sent, informing campus community of the shooting incident at West Ambler Johnston Hall (AJ).
- **9:31 a.m.**
  Alert posted to home page regarding the AJ shooting incident.
- **9:44 a.m.**
  Web staff overhears chatter on police scanner about gunshots at Norris Hall. Phone call placed to IT Webhosting alerting them to need for enhanced server support. I cancel our 10 a.m. WebComm staff meeting and call for shift to crisis mode.
- **9:58 a.m.**
  Alert posted to home page.



The alert reads "Emergency. Gunman on Campus, Stay Indoors and Away from Windows. See details."

VirginiaTech Invent the Future

Web Communications Goals for day of tragedy

- Communicate essential information
  - Home page all about brevity and clarity; click to inside page for more details
  - Navigation reduced to pertinent sections: About Virginia Tech, Administration, Campus Maps, Campus Buildings
- Expand server load balancing for VT.edu
- Establish communication workflows with Joint Information Center (JIC)

How it continued on 4/16

- **9:59 a.m.**
  Began preparing our "lite" home page to move to production.
- **10:03 a.m.**
  Began pulling Flash elements and graphics from home page.
- **10:17 a.m.**
  "Lite" home page launched with new alert: "All Classes Cancelled; Stay where you are."
- **10:33 a.m.**
  Shut down VT News database to reduce load; alert "details page" moved to VT.edu domain.
- **10:44 a.m.**
  IT Webhosting brings second server online to support VT.edu.
- **12:40 p.m.**
  Right after our first news conference, a podcast of Dr. Steger's statement is posted, along with notice of cancellation of all events. Note our "lite" home page layout.

- **2:33 p.m.**
  IT Webhosting brings third server online to support VT.edu.

Normal home page before 4/16

VirginiaTech Invent the Future

"Lite" home page on 4/16

VirginiaTech Invent the Future

"Details page" – 4/16 late afternoon

VirginiaTech Invent the Future

Late 4/16 / early 4/17 strategizing

- Connected with Larry Hincker regarding design and content ideas for VT.edu
- Held a WebComm team huddle early morning 4/17 to plan the next 24-48 hours
  - As much spirit rally as planning session
  - Checked in on personal and family situations
  - Mapped out new website architecture on whiteboard
  - Discussed hardware/software/server needs
  - Set deadline to launch new "In Memoriam" design for home page by 2 p.m. Convocation

VirginiaTech Invent the Future

Other things we decided

- Think multimedia; think Web 2.0
- Put students and families first in all decisions
- Choose words carefully to aid healing
- Find ways to engage the community
  - Create condolences/thoughts/prayers website
  - Post messages from other universities
  - Set up live video streaming for Convocation
  - Relocate webcam to stream Candlelight Vigil
- Suspend VT News daily e-mail

Home page around noon, 4/17

Home page around noon, 4/17

CONVOCATION TO BE STREAMED ONLINE; CLASSES CANCELED

Updated at 11:30 a.m., Tuesday, 04.17.2007

A live video stream of today's Convocation at 2 p.m. will be available at hokiesports.com.

During today's Convocation, the Merryman Center auditorium is being reserved for families of the victims who would like to attend the service in a private location.

Classes are canceled for the remainder of the week to allow students to mourn and begin healing. Campus will reopen Wednesday for administrative operations.

Norris Hall has been closed for the remainder of the semester.

The Virginia Tech Police Department has confirmed the identification of the gunman responsible for the multiple fatalities at Norris Hall on the Virginia Tech campus Monday. Ballistics match at both crime scenes.

The individual has been identified as Cho Seung-Hui, 23. Cho was enrolled as an undergraduate student in his senior year as an English major at Virginia Tech.

Get more details and continuous updates in our special section >

VirginiaTech *Invent the Future*

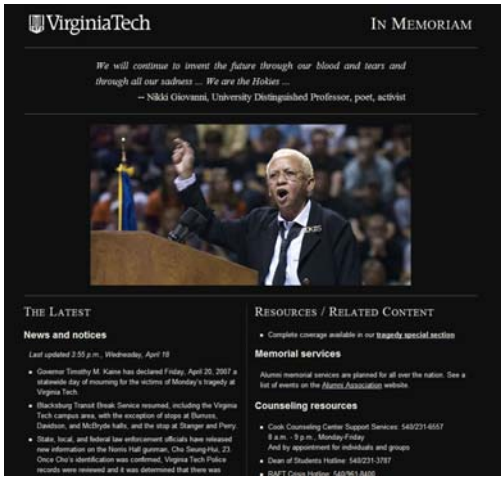
First version of "In Memoriam" design

VirginiaTech *Invent the Future*

Virtual participation in our grieving

VirginiaTech Invent the Future

Second version of "In Memoriam"



- Launched 4/18
- During Convocation, Dr. Nikki Giovanni provided exactly what we needed in a poem … words around which to build our messages to the world:

We Are the Hokies

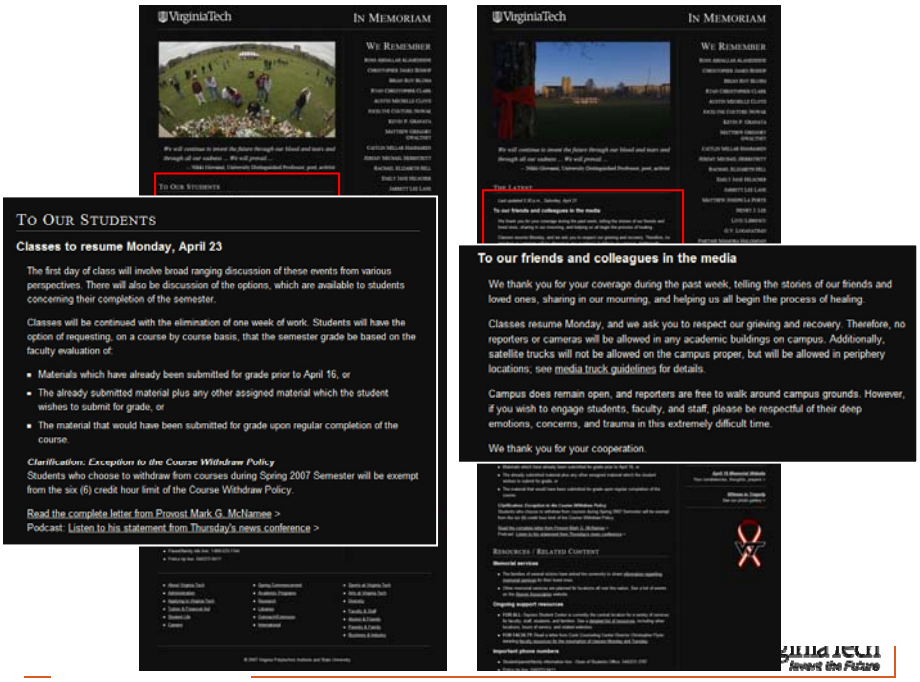
We Are Virginia Tech

We Will Prevail

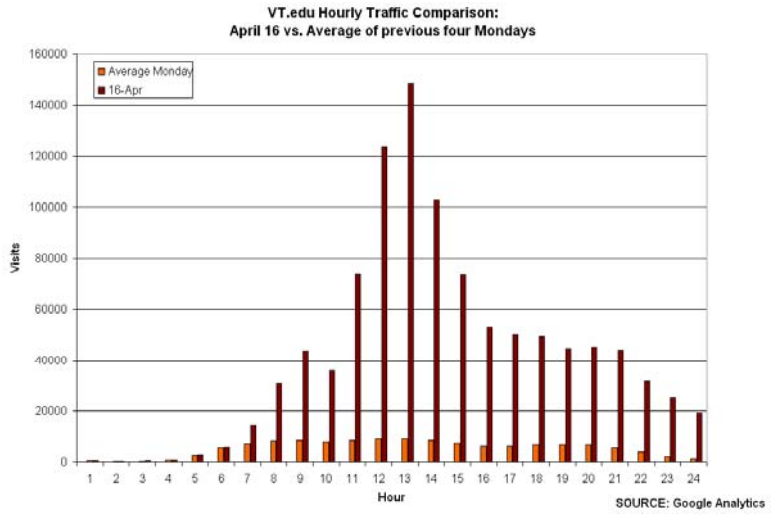
VirginiaTech Invent the Future

Third version of "In Memoriam"

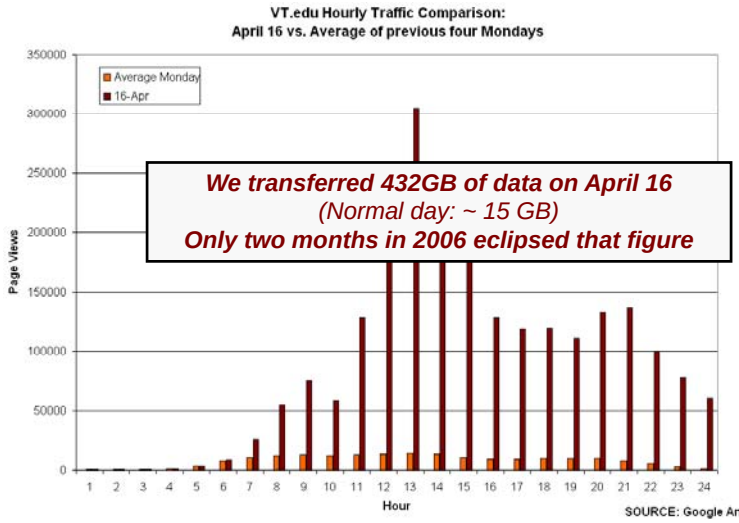
- The university began releasing names on 4/19, which we had to display prominently on the home page
- Very moving and poignant photos were coming in from our photo team



A humongous traffic spike …



… that tested our IT infrastructure



We transferred 432GB of data on April 16
(Normal day: ~ 15 GB)
Only two months in 2006 eclipsed that figure

Transitioning to "normalcy"

The situation:

- Classes set to resume Monday, April 23
- Tragedy still an open wound on campus
- Strong desire to begin recovery
- University needed to provide source of strength, leadership, resolve
- Determined not to let Virginia Tech be defined by this tragic event

Lessons learned (and reinforced)

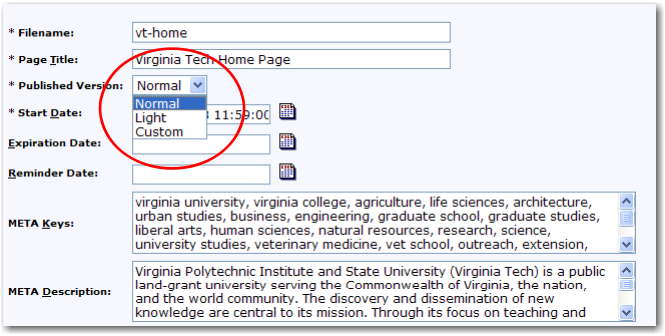
- Surround yourself with people who care
- Put students and their families first *always*, with faculty and staff right behind
- Provide multiple options for accessing news and information (text, audio, video, photos)
- Keep it simple; Don't overdo it; Let the facts and your audience tell the story
- If resources allow, place someone at your JIC

Get started at your institution

1. If you aren't joined at the hip with your IT team, schedule surgery now.
2. Define crisis communication scenarios and match each with available communication tools.
3. Develop a "lite" version of your home page.
4. Define roles and responsibilities in advance.
5. Conduct regularly scheduled "fire drills."
6. Ensure that politics can be left behind during crisis.
7. Plan for family matters – kids, pets, etc.
8. Surround yourself with cool, calm, collected "doers."
9. Expect to get very little sleep.
10. Don't forget about *you*.

"Custom" home page

Home page design "themes"



Notification System

A significant challenge during an emergency is providing mass notification of a threat and instructions for response.

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
- VT.edu (www.vt.edu) and the Virginia Tech News website
- University switchboard
- Public media (TV, radio, news websites)
- Siren system

No one method addresses all circumstances

VT Alerts

- A short list of vendors for this service was identified prior to 4/16/07
- Post-4/16 the vendor review process was expedited
- 3n was selected to provide hosted services for sending emergency messages
  - Through cellular phones
  - PDAs and other wireless devices
  - SMS/ text messaging
  - Email
  - Or to voice services

Notification System Policy Decisions

- Opt-In versus Opt-Out
- Source of data
- Liability
- Privacy
- Other university systems
- Uses of this information
- Conditions of Use
- Who can register

You Selected a System. You are Finished.

- Really?
- Policies and procedures
- The operational decisions
  - Who is responsible for sending messages?
  - Are they trained?
  - Who decides when to send a message?
  - Who decides on the message content?
  - How do you convey a message in 140 characters or less?
  - What instructions do you provide in the message?
  - Don't plan too much (defaults).
  - Testing

Notification System
You are Finished (cont.)

- Publicity
- Training Users
- Subscriptions
- Are more options better?
- Branding recognition
- How do you measure success?

Notification System
Future Considerations

- De-provisioning
- Dashboard
- First Responders
- The technology is not perfect.
- Users are not perfect.

Data Preservation and Collection

- **Cyberforensics:** a specialized form of e-discovery in which an investigation is carried out on the contents of the hard drive of a specific computer.
- **E-discovery:** refers to any process in which electronic data is sought, located, collected, secured, and ultimately searched with the intent of using it as evidence in a civil or criminal legal case.
- **ESI (Electronically Stored Information):** As data is requested during the discovery portion of a hearing or court case, ESI increasingly represents the bulk of what is requested, particularly in civil cases. With the recent (December 2006) update to the U.S. Federal Rules of Civil Procedure (FRCP), ESI received the same legal status as the more traditional "paper" files.
- **Metadata:** Generally defined as "data about data" or information within the electronic version of a document that travels with its file, but is usually not visible or otherwise apparent in printed format.

VirginiaTech Invent the Future

Data Preservation and Collection

- Timeline:
  - April 16th; meeting with central IT Support staff—Systems Support (System Administrators), Database Management Systems (DB Admins), Web Hosting (for both data preservation and load balancing of hosts to handle ever increasing traffic)
  - April 18th-27th; Direct Interaction with law enforcement (FBI, State Bureau of Investigation, local police, and VT PD)
  - April 23rd; First preservation memo issued by University Legal Counsel

VirginiaTech Invent the Future

Actual verbiage from "Hold Memo"

- In accordance with state and federal law, you are required to preserve any and all documents relating to the events, the suspect, and the victims regardless of whether the documents and information was created before or after event.
- In an abundance of caution, you should consider the phrase "documents and information" to be defined broadly. By way of illustration, not limitation, it includes all writings of any kind (handwritten, printed, electronic) including the originals, drafts, and all non-identical copies, regardless of their origin or location including, without limitation, correspondence, memoranda, notes, calendars, letters, minutes, contracts, reports, studies, statements, receipts, summaries, interoffice and intra-office communications, notes of any conversations or meetings, bulletins, computer printouts, facsimiles, drawings, sketches, worksheets, spreadsheets, photographs, and electronic recordings of any kind (including tapes, disks, hard drives, and thumb drives). Documents and information specifically include electronic data (including "metadata").

Actual verbiage from "Hold Memo"

- The following specific items referencing or regarding the event, the suspect and/or the victims must be preserved:
  - All electronic mail and information about e-mail (including message contents, header information and logs of e-mail system usage) sent or received; databases; activity logs; word processing files and file fragments; electronic calendar and scheduling program files or file fragments; spreadsheet files.
- To further minimize the risk of loss and/or destruction of relevant information:
  - All modification or deletion of any on-line electronic data files should cease; all activity that may result in the loss of any off-line data, such as the rotation, overwriting, or destruction of such media—including disk defragmentation or data compression—should cease.

Data Preservation and Collection

- Timeline (continued)
  - May 9th; First meeting with consultant
  - May 10th; First meeting with departmental I.T. representatives
  - June 7th; First image taken
  - Bulk of images (99%) completed late November 2007; last image taken January 8th, 2008; but there are "re-dos"
  - Now beginning process to restore and search data for e-discovery

Data Preservation and Collection

- Procedures:
  - Collection procedures could not be fully initiated until criminal investigation was concluded.
  - Members of ITSO, colleagues at Cornell, and consultants hired reviewed plans prior to implementation; collection procedures were developed and tested by GIAC certified engineers from VT.

Data Preservation and Collection

- Procedures (continued):
  - Meetings and interviews were conducted to determine who were likely data custodians, what type of data was relevant, what types of equipment were in use, and where the data was housed.

Data Preservation and Collection

- Procedures (continued):
  - E-mail & personal web site content was extracted for storage, and transmission to→
    - Law enforcement and families of victims
  - Initial imaging attempt used network for transfer direct to storage with encryption and compression; network speed presented an issue. (Hoped to avoid second step of copying data from USB drives to the NAS.)

Data Preservation and Collection

- Procedures (continued)
  - Moved to local USB drives using “dd” and “lzop.”
  - MD5 checksum performed on way out and while loading to NAS.
  - Some data types did not lend themselves to compression (audio and video files).
  - Once copied to the NAS, files were archived to tape backup and media removed to off-site facility.

Data Preservation and Collection

- Procedures (continued):
  - GPG Encryption (2K key size) used to store on NAS.
  - Keys passed to University Legal and stored in sealed envelope in records preservation vault.
    - A few laptops had encrypted data as well (BitLocker); keys for those were obtained and provided to University Legal as well.
  - Custodians signed and returned documents and survey forms.

Data Preservation and Collection

- Statistics:
  - 27 departments interviewed (including entire College of Engineering)
  - 150 individual custodians (over 200 total images)
  - 7TB stored for imaging
  - 10,000+ tapes set aside from backup systems; no rotation of tapes for 14 weeks; over 900TB stored
  - 5TB of log files stored

VirginiaTech Invent the Future

Data Preservation and Collection

- Statistics (continued):
  - Avg size of hard disk imaged= 80GB
    - Largest disk imaged= 500GB; smallest= 20GB
  - Avg image process duration= 1.75 hrs
    - Longest= 27.5 hours (250GB iMac);
    - Shortest= 20 minutes (40GB Dell D410)
  - Approx. 1600 person-hours spent on collection process so far, and counting.

VirginiaTech Invent the Future

Data Preservation and Collection

- Issues:
  - Privacy
  - Academic Freedom
  - Research Projects: Pros and Cons (Surveys, plus funded research).
  - Storage space, both online and in vault.
  - Scheduling; length of time required (MACs vs Intel products).

Data Preservation and Collection

- Issues (continued):
  - Equipment in homes.
  - Impact on operations, both staff that performed imaging and those who had to give up access to their computers during the process.
  - Assisting departments with resources such as additional tapes, desktops, servers.

Data Preservation and Collection

- Issues (continued):
  - Assuming control of resources purchased by/owned by other departments.
  - "Chain of evidence"; always 2 people on site; documenting various elements including—Owner of equipment (used PID); size of device; unique identifier for image file (especially when multiple hosts were in use by individual); time to image; cheksum value; type of machine (MAC vs. Intel; no LINUX based workstations in group).

Data Preservation and Collection

- Lessons Learned
  - Take time now to meet with your Security Officer and University Legal Counsel
  - Review your existing data retention policies; update or modify after consultation with ISTO and counsel
  - Document where your data is/are
  - Review existing privacy policies and regulations; Is a "Freedom of Information Act" part of your purview?

Data Preservation and Collection

- Lessons Learned (continued)
  - Consider funding “extra” storage and media for data preservation; potential for huge amounts is likely.
  - Open dialogues with peers; many have been through this already.
  - Provide training to key staff in IT.
  - Forewarn community of processes that will unfold if and when necessary. Make sure preservation memos make it to the right people.

Data Preservation and Collection

- Lessons Learned (continued):
  - Ensure space is available in secure, off-site location to store media and equipment. Usage of such space at VT grew by 350% over normal.
  - If you haven’t already purchased or investigated e-mail archiving products, you may wish to begin now.
  - Update or prepare your Standard Operating Procedures (SOP) document.
    - Include references to applicable policies and information about centrally provided services

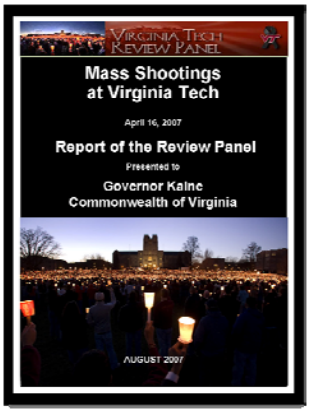
Resources

Governor's Review Panel final report

http://www.vtreviewpanel.org/report/index.html

Information and Communications Infrastructure Group report

http://www.vtnews.vt.edu/documents/2007-08-22_communications_infrastructure.pdf



Questions

Audio Seminar Sponsor

ACUTA would like to acknowledge the sponsorship of this audio seminar by Cisco Systems.

Contact:
Cisco Systems
Phone: (800) 553-NETS
Email: education@cisco.com
Web: http://www.cisco.com/offer/bizwisetv/campussafety/pdf

Cisco Systems

Cisco Campus Safety Solutions enable the convergence of the network and physical security to improve communication, collaboration and cooperation between safety systems, data systems and first responders.

Visit the Cisco Campus Safety Resource Center to see how your existing network can be used to significantly enhance safety and reduce costs.

http://www.cisco.com/offer/bizwisetv/campussafety/pdf

Evaluation Form

Please fax this evaluation to Michele West at ACUTA at 859.278.3268

Please rate the following:	Excellent	Very Good	Good	Fair	Poor
Speakers' presentations	5	4	3	2	1
ACUTA registration process	5	4	3	2	1
Cost of registration	5	4	3	2	1
Conference operator services	5	4	3	2	1
OVERALL RATING	5	4	3	2	1

Would you participate in another Audio Seminar?
___Yes ___No

What issues should we address in future sessions on this topic?

How could we improve the format of our audio seminars?

Thank you for participating today.

Please complete the evaluation form in your handout and fax it to ACUTA.