IT Orientation at Penn

Information Security

February 7, 2018

Joshua Beeman
University Information Security Officer
jbeeman@isc.upenn.edu
(215) 746-7077
www.upenn.edu/computing/security
security@isc.upenn.edu
Agenda

Intro to Penn Information Security
- Who we are
- What we do
- What we don’t do

What are “security incidents”?  
- Frequency and types
- Handling recommendations

Security policies
Poll #1

- How many people have had to support someone that had a machine that was infected at work?
- How many people have had a personal machine infected by a virus?
- How many people have ever received a letter from an organization letting them know that they had a data breach (so called “breach notification” or “disclosure letter”)?
Office of Information Security

Information Security’s core mission is to develop strategies and practices that protect Penn’s confidential and sensitive information assets.
Information Security - What Do We Do?

- Security Operations
- Consultations
- Risks & Threats
- Policy & Compliance
- Awareness & Outreach
- POC
- Identity & Access
- Reporting & Metrics
The Bottom Line

- Loss of reputation and/or resources
- Loss of intellectual property
- Privacy intrusions for constituents; loss of trust
- Non-compliance, can lead to penalties

Loss of control of Penn systems, networks or data
Some General Trends

- Mobility
- “Free” services
- Individual Behavior
- Compliance

All increase the need for security and privacy technical safeguards and education.

Our Goal: to support and enable Penn constituents embracing the positive aspects of these changes securely.
Poll #2

- What is the most common incident type at Penn?
  - Compromised credentials?
  - Compromised computers (OS or applications)?
  - DMCA take down notices?
  - Other?
Incident Trends - Takeaways

- Incident counts increasing
  - DMCA - An ongoing problem, mostly outside our control
  - Host Compromise - Better detection & response
  - Credentials - Tools and environment still evolving

- Reversing the trend
  - Faster notifications, timely disconnects
  - Blocking malicious traffic (campus firewall)
  - Limiting P2P?
Incident Trends cont’d…

- Increase in phishing and compromised credentials
- Increased need for assurances about vendor security
- Increased concern with security of web applications
Illegal Downloads

Entertainment industry monitors for infringing files continuously

Penn received more than 1,000 “takedown” notices last year

Material must be promptly removed

Student “repeat offenders” referred to Office of Student Conduct

Staff get disciplinary letter in their personnel file, counseling on policy

Serious cases have resulted in termination

Some students AND employees have also faced $3000 - $4000 fines or costly litigation
Most Common Problems We See

• Password issues (Users and Admins): weak, shared and/or openly displayed passwords
• Improperly secured and/or managed web applications
• Confidential data lost to "phishing" attacks
• Critical host not registered and/or not properly protected
• No program for scanning your own computers for weaknesses
• System patches and service packs not applied
• Reported security incidents are ignored
• Unneeded data left on machines
• Systems compromised by opening "infected" attachments, bad links, or vulnerable applications
Security Response

Active scanning program - we're scanning PennNet constantly

Sometimes we find hacked machines with sensitive data

When we do, please respond quickly

We will work with you to clean up and re-secure systems

At the end, we will give you a draft written report, and final version goes to senior management
Recommendations

LSPs: Identify your critical hosts, register them, and be fully compliant with the Computer Security policy.

Use strong passwords/passphrases, and *never* share them.

Apply security patches/service packs as soon as practical.

Use firewall devices and/or “personal firewall” software.

Use anti-virus software, and *keep it up to date*.

Mitigate risks specific to portable computers (e.g., use whole disk encryption, purchasing Computrace, etc.)
Policies

www.upenn.edu/computing/policy

- Copyright
- Acceptable Use Policy
- Disconnect Policy
- Computer Security Policy (new version incorporates the old Critical Host Policy)
- SSN Policy
- Incident Response Policy

Note: Open Expression & Electronic Privacy
What is a critical host?

Compromise could lead to legal liability or harm to Penn’s reputation.

Mission critical University-wide (e.g., BEN Financials, Payroll, pobox.upenn.edu)

Personally Identifiable Information (credit card numbers, salary, grades, patient data, Social Security Numbers, etc.)

University Proprietary Information (business plans, financial information, research data, trade secrets, others’ proprietary information)
Computer Security Policy Requirements

• Every computer user is responsible for securing and protecting the information technology resources and data over which he or she has control.

• Devices connected to PennNet including computers connected to PennNet via VPN but not RDP:
  – **Strong passwords**, encrypted in transit & storage
  – **Patched** as soon as reasonably practical
  – **Firewalls**: enabled if built-in, or mitigating controls
  – **Anti-virus**: installed with up-to-date signatures
Computer Security Policy Requirements (cont’d)

• **Portable computing and storage devices** that store confidential University data (including Penn- and personally-owned, on- and off-campus devices, and devices on 3rd party networks) have these additional requirements:
  – **Encryption** of Stored Data, with key recovery is required for:
    • Data that requires notification if compromised
      – SSNs, credit/debit/bank numbers
      – Data covered under HIPAA and HITECH Act
    • Particularly sensitive health information
      – Treatment, diagnosis, test results
      – Certain care setting
Computer Security Policy Requirements (cont’d)

• **Servers** that store confidential or operational data
  – **System administration**: full-time Penn IT staff or 3rd party with oversight by full-time Penn staff
    • Registered in Assignments
    • Properly trained
  – Confidential **data encrypted in transit** (certain protocols, no undue burden)
  – **Encryption of SSNs** in transit (per SSN policy)
  – Registered as **Critical Host**
  – **Physically secure** (locked area, limited access)
Computer Security Policy Requirements (cont’d)

• Servers that store confidential or operational data (cont’d)
  – Scanning
    • Info Security: quarterly scans
    • Admin: fix serious vulnerabilities in 2 business days
    • Admin: scan hosts behind firewall
  – Backup & recovery testing of operational data
  – Accounts disabled promptly
  – Secure data deletion of storage devices & media

• Email servers on PennNet
  – Virus protection plan
Incident Response Policy

- All security incidents must be reported to Information Security
- All compromises involving Confidential University Data:
  - Create a “PIRT” – Penn Incident Response Team
  - Manage incident response, possible forensics and disclosure questions
  - Create a Critical Incident Report
Be Alert for “Phishing” & Other Attacks

- Bogus email from PayPal/EBay about a completed auction.
- Bogus email from Amazon telling you about unpaid fees.
- Website telling you that the machine is infected and offering to provide software.
- Someone writes to tell you your face is all over YouTube, requiring you to install a video codec first.
- Bogus email telling you your email account is close to over quota.
- Promises of popular pictures or videos (“East Coast Earthquake!”,”Royal Wedding Dress!”,”Hurricane Irene!”)

See http://www.upenn.edu/computing/security/phish/ for more...

Trust us - No stranger will ever share $50 million with you!!
Phishing Example

From: IT helpdesk© <security@upenn.edu>
Date: Sun, Dec 9, 2012 at 9:54 AM
Subject: [UPENN] Important Update

To all our **PENN DOMAIN** Staffs,

Our records indicate that your account hasn't been updated as a part of our regular account University website maintenance for **staffs in Penn University**. Please fill in the form below to update your account now. If you do not verify your account now, **You** serve the risk of losing your account permanently. Thank you for your **usual** cooperation. We apologize for the inconvenience.

Sincerely,

IT Service Desk

University Staff Email Verification
*Full Name:* 
Department/Faculty:*:
Staff Pennkey/Username:
*Password:* 
*Confirm Password:* 
*E-Mail Address**:* 

*Note If the registration page does not appear on your email, switch to HTML or Click [Here](#) and the above requested info directly submit online.

"From" address is easy to forge

Strong warnings or threats, meant to instill a sense of urgency

Typos, inconsistent capitalization and strange phrases

A request in email for private data, including your password. Penn will never do this.

Hovering over the link will show what web page will open. Note that this is not a Penn URL.
Phishing Sample (cont’d)

Penn WebLogin

Enter your credentials to initiate a 10-hour Penn WebLogin session.

The session provides single sign-on access to many protected University web resources.

PennKey: [blank]
Password: [blank]

About Penn WebLogin
Log in
Three Things...

1. Two Factor

2. Endpoint Management (and patching)

3. Logging
Resources

- InfoSec website: www.upenn.edu/computing/security
- Email contact: security@isc.upenn.edu
- Top 10 Tips for Faculty, Staff & Students: http://www.upenn.edu/computing/security/checklists/Top10/
- IT Policy resources: http://www.upenn.edu/computing/policy/
  Includes “Electronic Privacy in Practice”
- Security Special Interest Group
  - e-mail listserv@lists.upenn.edu
  body of message: subscribe security-sig <Your Name>
- One Step Ahead - Almanac tips:
  http://www.upenn.edu/computing/security/footprints/index.php
  - Or via listserv: email to listserv@lists.upenn.edu
  - Message body: subscribe one-step-ahead <Your Name>