It's Not a Project:
Creating & Maintaining a Sustainable Cybersecurity Program

Bill Balint, Chief Information Officer

Indiana University of Pa. (IUP)

IUP

Session Goal

“To share how a data exposure outside of central IT’s responsibility led to the creation of a comprehensive cybersecurity program at a mid-sized public university.

A specific goal is to review the components of the program in a manner that would allow other entities to leverage, modify and enhance it for their own purposes.”

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?

About IUP

- Main campus located in Indiana, PA
  - 55 miles from University of Pittsburgh main campus
  - Four small satellite locations in Western Pa.
- Doctoral, High Research Activity Designation
- 9,250 students, 1,350 employees and affiliates
- Member, Pa. State System of Higher Education (PASSHE)
- Five 501(c)3 public, non-profit affiliates

By The Numbers

- 15,400 active wired network jacks
- 2,400 wireless access points
- 5,700-sq. foot Tier 2 primary data center
- Opened secondary data center in late 2010s
- 16,200 user accounts
- 45 IT employees excluding contractors & student workers
- 1.1 PB of raw storage

The Crisis – What Happened?

- User published sensitive data on non-IT web server
  - 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

The Crisis – Reaction

- 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

The Crisis – Resolution

- 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 - Resolution

- Challenges (cont.)
  - Dean of College ‘responsible’ was interim, tenured faculty member
  - Some deans and several 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?”*

Begin The Journey at Home - People

- Raised the priority of cybersecurity in Central IT
  - New job descriptions and setting of expectations
  - Performance evaluations
- Increased cybersecurity professional development for IT staff
  - SANS Institute
  - Gartner
  - REN-ISAC, Internet2, Educause Security Professionals,
  - Pittsburgh Technology Council/CyBurgh Initiative, C-CUE, KINBER

Begin The Journey at Home - Organization

- Created PASSHE's first IT Security Office
  - Led by Executive Director of IT Security
    - Direct report to CIO
    - Dedicated four senior-level FTE even though Central IT was losing positions
  - Policies, procedures, guidelines, best practices, etc.
  - Network administration
  - Security-related monitoring, alerts, resolutions, etc.
  - Legal/Right-to-Know engagements (now part of IT compliance)

Begin The Journey at Home - Investment

- Made tangential major investments
  - Significant upgrades and renovation to primary data center
  - Creation of alternate data center
  - Border firewall
  - Added network monitoring
  - Numerous softwares (such as sensitive data finder, Microsoft A5, etc.)
- Migrated from passwords to passphrases
- Toughened cybersecurity language in SaaS contracts

Get The IT Policy House in Order

- Avoided re-hashing items embedded in laws or existing policies
  - Examples: records retention, civility, codes of conduct
- Used procedures, guidelines and/or best practices to address anything where policy was not required
- IT serves only as SMEs for data governance
  - Example: Data Classification Policy

Get The IT Policy House in Order

- Modernized remaining two IT-centric and one ‘affiliated’ policies – primarily to address cybersecurity
  - Acceptable Use of Information Technology Resources (AUP)
  - Information Protection Policy
  - Email as an Official Means of Communication
- Eliminated other legacy IT-centric policies
- Kept policies very short and to the point

Get The IT Policy House in Order

- Focus procedures, guidelines, best practices and FAQs
  - Request for Enhanced Privilege Procedure
  - System Administrator Best Practices
  - Mobile Device Security Guidelines
  - Acceptable Use Policy FAQ
- Easier to regulate, administer and modify than policies
- Can add new elements as needs are identified

Pass The Word – Market/Educate

- Bolstered cybersecurity web presence
  - Cybersecurity mini-site
- Added safe computing practice expectations to new employee and student orientations
  - Freshmen courses, posters, welcome packets, residence hall materials
- Added mandatory annual cybersecurity awareness education program for all employees and affiliates in 2022

Pass The Word – Market/Educate

- Leveraged ‘teachable’ moments
  - Users responding to phishing schemes (including simulations)
  - Participation in student information literacy events
  - Asked business office to include cybersecurity - FERPA, GLBA training
- Embraced October as a focal point
  - National Cyber Security Month
  - Cybersecurity Day
  - Cybersecurity “tip of the week”, contests, etc.

Get Some Outside Help – No/Low Cost

- Leveraged free resources
  - National Cyber Security Alliance
    - “Stay Safe Online”
  - Educause, Internet2
  - CIS CSAT annual self-assessment
  - Colleagues in higher education
  - Government Agencies focused on IT security (NIST, FTC)
  - Industry websites and publications

Get Some Outside Help – No/Low Cost

- Reviewed Educause HECVAT for Cloud Vendor Assessment
- Used CIS critical controls for baseline hardware configurations
- Spent extensive planning time to exploit free resources
- Worked to avoid spikes in third-party engagement, preferring to factor in sustainability - ‘money, people and time’ constraints

Get Some Outside Help - Investments

- Conducted two third-party ‘simulated audits’
  - Center for Internet Security Critical Security Controls
  - NIST Framework
- Leverage other third-party engagements
  - As needed: PCI compliance and penetration tests
  - On-going: Incident Response Retainer contract
  - One time: Third party to study sensitive data identification techniques
- REN-ISAC membership

Make It Sustainable – 'Where to Spend?'

- Increased investment despite overall IT budget reductions
  - MFA
  - Cybersecurity awareness education platform
  - Backup/recovery
  - Border Firewall
  - Specific compute/storage for logs, forensics

Make It Sustainable – 'Where to Spend?'

- Additional Increased investments
  - Mobile device management
  - Sensitive data identification/data encryption
  - Incident response retainer
  - Endpoint device management
  - Anti-virus, anti-malware, anti-phishing, etc. tools; Microsoft A5

Make It Sustainable - ‘Forever’

- Largest concern is cybersecurity priority may wane over time and funding for making sustainable investments will falter
  - Will funds exist to:
    - continue expanding toolset?
    - continue maintenance on current tools?
    - fund on-going professional development?
  - Can IT security FTE be maintained as overall IT staffing shrinks
  - *“Big investments do not help if we do not have the money and/or staff to leverage them for the long run”*

What's Next?

- Continue to enhance the cybersecurity posture of IUP
  - Evolve the toolset, such as endpoint device management
  - Grow cybersecurity awareness education program
  - Continue to meet with executives or board semi-annually
  - Continue cloud move of confidential/sensitive data
  - Implement Identity and Access Management System
  - Grow use of Microsoft A5 capabilities
  - Comply annually with CIS Controls risk mitigation
  - Mature internal IT Security/IT Compliance partnership

What's Next?

Most importantly:

"Constantly remind the university community that cybersecurity needs never go away and are therefore components of a permanent program and not just a collection of projects!"

Q&A

Contact information:

Bill Balint

wsbalint@iup.edu