KSU Police Converged Security: A holistic approach to cyber safety and security

Cyber Security through Education & Awareness by Community Policing

Community Policing
- Initial meeting with parents and students at orientations
- Familiarization of crime prevention and crime statistics. Safe and Sound brochures
- Information about security cameras and emergency phone locations
- Importance of keeping serial/model numbers on all personal electronic equipment

Community Policing
- Social networking survey for security awareness and prevention on Police website
- Importance of reporting thefts as soon as possible to help deter future instances
- Timely Warnings issued campus wide through e-mail about ongoing potential threats or crimes on campus

Community Policing
- Provide information to students about harassing communications
- Which includes
  - Unwanted excessive text messages, phone calls and e-mails
  - How to obtain a Temporary Protective Order

Physical Protection & Prevention through Converged Security
By Office of Physical Security
The use of Physical Security

PHYSICAL SECURITY: Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Converged Security

KSU approaches Prevention through the use of Converged Security

What is Converged Security? The combination of cyber, physical, and human elements of security:
- Cyber-ITS
- Physical-Public Safety—largely by use of cyber based security items/tools/systems, also requirement of background for employees with access, etc.
- Human-physical patrols by police and security officers, investigations of crimes

Operations of Converged Security

KSU Police is charged with the physical security of cyber assets and systems.
The majority of our security mechanisms used are themselves, cyber-based items.

The use of Cyber Security

CYBER SECURITY: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.
- i.e. protect from theft, corruption, or natural disaster.

Tools used in Protection & Prevention:
- Cameras
- Alarms
- Access Controls
- Background Checks
- Patrolling
- Gate Access

Deterrence on Camera Locations:
- Life Safety
- High-dollar equipment and/or high-consequence areas
- Point of Sale
- Choke-points: entrances, exits, high-traffic areas

Cameras
Current Camera Options

Alarms
- Currently 33 Fire Alarms
- 23 Panic Alarms
- 22 Security Alarms
  - Increasing due to high-dollar equipment and/or high consequence areas, as well as KSU expansion to facilities off the main campus.

"None of our alarm systems, including fire, panic, security, are web based; however, we are moving in that direction.

Access Controls
- Building entrances
- Telco and Data Room
- Computer rooms
- Classrooms
- Mechanical rooms
- Storage, offices, suites, etc.

Background Checks
- Run on all KSU employees
- New policy addresses contractors access to restricted areas which is another physical security measure, aiding in the prevention of criminal activity

Patrolling

Gate Access
- Additional knowledge about who comes on campus and why
  - Use of other physical access controls such as visitors being managed on a restricted movement concept via the use of The Welcome Center Parking Area and other such "designated" areas

NetScan:
  - Web-based technology used to prevent the physical movement of undesirable personnel into the KSU environment and maintain separation between non-KSU personnel and the student body
  - Investigated tool providing logs from all gate locations (date, time, etc.)
Dual Functionality in Cyber Security: Investigations and Intelligence
By Criminal Investigation Unit

Cyber based Investigative Tools

- Investigations begin with initial research on persons or property identified as involved in the crime
- Research on both persons and property conducted via searches on web based applications
  - i.e. LexisNexis, social networking sites, media archives, GCIC/NCIC, Google, Craig's List, etc.

Cyber based Investigative Tools cont'd

- Use of campus web based tools:
  - Cameras
    - Analog and IP system cameras
    - Analog cameras will eventually be advanced to IP cameras
  - Access controls
    - Access logs from parking gates
    - Access logs on door locks

Investigating Cyber Crimes

- Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts.
- KSU's Information Security Office is heavily relied upon in these crimes to identify the who, what, when, where, why, and how when it is contained in cyber activity on campus. They are also used as forensic crime scene technicians and are certified forensic examiners of computer related equipment.

Investigating Cyber Crimes

- In this position, these 'technicians' and 'examiners' are used to seize equipment, make mirror images of hard drives for examination, maintain chain of custody and even provide testimony in court proceedings following criminal charges
- General challenges faced during investigation of cyber crimes:
  - Victims of computer-related crimes are sometimes unaware that a crime has been committed; therefore, a lengthy delay in reporting occurs.

Investigating Cyber Crimes

- Assigned investigators that have not been properly trained face challenges when dealing with computer-related crimes
  - i.e. cyber criminals are usually more technologically sophisticated and have more resources, more access to the newest technology, and more time to devote
- Due to continuous development of advanced technology and cyber capability, in order to remain aware of current trends in cyber criminal activity, Law Enforcement must constantly seek training in the following areas: the unique requirements of computer-related crimes; digital evidence; identifying, marking and storing this evidence; the capabilities of present private and state agencies to analyze this evidence; and the procedures for developing teams to conduct investigations of computer-related crimes.
Investigating Cyber Crimes

- Difficulties exist in determining jurisdiction when equipment being employed criminally is located in one community and the computer that is illegally entered electronically is in another state or even country.
- Another major challenge in investigating computer-related crimes include the need to determine the exact nature of the crime and to gather evidence in ways that do not disrupt an organization's operation.

Intelligence Gathering

- Through an investigation, intel about cyber security is obtained and then reported back to the appropriate areas for modifications, or further research of items. CIU is a major point of intel gathering for all cyber security on campus.
- CIU reports back to CPU when new cyber threats are discovered that may affect our student population; Therefore, new cyber safety tips can be added to information given at orientations, posted on department website, etc.

Intelligence Gathering

- Criminal Investigations Unit reports intel back to the Office of Physical Security when problematic items arise or there is potential for criminal activity. Physical security modifications or increases may prevent as well as, observed failures in current systems that are in place.
- CIU reports back to ISO when breach in cyber systems occur, or we learn the potential exists. We also report to them when a currently used cyber system doesn’t have what it needs to be able to ensure it is secure and will provide information of good evidentiary value in court. ISO performs vulnerability assessments on systems or potential weaknesses identified.

Cyber Security of Police Assets:
By Support Services Division

- Report Exec Direct (Records Management System)
  - Web-based. The data base is remotely hosted and data is secure and encrypted.
  - Each user is assigned a unique user name and password by the departmental system administrator. When employment with the department is terminated, the user is locked out of the system and no longer has access.

KSU Police Internal Cyber Security

- Release of Reports. Copies of reports are released to the general public in accordance with the Georgia Open Records Act and departmental policy.

KSU Police Internal Cyber Security

- [SCREENSHOT REDACTED FOR SECURITY]
Georgia Crime Information Center (GCIC)
- Provides criminal justice information on individuals, such as criminal histories, drivers license information, and vehicle registration.

Every member of the Department of Public Safety is required to sign a GCIC Awareness Statement. The Awareness Statement informs them that access to and dissemination of GCIC information is governed by state and federal laws and GCIC Council Rules. It also describes the criminal penalties if the information is used, except as permitted by law.

Every member of the Department of Public Safety is required to be trained in Security and Integrity of Criminal Justice information. The training must be received every three years.

All members of the Department of Public Safety who perform the duties of dispatcher must complete the Terminal Operator Training Program and be certified as Entry Level Operators within 3 months from their date of employment. They must be re-certified every two years.

Equature Audio Recording System
- Used to record emergency phone lines and police radio traffic

Web based. Database is hosted on site in a secure Telco room located in the Public Safety Building. Installation was overseen by the KSU Information Systems Security Officer to ensure security of the KSU network.

Access to recordings is strictly limited. Users are assigned a unique user name and password to gain access to the recordings. One member of the department is assigned administrator access and controls access to the database.

Copies of recordings are provided, upon request, as set forth in the Georgia Open Records Act and departmental policy.

Digital In-Car Video Recording System (DP2)
- Used to record audio and video of police activity from a police car.
Digital In-Car Video Recording System (DP2)

• Web based. The database is hosted on site in a secure Telco room located on campus. Installation was overseen by KSU ITS personnel to ensure network security.
• Access to recordings is strictly limited. Users are assigned a unique user name and password to gain access to the database. Only certain members of the department are assigned administrator access and control access to the database.
• Copies of recordings are provided, upon request, as set forth in the Georgia Open Records Act and departmental policy.

SGT. Bernadette Haynes, Community Policing; (770)423-6206, bhaynes@kennesaw.edu
Maureen Patton, Physical Security Coordinator; (770) 423-3053, mpatton@kennesaw.edu
SGT. Jennifer Elliott, Criminal Investigation; (678) 797-2043, jelliott@kennesaw.edu
LT. Maloney, Support Services; (770) 423-3035, kmaloney@kennesaw.edu