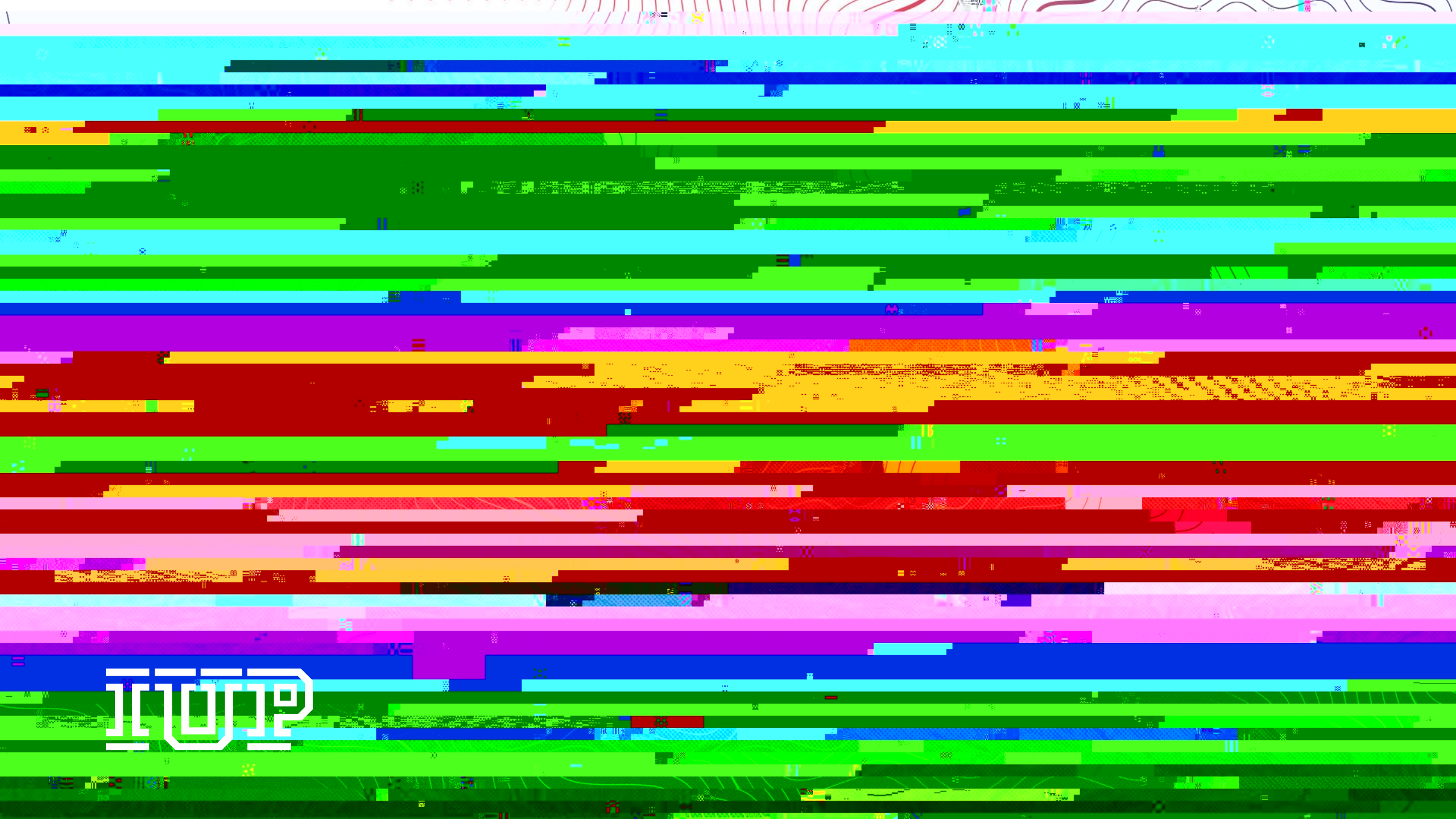

responsibility led to the creation of a comprehensive cybersecurity program at a mid-sized public university.

A specific goal is to review the components of the program in a manner that would allow other entities to leverage, modify and

- 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?

- ÅMain campus located in Indiana, PA
  - Å55 miles from University of Pittsburgh main campus
  - ÅFour small satellite locations in Western Pa.
- ÅDoctoral, High Research Activity Designation
- Å9,250 students, 1,350 employees and affiliates
- ÅMember, Pa. State System of Higher Education (PASSHE)
- ÅFive 501(c)3 public, non-profit affiliates

Å15,400 active wired network jacks

Å2,400 wireless access points

Å5,700-sq. foot Tier 2 primary data center

ÅOpened secondary data center in late 2010s

Å16,200 user accounts

Å45 IT employees excluding contractors & student workers

Å1.1 PB of raw storage

- 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

- 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

ÅSecurity responsibility for ALL servers moved to Central IT

ÅChallenges were numerous and complex

- Challenges (cont.)
  - Dean of College ôresponsibleõ 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 ôgapsõ in IT security
- General attitude:

- 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

- Created PASSHEÕs 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-

- 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

- 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

- 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

- 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

- Leveraged ñteachableô 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 ñtip of the weekò, contests, etc.

- 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

- 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

- Conducted two third-party ósimulated auditsô
  - 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

- 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

Å

Most importantly:

needs never go away and are therefore components of a permanent

Contact information:

Bill Balint

wsbalint@iup.edu