EAB

IT Forum

Virtual Executive Roundtable

Developing a Security-First Culture: How to Engage Boards, Cabinets, and End-Users to Combat Escalating Threats

We will start promptly at 1:03 PM EST once everyone has joined

Ransomware Brings Department to Standstill

Michigan State University Loses Research and Student Data in Cyberattack

Key Events of the Michigan State University (MSU) Ransomware Attack

Hacker Infiltrates Academic Department

Ransomware attack hits MSU's Physics and Astronomy (PA) department in May 2020.

Double Extortion

Attackers encrypt 700 GB and exfiltrate 8 GB of data, including PII[1] affecting over 9,000 students. One researcher loses a year's worth of research.

Ransom Demands Unmet

MSU leadership decides not to pay $6 million ransom even when hackers publish stolen PII on the Internet.

Systems Recovery Delayed

PA systems remain offline for majority of summer. Estimated 50 to 70 percent of research halted and some research could not start up again for six months.

Remediation Costs Pile Up

Total remediation cost estimated at **$1,093,000**, including IT response and recovery time, lost PA staff and research time, legal bills, notification of identity theft risk, etc.

Origin of the Attack: Unpatched VPN[2] Server

Hacker, allegedly affiliated with the NetWalker criminal organization, entered MSU's PA network through a test VPN server that had been running for a couple of weeks without being patched.

[1] Personally Identifiable Information

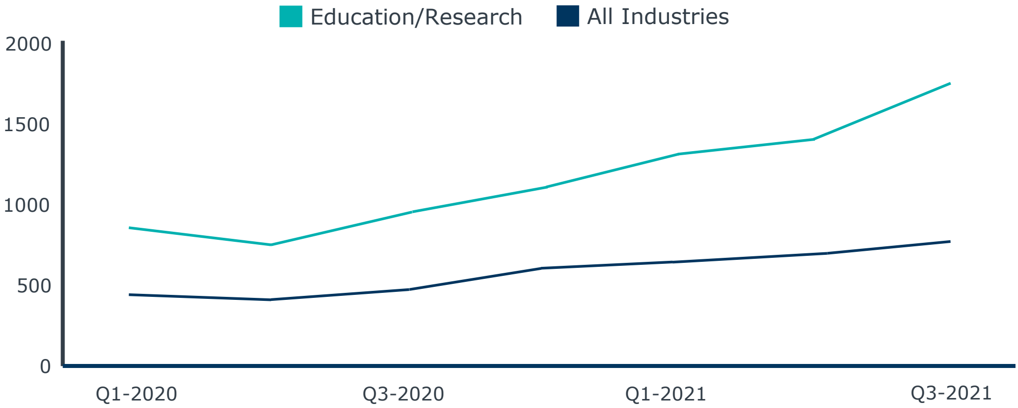
[2] Virtual Private Network

Source: A. Adams, T. Siu, J. Songer, and V. Welch, "Research at Risk: Ransomware attack on Physics and Astronomy Case Study", *NSF Cybersecurity Center of Excellence, Trusted CI*, June 2021; EAB interviews and analysis.

Higher Ed a Particularly Appealing Target

No Industry Has Been Spared—but Ours Bears the Brunt

Weekly Average Attacks per Organization Globally



Education: the New Hotspot for Cyberattacks

3,936%

increase in security incidents in education from 2013 to 2020

1,605

average attacks per week on education/research organizations in 2021

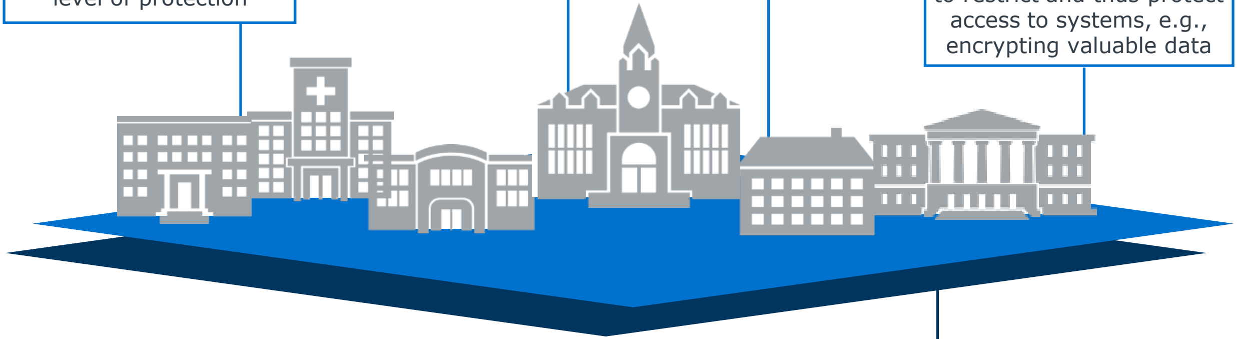
44%

of educational institutions in a survey of 499 IT leaders were hit by ransomware in 2020

Source: Check Point Research, "Cyber Attacks Increased 50% Year over Year," *Check Point*, August 8, 2021; Check Point Research, "Education sector sees 29% increase in attacks against organizations globally," *Check Point*, August 8, 2021; Sophos, "The State of Ransomware in 2021", *Sophos*, July 2021; Verizon, "2014 Data Breach Investigations Report", *Verizon*, 2014; Verizon, "2021 Data Breach Investigations Report", *Verizon*, 2021; EAB interviews and analysis.

My, What Big Data You Have

Many Factors Make Higher Ed a Valuable (and Vulnerable) Target



High Volume of Valuable Data
Personal, financial, and medical information on par with banks, hospitals, etc. – without the same level of protection

Research & Intellectual Property
Research (especially government or industry-sponsored) is a profitable target for hackers

Digital Sprawl
Sprawl and lack of adherence to basic security measures, e.g., vendor security assessments

Open Academic Environment
Culture of academic freedom means reluctance to restrict and thus protect access to systems, e.g., encrypting valuable data

Resource Scarcity
Unable to compete in labor market or dedicate resources to posture at level comparable to similar private organizations

Pandemic Exacerbated Historical Weaknesses !

- Increased network and system architecture complexity
- Increased number of unprotected devices accessing environment
- Increased vendor purchases and products

Source: EAB interviews and analysis.

Cyberattacks Cost So Much More Than a Ransom

Atlanta Shells Out $17M for a $52K Ransom (Which They Didn't Pay)

Approximate Costs

Restoring the city's computer networks	*$2.7 million*
New devices (e.g., laptops, smart phones)	*$1.1 million*
Immediate post-incident consulting services with eight different firms	*$1.5 million*
Legal fees:	
Law firm	*$485 per hour*
Law associates	*$300 per hour*
Upgrading security and software services	*$6 million*

Average Total Cost of a Single Data Breach in Education in 2020

$3.9M

Insurance Premiums Are Rising, Even Without Attack History

300%

Reported increase in insurance premiums and deductibles, with sub-limits on certain types of events like ransomware and co-insurance requirements, according to Katherine Mayer, AVP of information security at the University of Wisconsin

Source: IBM Security, "Cost of a Date Breach Report 2021", *IBM*, July 2021; J Jorstad, "Higher-Ed Cybersecurity Insurance: Are You in Good Hands?", *GovTech*, November 19,2021; S Deere, "Cost of City of Atlanta's cyber attack: $2.7 million — and rising," *The Atlanta Journal-Constititution*, October 1, 2019; EAB interviews and analysis.

Quick Poll 1

How does your institution plan to address imminent increases in cyber insurance rates? (select all that apply)

a. We will pay increased premiums
b. We are considering self-insurance
c. We will not be utilizing cyber insurance in the future
d. Other (please type in chat)

Impact Across the Board

How Cyberattacks Put Strategic Priorities and Transformation Agenda at Risk

Business Operations

Brown University had to **ask faculty and staff to temporarily stop using Microsoft Windows-based machines** and was forced to shut down its central data center and supporting systems after a cyberattack.

Student Success

A ransomware attack forced Howard University to **cancel online and hybrid classes** for two days.

Student Health & Safety

Richmond Community Schools **extended its break** because ransomware had infiltrated systems through and shut down its **heating and cooling system.**

Enrollment

Students at Long Beach City College were **unable to enroll for classes for nearly a month** after a malware attack infiltrated multiple computer systems.

Research

A top researcher at a public research university **was unable to execute a research grant** with the state to conduct COVID-19 research because its cyber defenses did not meet state-defined security standards.

Reputation

Simon Fraser University was in the **news two years running** after experiencing large-scale attacks which compromised staff and student data in consecutive years.

Source: B Foresman, "Ransomware used HVAC to infect Michigan K-12 district", *EdScoop*, Jan 2, 2020; L Borg, "Brown University Recovering from Cyber Attack", *GovTech*, April 12, 2021; M Ngo, "Howard University Hit by a Ransomware Attack", *The New York Times*, September 7, 2021; S Rivera, "Security Firm Investigating Malware Attack at Long Beach City College", *Long Beach Post*, May 8, 2018; T Stankard, "Colleges Continue to Withstand Cyberattacks in 2021", *TitanHQ*, April 13, 2021; EAB interviews and analysis.

A Shift in the Tide

> “A recent attack on a neighboring institution scared our board and senior leadership into action. We suddenly got a blank cheque to upgrade our security posture.”
>
> — Chief Information Officer
> *Private Research University*

Roadmap for Today’s Discussion

PART 1: DEVELOPING A SECURITY-FIRST CAMPUS CULTURE

I. Building Leadership Commitment to Enterprise-Wide Security

Tactic 1: Proactive Risk-Rated Escalation Paths

Tactic 2: Executive-Level Tabletop Exercises

Tactic 3: Cyber Enforcement Mandate from the Board

Tactic 4: Monthly Risk-Based System Quarantines

II. Improving End-User Engagement in Security

Tactic 5: Components of Effective Training

- Gamified Security Platform
- Department-Tailored Training
- Mandatory Training with Penalties for Non-Compliance
- Monthly Self-Phishing

PART 2: ENHANCING IT’S CYBER RISK MANAGEMENT CAPABILITIES

Pinpointing High-Value Security Investments and Staffing Solutions in Higher Ed

- Flagship, High Research - February 24th, 1:00 PM to 2:30 PM EST
- Large Public or Private - March 2nd, 10:00 AM to 11:30 AM EST
- Small or Private - March 9th, 5:00 PM – 6:30 PM EST

EAB

Building Leadership Commitment to Enterprise-Wide Security

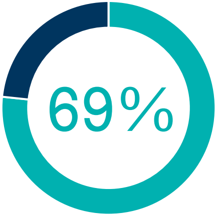
SECTION 1

- Tactic 1: Proactive Risk-Rated Escalation Paths
- Tactic 2: Executive-Level Tabletop Exercises
- Tactic 3: Cyber Enforcement Mandate from the Board
- Tactic 4: Monthly Risk-Based System Quarantines

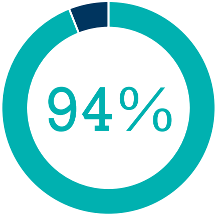
IT Cannot Protect Everyone On Their Own

Difficult for IT to Keep Up with Threats without Organizational Support

CISOs Across Industries Express Anxiety about Security Posture…



of cybersecurity professionals rate their team's **security readiness average** or **below average**



of cybersecurity professionals are **moderately to extremely concerned about** their **cloud security**

…And Those Anxieties Flow Upwards

> "Cybersecurity risk is a top-of-mind issue in our leadership discussions; our Board is regularly asking for reports on cybersecurity."
>
> Peter Han, Chief of Staff to the President
> *Colorado School of Mines*

Source: "2020 Cloud Security Report (ICS)[2]", *Cybersecurity Insiders*, 2020; Colorado School of Mines, Golden, CO; EAB interviews and analysis.

Risks Are Shared, So Must the Responsibilities

Challenges That Undermine Enterprise-Wide Security

Security Risks Are Not Appropriately Elevated to or Assessed by Leadership

"We lack a systematic way of involving non-IT leaders in assessing, accepting, or mitigating risks for the institution.

Leadership Lack Decision-Making Preparedness to Respond to Incidents

"If we get attacked, our executives will be facing these decisions for the first time and I worry that we will lose critical time and make suboptimal decisions."

Distributed Stakeholders Flout Information Security Policies

"We do not have the political clout within IT to enforce penalties for noncompliance."

Key Imperative

Apprise Leadership of High-Priority Risks to Determine Response Options

- Tactic 1: Proactive Risk-Rated Escalation Paths

Practice Decision Making Pathways for Responding to Security Events

- Tactic 2: Executive-Level Tabletop Exercises

Empower IT to Enforce Security Standards Across Campus

- Tactic 3: Cyber Enforcement Mandate from the Board
- Tactic 4: Monthly Risk-Based System Quarantines

Source: EAB interviews and analysis.

Vanderbilt's Risk Register

Translates Cyber Risks into Business Risks and Outlines Treatment Plan

Vanderbilt University Risk Register Template Ensures Response Accountability

ID	Category 1	Risk	Caused by	Result/ Impact
#	**Business risk category that the risk applies to**	Short statement that describes the risk	The trigger that causes the risk to occur	The effect the risk could have

Likelihood	2 Impact Rating	Risk Exposure 3	Change and Review Date
Scale of 1-5	**Scale of 1-5**	• **Minor** • **Moderate** • **Major** • **Extreme** • **Very Extreme**	Type of change and date of last review

Control	Risk Response Options 4	Estimated Risk Response Cost	Workplan 5
Existing information on security controls	• **Accept** • **Mitigate** • **Transfer** • **Avoid**	Expected costs or specific resourcing requirements	**Ownership and timeline for risk response or if included in Work Plans**

Source: Vanderbilt University, Nashville, TN. EAB interviews and analysis.

Establish Evaluation Criteria for Risk Framework

Vanderbilt Assigns Risks Based on Discrete Impact and Likelihood Scores

Six Categories of Risk

- Financial
- Operational
- Legal & Regulatory
- University Mission
- Reputational
- Health & Safety

Financial Risk Impact Rating Definitions

Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
$	$$	$$$	$$$$	$$$$$

Source: Vanderbilt University, Nashville, TN. EAB interviews and analysis.

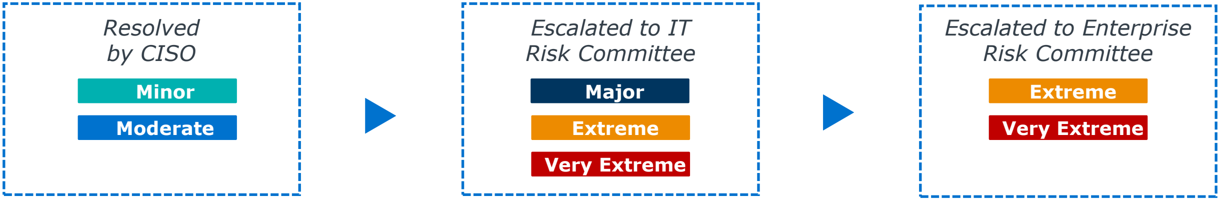
Triage Risks for Leadership Assessment

Vanderbilt Establishes Escalation Criteria Based on Risk Exposure Rating

Risk Exposure Rating Matrix

Likelihood/ Impact Rating	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	Minor	Moderate	Major	Extreme	Very Extreme
Likely (4)	Minor	Moderate	Major	Extreme	Very Extreme
Possible (3)	Minor	Moderate	Major	Major	Extreme
Unlikely (2)	Minor	Moderate	Moderate	Moderate	Major
Rare (1)	Minor	Minor	Minor	Moderate	Moderate

Risk Escalation Criteria



Resolved by CISO

Minor

Moderate

Escalated to IT Risk Committee

Major

Extreme

Very Extreme

Escalated to Enterprise Risk Committee

Extreme

Very Extreme

Source: Vanderbilt University, Nashville, TN. EAB interviews and analysis.

Quick Poll 2

Do you regularly escalate cyber risks to non-IT executives? (select all that apply)

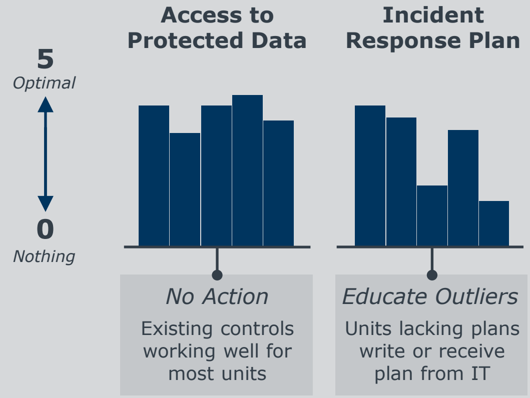
a. We escalate major risks to the cabinet whenever we find them
b. We escalate risks every quarter
c. We escalate risks every month
d. We don't escalate risks to non-IT executives

Peer Pressure Bolsters Risk Improvement Campaign

Unit Risk Scorecards and Heat Map Drive University-Wide Risk Improvements

Information Security Scorecard for Board[2]

(illustrative)



No Action

Existing controls working well for most units

Educate Outliers

Units lacking plans write or receive plan from IT

"3 And Green" Campaign

2014: Board is apprised of goal to **get all units above 3.0** by 2017 in **self-attested campus security survey** quantifying unit risk

2017: **Average unit score surpasses 3.0** as a result of **departments and IT targeting improvements based on survey scores** (e.g., asset tracking, response plans, vendor screening)

2022: IT launches **controls validation dashboard** which lets units compare metrics for key controls aligned with NIST SP 800-53[1] and automatically resolve certain vulnerabilities

[1] National Institute of Standards and Technology Special Publication 800-53

[2] EAB's IT Forum Elevating Security Awareness

Source: The Ohio State University, Columbus, OH; EAB interviews and analysis.

Translating Risks Up the Escalation Ladder

Elevated Talking Points for a Vulnerable Server

Messages about Cyber Risks Adapted Using Mission-Oriented, Non-Technical Language as They Are Delivered Up the Hierarchy

VANDERBILT UNIVERSITY

Technical Explanation

A pre-patent server vulnerable to attack requires frequent patching. If it becomes compromised, we need to intervene immediately.

Relevant Stakeholder Messaging

This server holds all of Vanderbilt's pre-patent information. If it's down, we can't access that information. Our ability to provide this service to our researchers is degraded.

Senior Leader Messaging

If we don't protect this server and it is hit by ransomware, our pre-patent intellectual property data that we could have patented and commercialized could be stolen. This would have a direct material impact on the university.

Source: Vanderbilt University, Nashville, TN. EAB interviews and analysis.

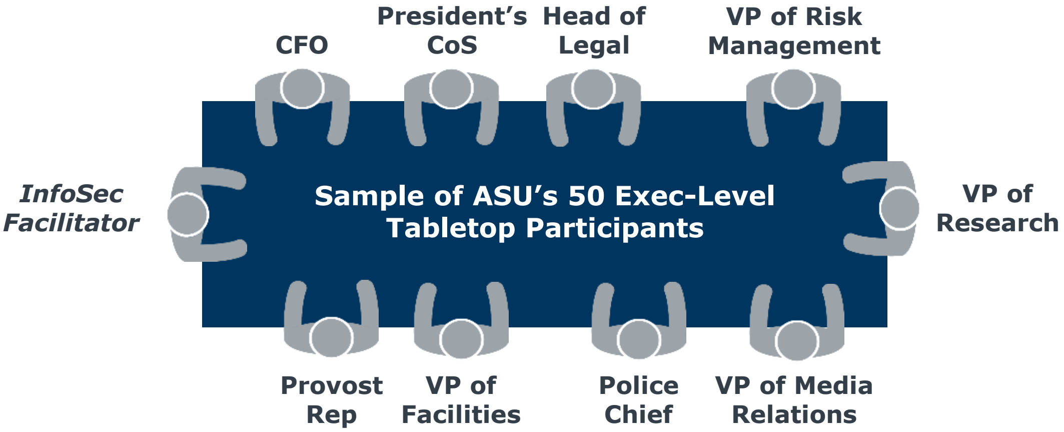
Coffee Break

Thank you for staying with us. Let’s take a 5-minute break….

We will reconvene promptly at 1:50 PM EST

Make Cyber Risk Real to Institutional Leaders

Practice Decision-Making Pathways with Leadership Tabletop Exercises



Key Attributes of Successful Exec-Level Tabletops

1. **Keep exercises short** (90 minutes to two hours) and incorporate **multiple, realistic scenario injects**
2. Curate a **cross-functional group** of **exec-level decision makers**
3. Focus on **practicing decision making** and clarifying exec roles and responsibilities over IT issues
4. Force **clear articulation** of **organizational priorities**

Source: Arizona State University, Tempe, AZ; EAB interviews and analysis.

Practice Makes Perfect

How Two Institutions Designed and Administered Their Exec-Level Tabletops

Case in Brief: University of Auckland

Participant Sample

- CIO, CISO, Provost, Deputy Vice-Chancellor of Operations, Head of Legal, Director of HR, Faculty Head, and Deputy Vice-Chancellor of Strategic Engagement

Ransomware Attack Scenario Injects

1. Complete **institution-wide system shutdown**, from educational systems to HVAC to building access controls
2. **Leak of personal information** and whether to pay ransom
3. **Compromise of backup systems**, i.e., some data could not be recovered unless ransom was paid

- Injects forced Auckland to **clearly articulate which systems to prioritize recovering** in case of attack, settling on health and safety first and communications second

Case in Brief: Arizona State University

Exercise Set-Up

- Two-hour session covered **multiple scenario injects** over course of a hypothetical week (e.g., ASU's website crashing to students being unable to access ASU during pandemic)
- **InfoSec facilitators** with gaming backgrounds guided groups of ten through exercise

After Action

- Exercise prompted IT and Risk Management leadership to rethink disaster recovery plans
- **IT disseminated key takeaways** (strengths, vulnerabilities, and plans of action); **CISO followed up with participants** based on noted engagement levels
- Exec-level tabletop findings **triggered lower-level tactical tabletops** (e.g., attack on online learning)

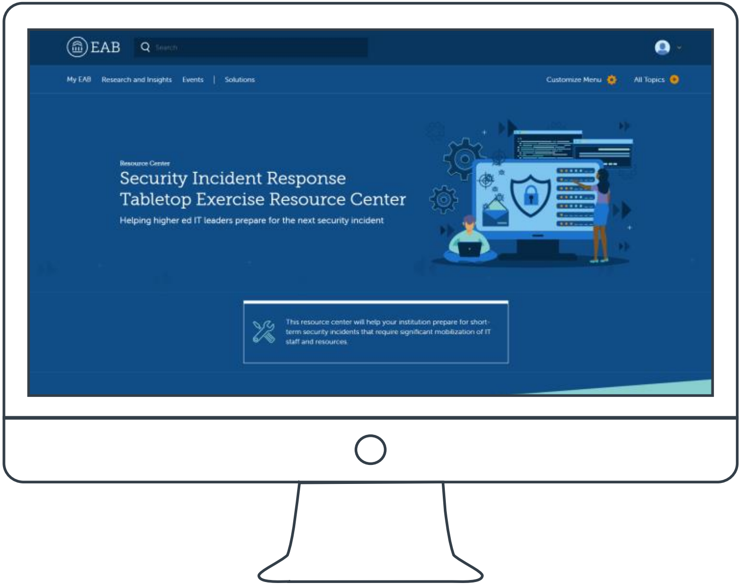
Source: Arizona State University, Tempe, AZ; University of Auckland, Auckland, NZ; EAB interviews and analysis.

Building Cyber Resilience

EAB’s Suite of Tabletop Exercise Resources

Security Incident Response Tabletop Exercise Resource Center

- Help **prepare university leaders to navigate security incident crises**. Resources include:
  - An introduction to tabletop exercises, ground rules, and **incident response prompts and scenarios**
  - **After-action report** to facilitate debriefing and discussions around key takeaways and questions
- Access the Resource Center here
- Contact us to have one of EAB’s senior experts facilitate the tabletop exercises for your institution



Resource Center

Security Incident Response Tabletop Exercise Resource Center

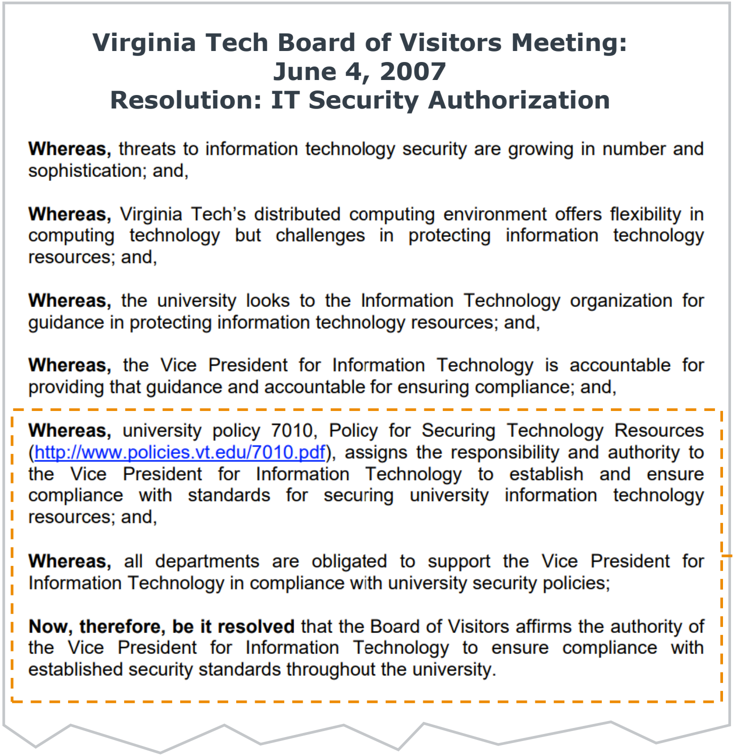
Helping higher ed IT leaders prepare for the next security incident

This resource center will help your institution prepare for short-term security incidents that require significant mobilization of IT staff and resources

Source: EAB interviews and analysis.

Empowering CIO/CISO to Ensure Compliance

Board Codifies Ultimate Authority to IT Executive in Minutes



Virginia Tech Board of Visitors Meeting: June 4, 2007 Resolution: IT Security Authorization

Whereas, threats to information technology security are growing in number and sophistication; and,

Whereas, Virginia Tech's distributed computing environment offers flexibility in computing technology but challenges in protecting information technology resources; and,

Whereas, the university looks to the Information Technology organization for guidance in protecting information technology resources; and,

Whereas, the Vice President for Information Technology is accountable for providing that guidance and accountable for ensuring compliance; and,

Whereas, university policy 7010, Policy for Securing Technology Resources (http://www.policies.vt.edu/7010.pdf), assigns the responsibility and authority to the Vice President for Information Technology to establish and ensure compliance with standards for securing university information technology resources; and,

Whereas, all departments are obligated to support the Vice President for Information Technology in compliance with university security policies;

Now, therefore, be it resolved that the Board of Visitors affirms the authority of the Vice President for Information Technology to ensure compliance with established security standards throughout the university.

Board Minutes Clearly Articulate and Document…

1. …that the Vice President for IT has the authority to **"establish and ensure compliance" with IT security policies**.
2. …the expectation that **"departments are obligated to support"** the Vice President for IT's security policies.

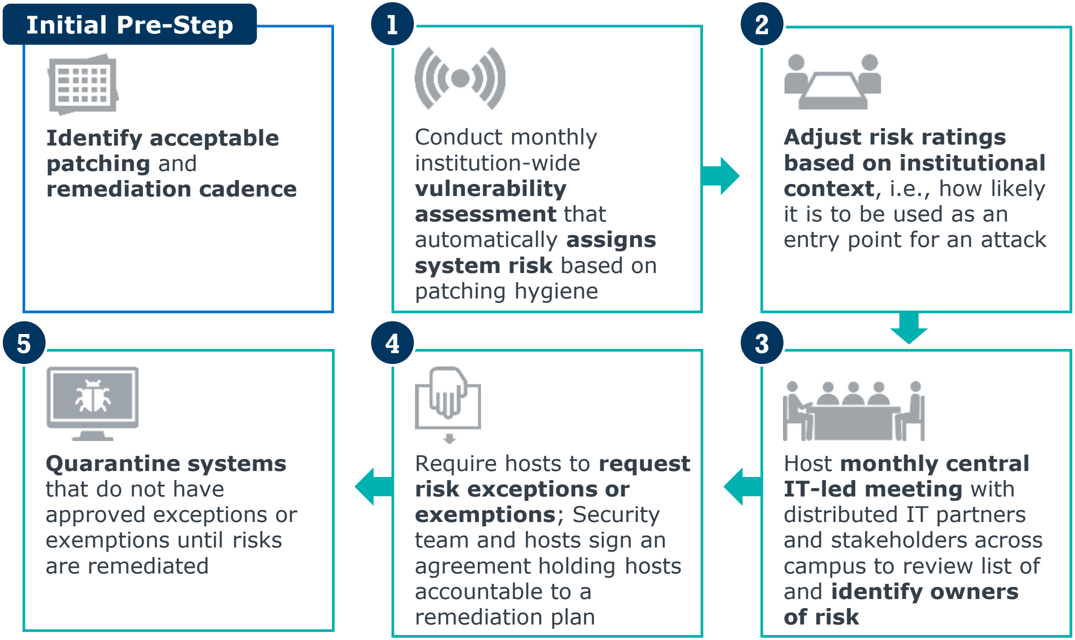
Source: Virginia Polytechnic Institute and State University, Blacksburg, VA; EAB interviews and analysis.

Tactic 4: Monthly Risk-Based System Quarantines

Patching Up Weaknesses Non-Negotiable

Rice University's Monthly[1] Risk-Based System Quarantine Process

RICE



Initial Pre-Step

Identify acceptable patching and **remediation cadence**

1

Conduct monthly institution-wide **vulnerability assessment** that automatically **assigns system risk** based on patching hygiene

2

Adjust risk ratings based on institutional context, i.e., how likely it is to be used as an entry point for an attack

3

Host **monthly central IT-led meeting** with distributed IT partners and stakeholders across campus to review list of and **identify owners of risk**

4

Require hosts to **request risk exceptions or exemptions**; Security team and hosts sign an agreement holding hosts accountable to a remediation plan

5

Quarantine systems that do not have approved exceptions or exemptions until risks are remediated

100-300 **systems reviewed** with critical and high exploitable vulnerabilities per month

10 average approximate number of **systems quarantined** per month

[1] Process (steps one through five) repeated monthly except when it interferes with the academic calendar

Source: Rice University, Houston TX: EAB interviews and analysis.

EAB

Improving End-User Engagement in Security

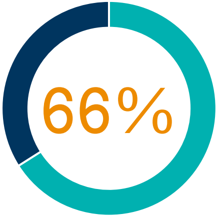
SECTION 2

- Tactic 5: Components of Effective Training
  - Gamified Security Platform
  - Department-Tailored Training
  - Mandatory Training with Penalties for Non-Compliance
  - Monthly Self-Phishing

A People and Process Issue

Poor Security Awareness and Human Error Are Main Sources of Cyber Risk

Majority of Breaches are the Fault of Humans…



of breaches were due to social engineering or miscellaneous human error in education sector in 2020

…Smaller Proportion of Breaches Due to Technology

Only

23%

of cyber breaches a result of **inadequate technology** in all sectors

Attacks Target and Resulting From Human Fallibility

Phishing/Spear Phishing

Attackers use communications like emails to convince victims to click on malicious links, send information, or download infected attachments. Attackers can gather personal information about victims to craft tailored emails.

Spoofing

Attackers pose as a person, business, or organization familiar to a victim to gain access or commit a malicious act.

Human Error

Humans can unintentionally put institutions at risk by sending data to wrong recipients, misconfiguring cloud systems, etc.

Source: Boston Consulting Group, "The CEO's Guide to Cybersecurity", *BCG Executive Perspectives*, September 2021; "Insider Threat – Cyber", *Cybersecurity & Infrastructure Agency*; Verizon, "Interactive Data Breach Investigations Report 2021", *Verizon*, 2021; EAB interviews and analysis.

Traditional Training Strategies No Longer Sufficient

Traditional Training	Emerging Training Trends
Training is delivered either once during onboarding/ orientation and/or **annually**	Training is **gamified**, rewarding ongoing participation or is administered on a **recurring** basis
Generic, one-size-fits-all modules are administered to faculty, staff, and students	**Department-tailored trainings** optimizes their engagement and addresses business needs
Effectiveness of training is **untested**	Effectiveness of trainings is measured through **monthly self-phishing** exercises
Training is either voluntary or mandatory but with **no penalties for non-compliance**	**Mandatory training** is coupled with enforced **penalties for non-compliance**

Source: EAB interviews and analysis.

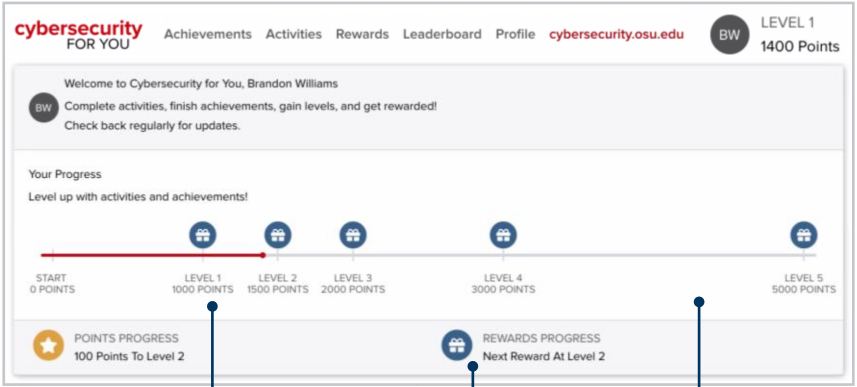
Quick Poll 3

How would you describe your security awareness and training program? (select all that apply)

a. Gamified training platform
b. Tailored to departmental needs
c. Coupled with monthly self-phishing campaigns
d. Includes penalties for non-completion

Gamified Security Platform

Ohio State's Cybersecurity4You Security Awareness Platform



cybersecurity FOR YOU

LEVEL 1
1400 Points

Welcome to Cybersecurity for You, Brandon Williams
Complete activities, finish achievements, gain levels, and get rewarded!
Check back regularly for updates.

Your Progress
Level up with activities and achievements!

START 0 POINTS
LEVEL 1 1000 POINTS
LEVEL 2 1500 POINTS
LEVEL 3 2000 POINTS
LEVEL 4 3000 POINTS
LEVEL 5 5000 POINTS

POINTS PROGRESS
100 Points To Level 2

REWARDS PROGRESS
Next Reward At Level 2

Achieving level 1 satisfies annual, one-hour security awareness requirement

Content dropped quarterly to spread utilization across year

THE OHIO STATE UNIVERSITY

Faculty and staff **can earn points** and **level up** to **satisfy security awareness requirements** and **receive rewards**. Users complete security awareness activities that tap into their self-interest (e.g., defending home networks) to change digital behavior

8,488

users accessed an activity on the C4U platform in the first two years of the program **without** it being required

Types of Rewards, From Charitable Donations to Digital Subscriptions

Level 2

- $3 to the James Fund for Life
- $3 to the Ohio State Fund for Scholarships

Level 3

- Year Subscription to Norton 360 Standard for Home
- $5 to the James Fund for Life

Level 4

- Year Subscription to Malwarebytes Premium for Home
- $10 to the Ohio State Fund for Scholarships

Level 5

- Yubico YubiKey
- $15 to the James Fund for Life

Source: The Ohio State University, Columbus, OH; EAB interviews and analysis.

Spur Department Interest in Security Awareness

Arizona State University Develops Department-Tailored Security Experiences

ASU's Department-Tailored Learning Experiences

InfoSec liaisons meet with department leadership to discuss unique department security needs and develop tailored security training learning experiences.

Peer-to-Peer Training Modules

Sandra Day O'Connor College of Law

For the College of Law, InfoSec is creating video modules of the college's dean and faculty discussing **cybersecurity legislation and policy**, e.g., the future of privacy regulation or incident response reporting.

InfoSec Department-Tailored Training Events

Enrollment Management

InfoSec hosted a **lunch-and-learn** to **discuss phishing and spoofing of call centers**, highlighting recent and nearby incidents.

Benefits of Peer-to-Peer Security Training

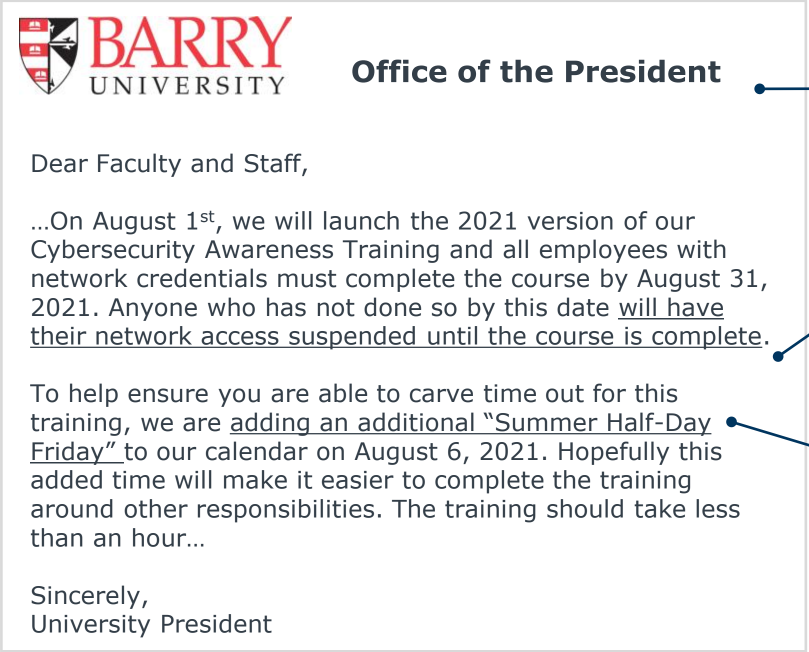
- A **more engaged audience** as a result of connecting cybersecurity with department terrain
- Faculty and staff are **more receptive** to training delivered by and learning from department colleagues

Source: Arizona State University, Tempe, AZ; EAB interviews and analysis.

No Training? No Service

Universities Push Through Mandatory Training with Non-Compliance Penalties

Training Announcement Excerpt at Barry University



BARRY UNIVERSITY

Office of the President

Dear Faculty and Staff,

…On August 1st, we will launch the 2021 version of our Cybersecurity Awareness Training and all employees with network credentials must complete the course by August 31, 2021. Anyone who has not done so by this date will have their network access suspended until the course is complete.

To help ensure you are able to carve time out for this training, we are adding an additional "Summer Half-Day Friday" to our calendar on August 6, 2021. Hopefully this added time will make it easier to complete the training around other responsibilities. The training should take less than an hour…

Sincerely,
University President

Executive support increases gravity of the requirement

Meaningful **penalty for non-compliance** compels completion of training

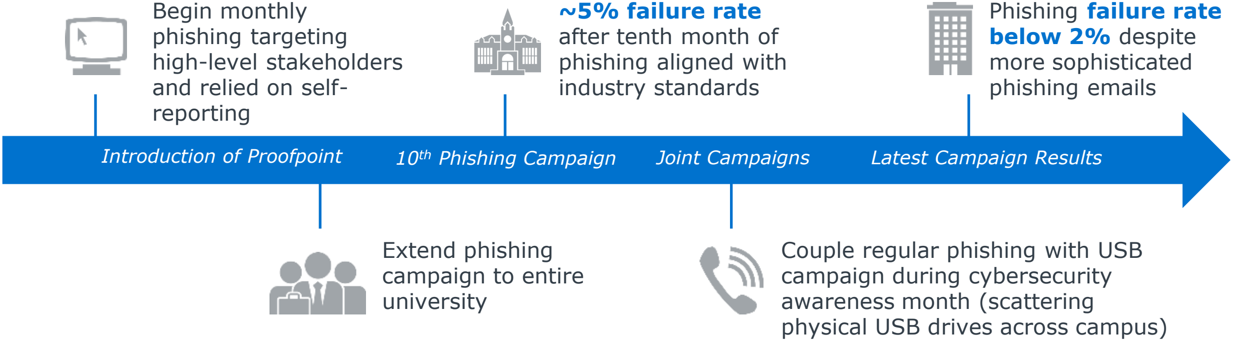
Inducements incentivize compliance and mitigate complaints about training burden or inconvenience

Source: Barry University, Miami, FL; EAB interviews and analysis.

Frequent Phishing Has Become the Norm

Measuring Training Performance with Monthly Self-Phishing Campaigns

Progression to Monthly Self-Phishing at Fairfield University



Begin monthly phishing targeting high-level stakeholders and relied on self-reporting

Introduction of Proofpoint

Extend phishing campaign to entire university

~5% failure rate after tenth month of phishing aligned with industry standards

10th Phishing Campaign

Joint Campaigns

Couple regular phishing with USB campaign during cybersecurity awareness month (scattering physical USB drives across campus)

Latest Campaign Results

Phishing **failure rate below 2%** despite more sophisticated phishing emails

YOU'VE BEEN CAUGHT!

✓

Combined with the increased frequency of self-phishing and security testing, such as the USB campaign, the **policy of positive reinforcement** for individuals who fail rather than punitive measures has **cultivated campus-wide acceptance of regular training** measures rather than distrust for the IT department.

Source: Fairfield University, Fairfield, CT; EAB interviews and analysis.

Applying Our Discussion to On-Campus Strategy

Choose the Top Three Tactics You’ll Use in the Next Six Months

Please place a **Star stamp** next to the three tactics you choose. To access the stamp, select View Options at the top of your Zoom screen, then click **Annotate > Stamp**

I. BUILDING LEADERSHIP COMMITMENT TO ENTERPRISE-WIDE SECURITY

Tactic 1: Proactive Risk-Rated Escalation Paths

Tactic 2: Executive-Level Tabletop Exercises

Tactic 3: Cyber Enforcement Mandate from the Board

Tactic 4: Monthly Risk-Based System Quarantines

II. IMPROVING END-USER ENGAGEMENT IN SECURITY

Tactic 5: Components of Effective Training

- Gamified Training Platform
- Department-Tailored Training
- Mandatory Training with Penalties for Non-Compliance
- Monthly Self-Phishing

Upcoming

Part 2 of Our Roundtable Series

Event Dates

Feb 24th

March 2nd

March 9th

Enhancing IT's Cyber Risk Management Capabilities in Higher Ed

Pinpointing High-Value Security Investments and Staffing Solutions

Register for the event here.

Contact the ITF Team

Afia Tasneem
Director
Research

ATasneem@eab.com

Linnea Hengst
Strategic Leader
Research

LHengst@eab.com

Connect with EAB

f @EAB

🐦 @EAB

in @eab_