Indiana University of Pennsylvania

It's Not a Project!

IT Security as a Living Program

Bill Balint, Chief Information Officer
Paul Grieggs, Executive Director, IT Security
Indiana University of Pennsylvania

Indiana University of Pennsylvania

Session Goal

"To share how a data exposure outside of central IT's responsibility led to the creation of IUP's comprehensive IT security program. A specific goal is to review the components of the program in a manner that would allow other institutions to leverage, modify and enhance it for their own purposes."

Indiana University of Pennsylvania

Agenda

- About IUP
- The Crisis
- Objective 1: “Begin The Journey at Home”
- Objective 2: “Get The IT Policy House in Order”
- Objective 3: “Pass The Word”
- Objective 4: “Get Some Outside Help”
- Objective 5: “Make It Sustainable”
- What’s Next?

Indiana University of Pennsylvania

About IUP

- Main campus located in Indiana, PA
  - 60 miles northeast of Pittsburgh
  - Four small satellite locations in Western Pa.
- Doctoral, Research-Intensive University
- 12,000 students, 1,600 employees
- Member, Pa. State System of Higher Education
- Four public, non-profit affiliates

Indiana University of Pennsylvania

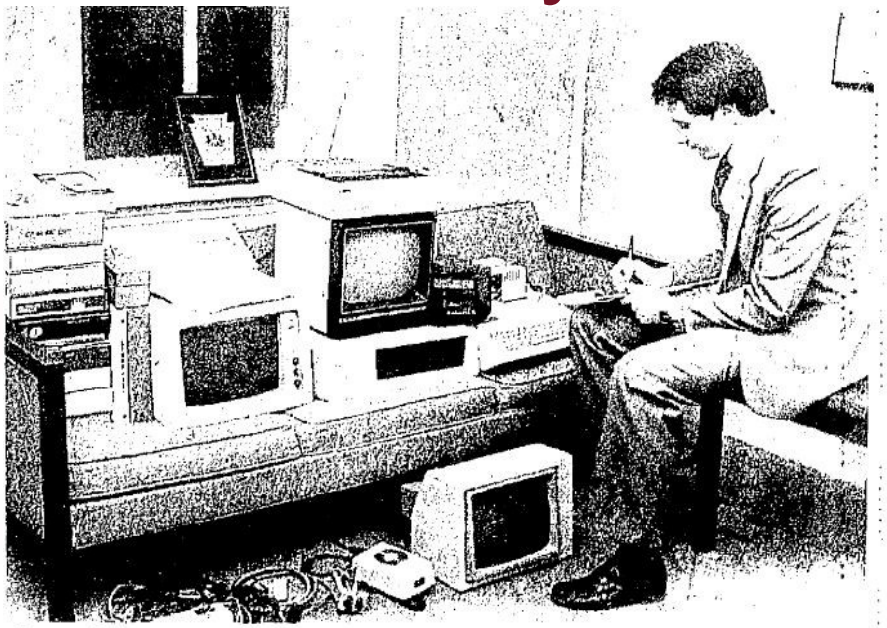
By The Numbers

- 17,000 active wired network jacks
- 1,800 wireless access points
- 21,000 active computing accounts
- 5,700-sq. foot Tier 2 data center
- 1PB raw storage
- 35,000 annual help desk requests
- 65 IT employees excluding temps & student workers

Indiana University of Pennsylvania

Initial Security Posture

1984 Incident



Gregory Davis, criminal investigator for the Indiana University of Pennsylvania Police, is shown preparing an inventory of items stolen from the university computer center since last October.
(Gazette photo by Bechtel)

Indiana University of Pennsylvania

Initial Security Posture

- Good practices in central systems/networks
  - ✓ Incident response procedures
  - ✓ Strong patch management on central systems
  - ✓ Internal technical controls
  - ✓ Secure account and initial password distribution

Indiana University of Pennsylvania

Initial Security Posture

- Provided distributed server and workstation management with security guidelines and templates, but no proactive enforcement
- Central IT handled incidents on non-central systems after they occurred (Account theft, copyright, resource theft, online vandalism)

Indiana University of Pennsylvania

The Crisis

- Decentralized web server user published sensitive data
  - Applicant SSNs, transcripts, addresses, etc.
  - Some were from applicants that had been rejected
- Created substantial investigation to identify exposure
  - Much of the data was on scanned images, requiring manual review of more than 1,000 images

Indiana University of Pennsylvania

The Crisis

- Significant legal and executive-level engagement
  - Letters to all impacted individuals, some of whom were difficult to find since some of the exposed information was dated
- President had been in place only six weeks
  - Tough explaining why Central IT was unable to address how decentralized web servers were configured, administered and the related data practices

Indiana University of Pennsylvania

The Crisis

- Security responsibility for ALL servers moved to Central IT
- Challenges were numerous and complex
  - No direct new budget or positions
  - Decentralized IT had existed for 20 years
  - Security (but not server ownership) was transferred to Central IT
  - Some systems administered by unionized, tenured faculty

The Crisis

- Challenges (cont.)
  - Dean of College ‘responsible’ was interim, tenured faculty member
  - Some deans and a number of faculty did not agree with decision to further empower Central IT
  - Central IT had its own ‘gaps’ in IT security
- General attitude: *“Why change everything due to the careless behavior of a single person?”*

Indiana University of Pennsylvania

Begin The Journey at Home

- Raised the priority of IT security in Central IT
  - New job descriptions and setting of expectations
  - Performance evaluations

- Increased percentage of Central IT expenditure
  - SANS Institute
  - Gartner
  - REN-ISAC, Internet2, Educause Security Professionals
  - Regional opportunities
    - Pa.-based group membership, training and conferences

Indiana University of Pennsylvania

Begin The Journey at Home

- Created the Pa. State System's first IT Security Office
  - Led by Executive Director of IT Security
    - Direct report to CIO
  - Policies, procedures, guidelines, best practices, etc.
  - Network administration
  - Security-related monitoring, alerts, resolutions, etc.
  - Legal/Right-to-Know engagements
  - Four FTE (all senior level) even though Central IT was losing permanent, full-time positions

Indiana University of Pennsylvania

Begin The Journey at Home

- Made tangential major investments
  - Significant upgrades and renovation to primary data center
  - Creation of new alternate data center
  - Border firewall
  - Network Monitoring

Indiana University of Pennsylvania

Get The IT Policy House in Order

- Avoided re-hashing of items embedded in laws and pre-existing policies
  - Examples: records retention, civility, codes of conduct
- Allowed procedures, guidelines and best practices to address anything where policy was not required
  - Policies must often be very broad and required Senate review and Presidential signature

Indiana University of Pennsylvania

Get The IT Policy House in Order

- Modified two IT-centric and one ‘affiliated’ policies
  - Acceptable Use of Information Technology Resources
  - Information Protection Policy
  - Email as an Official Means of Communication
- Eliminated all other IT-centric policies
- Kept policies very short and to the point
  - Used FAQs to help users understand

Indiana University of Pennsylvania

Get The IT Policy House in Order

- Built out procedures, guidelines and FAQs instead
  - Request for Enhanced Privilege Procedure
  - System Administrator Best Practices
  - Mobile Device Security Guidelines
- Easier to regulate, administer and modify over time
- Can create new as needs are identified

Technical Controls

- Sans/CIS Top 20
  - Standard desktop; no admin privileges
  - Network monitoring and visibility for inventory
  - Out of band network management
  - Border and internal firewalls
  - External audit and penetration testing

Indiana University of Pennsylvania

Pass The Word

- Bolstered IT security web presence
  - IT security mini-site
- Added safe computing practice expectations to new employee and student orientations
  - Freshmen courses, posters, welcome packets, residence hall materials

Indiana University of Pennsylvania

Indiana University of Pennsylvania

Pass The Word

- Leveraged ‘teachable’ moments
  - Users responding to phishing schemes
  - IT Security Office participation in student events
  - Work with business offices to include IT security in FERPA, GLB and other training
- Embraced an annual event to bring added attention
  - National Cyber Security Month/Alliance
  - Information Assurance/IT Security Day
  - IT security “tip of the week”, contests, etc.

Indiana University of Pennsylvania

Pass The Word

- Engage Faculty though our Teaching Excellence Center
  - Improve faculty awareness of threats and safe practices
  - Provide IT Security and privacy related material in formats that can be included in classes
  - Provide guest lectures by IT Security office personnel

Indiana University of Pennsylvania

Pass The Word

- Leveraged free resources
  - National Cyber Security Alliance
    - “Stay Safe Online”
  - Kinber/Educause/Internet2
  - Fellow institutions
  - Government Agencies focused on IT security
  - Trade Publications

Indiana University of Pennsylvania

Get Some Outside Help

- Worked to avoid spikes in third-party engagement, preferring to build consistency within ‘money, people and time’ constraints
- Engaged a third-party ‘simulated audit’ via consulting following data exposure
  - SANS 20 Critical Security Controls used as the standard

Indiana University of Pennsylvania

Get Some Outside Help

- Developed structure for paid third-party engagements
  - PCI
  - Penetration test
  - Incident Response
  - Identifying sensitive data
- REN-ISAC membership
- Educause HECVAT for Cloud Vendor Assessment
- SANS and CIS templates for baseline configurations

Indiana University of Pennsylvania

Make It Sustainable

- Increased third-party tool investment despite overall IT budget reductions
  - Data center
  - Backup/recovery
  - Border Firewall
  - IPS and internal firewalls
  - Compute/Storage for IT Security
  - Anti-virus, anti-malware, anti-spam, anti-spyware
  - Mobile device management
  - Sensitive data identification, data encryption

Indiana University of Pennsylvania

Make It Sustainable

- Largest concern is that emphasis on IT Security may wane over time and funding for making sustainable investments will fall into jeopardy
  - Will funds exist to:
    - continue expanding toolset?
    - continue maintenance on current tools?
    - fund continuous professional development?
  - Will time commitments be available as staff resources decline in other parts of the organization?

Indiana University of Pennsylvania

What's Next?

- Continue to enhance the security posture of IUP
  - PII scanning, password-to-passphrase initiative
  - Engage executives, such as Council of Trustees
  - When in doubt, go back to core principles and goals

- Make all investments in a sustainable manner
  - Big purchases do not help if we do not have the money or staff to leverage them for the long run

Indiana University of Pennsylvania

What's Next?

Most importantly:

"Educate the university community that IT Security never goes away and is therefore a program and not just a collection of projects!"

Indiana University of Pennsylvania

Q & A

Contact information:
Bill Balint
wsbalint@iup.edu

Paul Grieggs
pmgriegg@iup.edu

Indiana University of Pennsylvania

References

http://www.iup.edu/itsupportcenter/cyber-security/national-cyber-security-awareness-month-resources/

http://www.iup.edu/itsupportcenter/get-support/its-services/itsecurity/phishing-and-other-threats/

http://www.iup.edu/itsupportcenter/get-support/its-services/itsecurity/staying-safe-online/

http://libraryguides.lib.iup.edu/c.php?g=585558

Indiana University of Pennsylvania

References

http://libraryguides.lib.iup.edu/c.php?g=511835&p=3497585

http://www.iup.edu/itsupportcenter/about/policies/

http://www.iup.edu/itsupportcenter/about/policies/policies/it-acceptable-use-policy/

http://www.iup.edu/itsupportcenter/about/policies/policies/it-acceptable-use-policy-faq/