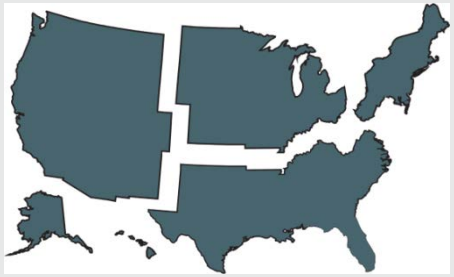
Entrepreneurs and Their Communities

Security and Organizational Risk Planning – Protecting Personal Information for Small Businesses

Brad Reed
Instructor of Computer Science, Glenville State College – West Virginia

March 8, 2012

Co-Sponsored by



RRDC
REGIONAL RURAL DEVELOPMENT CENTERS

extension
more mind reach

Housekeeping Details

- If you haven't already done so, enter your name/email address into the chat box
- Session will be recorded
- Feel free to type questions/comments at any time
- Evaluation - http://go.unl.edu/securityevaluation

extension
more mind reach

Glenville State College
Computer & Information Systems

Security and Organizational Risk Planning

Brad Reed, Computer Science Instructor

&

Rob Kerns, Infrastructure and Security

Glenville State College
Computer & Information Systems

Section I

COMPUTER SECURITY

Glenville State College
Computer & Information Systems

Physical Security

- Never leave unattended machines unlocked
- Never leave keys/cellphones unattended
- BIOS password
- Hard drive encryption
  - 48 NASA Laptops stolen in the last 2 years! (PC World)
  - Logon password and BIOS password does not protect raw data on hard drive.
  - Included in Windows 7 Ultimate and Enterprise
  - http://www.pcworld.com/article/226785/how_to_encrypt_a_hard_drive.html

Glenville State College
Computer & Information Systems

Internet/Network Security

- Don’t trust unsecured wireless.
  - WEP is very basic and easy to hack
  - WPA and WPA2 are the best
- Wired connectivity is always better and more reliable
- Network-Edge security device
  - Need a firewall and/or intrusion detection device between your network and internet connection

Glenville State College
Computer & Information Systems

Internet/Network Security

- Passwords
  - Password vs. Passphrase
  - Password length
    - Greater than or equal to 16 characters
- Security Questions
  - Don’t answer with single words or easy to find answers
  - Examples:
    - What street did you grow up on?
      - 983main (House number and street)
    - Favorite Pet?
      - Rover2003 (Pet name and year born or adopted)

GLENVILLE STATE COLLEGE
1872
Computer & Information Systems

Social Networking Security

- Don’t post anything you wouldn’t post on a bulletin board.
- Make sure no easily-accessed information on a social networking site connects to password or security question.
- Careful what information is in photos or wall posts
  - Clothes with town names
  - Stating that you are leaving town

Glenville State College
Computer & Information Systems

Email Security

- Never communicate sensitive information via email.
  - Anything you are uncomfortable with shouting at the top of your lungs in a crowd should not be communicated via email.
- Phishing
  - It's best not to click on links in an email message.
    - Open a browser and type the link directly
  - Snopes.com
- Viruses
  - Most common form of virus transmission

Glenville State College
Computer & Information Systems

Section II

SECURITY SOLUTIONS

Glenville State College
Computer & Information Systems

Domains

- What is a domain?
  - Multi-building campus with a security office in every building vs. a multi-building campus with a centralized security office
- When should you have one?
  - 10 or more employee users or workstations
  - Need for own email and scheduling system in house

Glenville State College
Computer & Information Systems

Devices

- Paid Solutions
  - SonicWALL
  - Cisco
  - Fortinet
- Open Source Solutions
  - IPCop
  - PF

Glenville State College
Computer & Information Systems

Threat Audits

- Asset Identification
- Threat Evaluation
- Vulnerability Appraisal
- Risk Assessment
- Risk Mitigation

Glenville State College
Computer & Information Systems

Threat Audits

- Asset identification
  - Process of inventorying items with economic value
- Common assets
  - People
  - Physical assets
  - Data
  - Hardware
  - Software

Glenville State College
Computer & Information Systems

Threat Audits

- Determine each item's relative value
  - Asset's criticality to organization's goals
  - How much revenue asset generates
  - How difficult to replace asset
  - Impact of asset unavailability to the organization
- Could rank using a number scale

Glenville State College
Computer & Information Systems

Threat Audits

- Threat evaluation
  - List potential threats
- Threat modeling
  - Goal: understand attackers and their methods
  - Often done by constructing scenarios
- Attack tree
  - Provides visual representation of potential attacks
  - Inverted tree structure

Glenville State College
Computer & Information Systems

Threat Audits

Category of threat	Example
Natural disasters	Fire, flood, or earthquake destroys data
Compromise of intellectual property	Software is pirated or copyright infringed
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Hardware failure or errors	Firewall blocks all network traffic
Human error	Employee drops laptop computer in parking lot
Sabotage or vandalism	Attacker implants worm that erases files
Software attacks	Virus, worm, or denial of service compromises hardware or software
Software failure or errors	Bug prevents program from properly loading
Technical obsolescence	Program does not function under new version of operating system
Theft	Desktop system is stolen from unlocked room
Utility interruption	Electrical power is cut off

Glenville State College
Computer & Information Systems

Threat Audits

- Vulnerability appraisal
  - Determine current weaknesses
    - Snapshot of current organization security
  - Every asset should be viewed in light of each threat
  - Catalog each vulnerability
- Risk assessment
  - Determine damage resulting from attack
  - Assess likelihood that vulnerability is a risk to organization

Threat Audits

Impact	Description	Example
No impact	This vulnerability would not affect the organization	The theft of a mouse attached to a desktop computer would not affect the operations of the organization
Small impact	Small impact vulnerabilities would produce limited periods of inconvenience and possibly result in changes to a procedure	A specific brand and type of hard disk drive that fails might require that spare drives be made available and that devices with those drives be periodically tested
Significant	A vulnerability that results in a loss of employee productivity due to downtime or causes a capital outlay to alleviate it could be considered significant	Malware that is injected into the network could be classified as a significant vulnerability
Major	Major vulnerabilities are those that have a considerable negative impact on revenue	The theft of the latest product research and development data through a backdoor could be considered a major vulnerability
Catastrophic	Vulnerabilities that are ranked as catastrophic are events that would cause the organization to cease functioning or be seriously crippled in its capacity to perform	A tornado that destroys an office building and all of the company's data could be a catastrophic vulnerability

Glenville State College
Computer & Information Systems

Threat Audits

- Estimate probability that vulnerability will actually occur
- Risk mitigation
  - Determine what to do about risks
  - Determine how much risk can be tolerated
- Options for dealing with risk
  - Diminish
  - Transfer (outsourcing, insurance)
  - Accept

Glenville State College
Computer & Information Systems

Section III

DISASTER RECOVERY

Glenville State College
Computer & Information Systems

Disaster Recovery

- This is part of your Threat Audit
- Have action plans ready for various scenarios
  - Disaster Recovery Template
    - Included with this presentation
- Once you develop your plans, test them periodically
  - Once a season or a minimal of annual testing
  - Run business operations from backup hardware for a day
  - If an offsite operations room is in planning, run operation from that site for a day
  - Restore data from tapes or backup devices periodically

Glenville State College
Computer & Information Systems

Section IV

LAWS AND REGULATIONS

Glenville State College
Computer & Information Systems

PCI Compliance

- Maintain a secure network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Glenville State College
Computer & Information Systems

SOX Compliance

- Contains provisions for:
  - Network and data security
  - Data access logs
  - Network access logs
  - Backing up data

Glenville State College
Computer & Information Systems

eDiscovery

- Provides laws for gathering and storing data for litigation purposes.
  - Data and electronic messages cannot be deleted when notified of pending litigation
  - Includes “raw data” on a network, email, voicemail, smartphones, PDAs and other messages or data owned by the organization
  - Data and documents need to be saved or archived in formats for investigators

Glenville State College
Computer & Information Systems

Section V

NOTEWORTHY TIDBITS

Glenville State College
Computer & Information Systems

Tidbits

- Security and DR will never be 100%
- Security through obscurity
- Common sense

Thank You!

- Mark your calendars for the upcoming webinars of this season – 2nd Thursday, 2:00pm (ET)
  - Apr/May/June 2012 will focus on Art and Business
  - **April 12, 2012**
- Evaluation - http://go.unl.edu/securityevaluation

extension
more mind reach