EAB

HE Sector Held Hostage

The Risks Cyberattacks Pose and Why Senior Leaders Must Pay Attention

IT Forum

IT Forum Research Team

Afia Tasneem
*Director,
Research Design
and Discovery*

Abhi Panthagani
Senior Analyst

Nalika Vasudevan
Senior Director

Ron Yanosky
*Director,
Research Advisory
Services*

Connect with EAB

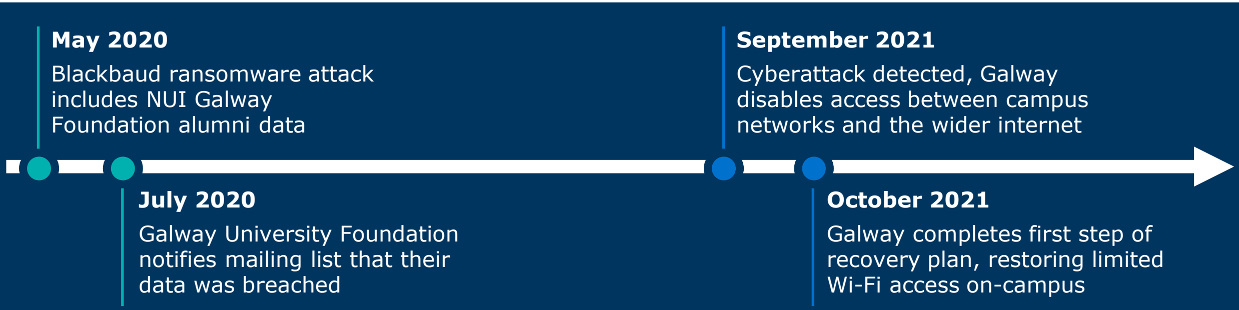
f @EAB

@EAB

in @eab_

A Digital One-Two Punch

NUI Galway Faces Two Years of Cyber Attacks



May 2020
Blackbaud ransomware attack includes NUI Galway Foundation alumni data

July 2020
Galway University Foundation notifies mailing list that their data was breached

September 2021
Cyberattack detected, Galway disables access between campus networks and the wider internet

October 2021
Galway completes first step of recovery plan, restoring limited Wi-Fi access on-campus

2020 Blackbaud Attack

- During ransomware attack, a cybercriminal removes a copy of a backup file containing NUI Galway data
- Blackbaud pays the cybercriminal to destroy data stolen in the hack
- Galway University Foundation launches internal investigation

2021 NUI Galway Attack

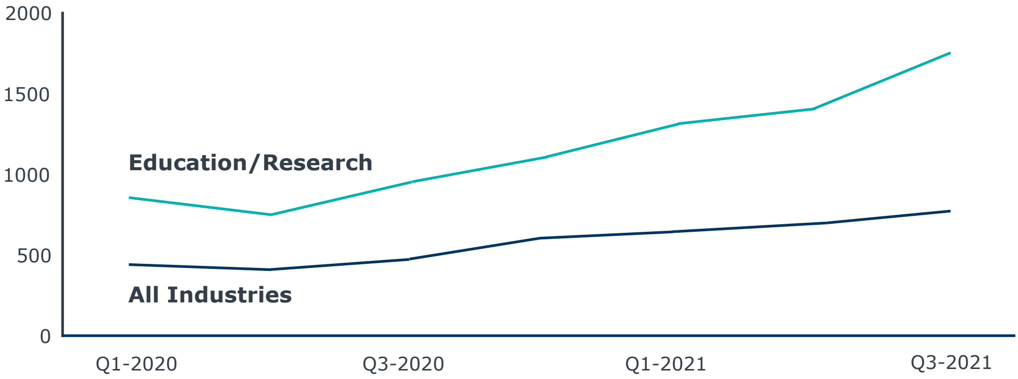
- Response disrupts online lectures, learning resources, winter conferring ceremonies.
- Internet remains fully disconnected for over a week
- Galway installs limited, temporary Wi-Fi system while rebuilding + restoring data

Source:, "NUI Galway targeted in international cybercrime attack", *Breakingnews.ie,* July 30, 2020; J. Power, "Hacker paid off after personal information of NUI Galway alumni breached", *The Irish Times*, July 30, 2020; "Blackbaud-Incident", *NUI Galway*; C. O'Brien, "Attempted cyberattack causes disruption at NUI Galway", *The Irish Times,* September 30, 2021; V. McHugh, "NUI Galway Cyber-Attack: Next step of recovery complete", *Student Independent News*, October 19, 2021; "NUI Galway on-campus internet access disabled after attempted cyber attack", *thejouranl.ie,* September 30, 2021; P. Henry, "NUI Galway cyber attack: College confirm attempted security breach hacking", *Galway Beo*, September 30, 2021; EAB interviews and analysis.

HE a Particularly Appealing Target

No Industry Has Been Spared—but Ours Bears the Brunt

Weekly Average Attacks per Organisation Globally



Education: the New Hotspot for Cyberattacks

3,936%

increase in security incidents in education from 2013 to 2020

200%

increase in attacks on education during peak of the pandemic (March and August 2020)

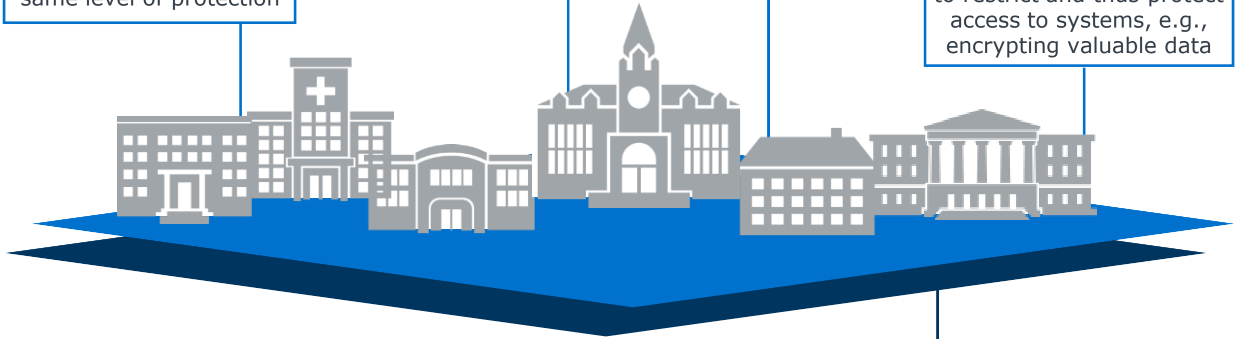
44%

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 HE a Valuable (and Vulnerable) Target



High Volume of Valuable Data

Personal, financial, and medical information on par with banks, hospitals—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 labour market or dedicate resources to posture at level comparable to similar private organisations

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

City of 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*

Recovery Comes at a Steep Price

$3.79M

Average total cost of a single data breach in education in 2021

Source: IBM Security, “Cost of a Date Breach Report 2021”, *IBM*, July 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.

No Safe Haven in Cyber-Insurance

Insurance Prerequisites Strengthen While Premiums Grow

Insurers are **strengthening requirements for**—and double-checking—a customer's security controls before writing policy

Premiums are up **50%** for best-in-class subjects and **100-300%** for lower security organisations (if quotes are provided at all)

> [A] California insurance executive reported that her education-sector clients were declined for cyberinsurance 37 times last year while her clients who found coverage saw deductibles climb from $18.7K to $747.4K and premiums increase as much as ten-fold.

AP

May 6, 2021

Insurer AXA halts ransomware crime reimbursement in France

'AXA, among Europe's top five insurers, said it was suspending the option [*to reimburse customers for ransomware payments*] in response to concerns aired by French justice and cybersecurity officials during a Senate roundtable in Paris last month about the devastating global epidemic of ransomware.'

Source: Bajak F, "Insurer AXA Halts Ransomware Crime Reimbursement in France," *AP* News, May 6, 2021; Butler C, "The Future of Cyber Insurance," *Dark Reading,* February 25, 2022; Gallagher, 2022 Cyber Market Conditions, January 2022; Kuykendall K, "Cyberinsurance Companies Raising Rates, Tightening Requirements," *Campus Technology,* February 4, 2022; EAB interviews and analysis.

Cybersecurity Expertise in High Demand

While HE Struggles to Keep Up with the (Private Sector) Joneses

HE Is Not Alone in Talent Crunch…

2.77%

Average monthly job growth in the UK in the past twelve months

20%

Longer to fill cybersecurity roles compared to other IT roles

37%

of all cybersecurity firm vacancies in UK since 2019 have been hard to fill

…But Certainly, at a (Pay) Disadvantage

HE Funding Structure Limits Ability to Raise Wages…

- Tightening budgets
- Inability to pass along costs to customers

…and Wage Increases Fraught with Ongoing Concerns

- Uncertain funding for recurring wage increases
- Existing staff discontent over wage compression

Source: Department for Digital, Culture, Media & Sport, "Cyber Security Skills in the UK Labour Market 2021"; *IBM Training and Skills Blog*, "The Demand for Cybersecurity Skills Is Outstripping the Supply of Skilled Workers,"; "Top Cybersecurity Skills for 2021," Burning Glass; EAB analysis of Emsi Burning Glass data.

Cyber Attacks Put Our Priorities at Risk

Business Operations

Brown University had to **ask instructors and staff to temporarily stop using Microsoft Windows-based machines** and 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.**

Enrolment

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.

Change Is in the Air

> ‘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*

Source: EAB interviews and analysis.

Three Must-Dos to Improve Security

1

Invest in Safety

Ensure cybersecurity budget reflects recurring needs like greater staffing and ongoing services—not just one-time expenses.

2

Make Security Everyone's Job

Set the cyber ambition in collaboration with IT, define acceptable risk, and then distribute accountability across the institution.

3

Enforce Aggressive Training Standards

The most effective trainings are mandatory, tested with self-phishing exercises and enforced with leadership backing.

Source: EAB interviews and analysis.

EAB

Invest in Safety

SECTION

1

Supporting Ongoing Cyber Investments

From CapEx to OpEx

‘The past two years have been good and bad for me. On one hand, my cabinet better understands why we’re at risk of cyber attacks. And they’ve given me money to invest in more protections. But it’s mostly been one-time funds. And I need recurring dollars to protect our assets.’

CIO
Public Research University
United States

Investments IT Leaders Needs to Make

1. **Software that extends security controls (and offsets lack of staff)**

   Example: *Extended Detection and Response (XDR)*

2. **Technology that simplifies end-user protection efforts**

   Example: *Data security and privacy software*

3. **Programmes to build internal pipeline of cybersecurity talent**

   Example: *Internal cybersecurity apprenticeship programme*

Source: EAB interviews and analysis.

Tools to Extend the Reach of IT Staff

Private University Sees Value from XDR[1] During Demo Phase

XDR Demo and Implementation

CHALLENGE ▶

IMMEDIATE VALUE ▶

CONTINUOUS RESULTS ▶

Reeling from an attack

A small, private institution was undergoing a CrowdStrike Falcon pilot when it was targeted by a NetWalker ransomware attack amid COVID.

'[With such a small IT staff], we cannot have our eyes on everything all the time.'

Minimising Damage and Exposure

The pilot CrowdStrike Falcon XDR[1] services alerted the institution to the threat and began remediation workflows, resulting in:

30% **Impacted Infrastructure,** substantially less than expected and shielding the main ERP and SIS from contamination

64 **Devices** touched by malware

4 **Weeks** of recovery with the aid of CrowdStrike Falcon to conduct a forensic investigation and restore full operations

Ongoing and As Needed

Within first 18 months of use, security team has:

- Received an average of 2-3 notifications to investigate vulnerabilities per week
- Identified and resolved 2 major vulnerabilities
- Recouped time from monitoring logs for higher order tasks

[1] Extended detection and response.

Source: EAB interviews and analysis.

Give Users Tools to Purge Sensitive Data

User-Driven Sensitive Data Removal

Institutions introduce data loss prevention technologies that proactively scan devices for personal information (PI). IT then equips units with remediation steps to protect or remove the PI, ensuring the institution reduces potential exposure in cyberattacks

1

Identify high-risk units

Install automated data loss prevention software in high-risk units or roles more susceptible to attacks or more likely to have PI incorrectly stored.

2

Automate device scanning

While voluntary adoption and on-demand scans are steps in the right direction, we recommend automating the scanning to occur at least monthly.

3

Recommend remediation actions

A representative from each college/division receives detailed reports provide guidance on how to destroy the files or redact the PI.

4 SPIRION

Generate buy-in from core users

Ideally, this tool will be set up to run automatically on a monthly or more frequent basis. However, some institutions have found that making the scans user-driven was key to ensuring buy-in.

Source: Ohio University, "Spirion"; Rochester Institute of Technology, "Private Information Management Initiative"; University of North Dakota, Grand Forks, ND; EAB interviews and analysis.

Expanding NICE-ly: Rice Trains Apprentices

Partner with HR to Build Programme

HR Consultation Emphasises Fairness, Commitment

CISO worked with HR to design a programme that is fair, measurable, and potentially scalable to the entire university

NIST[1] NICE[2] Framework

Formal training and roles framework contributed to programme design and is an advantage for cybersecurity over other potential fields for apprenticeship

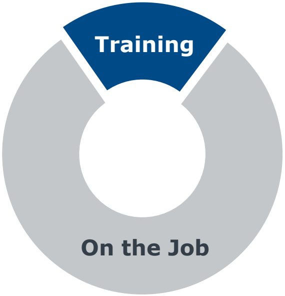
Select Core Training Programme

Training Portfolio

Training includes **Cybrary, SANS, Splunk,** and **Tenable** modules in both self-study and group formats

Learning While Doing

Roughly 20% time formal training and 80% on-the-job learning under security staff



Tier One Cybersecurity Apprentice

Tier One Employee

Regardless of previous position, the apprentice is classified and paid as tier one staff

Six Month Training Window

Following successful completion of training, candidate becomes an FTE in the cybersecurity group

CIO Backfills Candidate Position for Three Months

CIO is responsible for finding a replacement at the three-month mark

[1] National Institute of Standards and Technology.
[2] National Initiative for Cybersecurity Education, a framework to categorise and describe cybersecurity work.

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

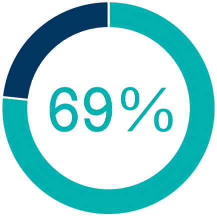
EAB

Make Security Everyone’s Job

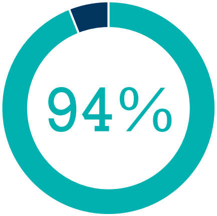
SECTION 2

IT Cannot Protect Everyone On Their Own

CISOs[1] 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

[1] Chief information security officer.

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

Distributed Stakeholders Flout Information Security Policies

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

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 Lacks 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.’

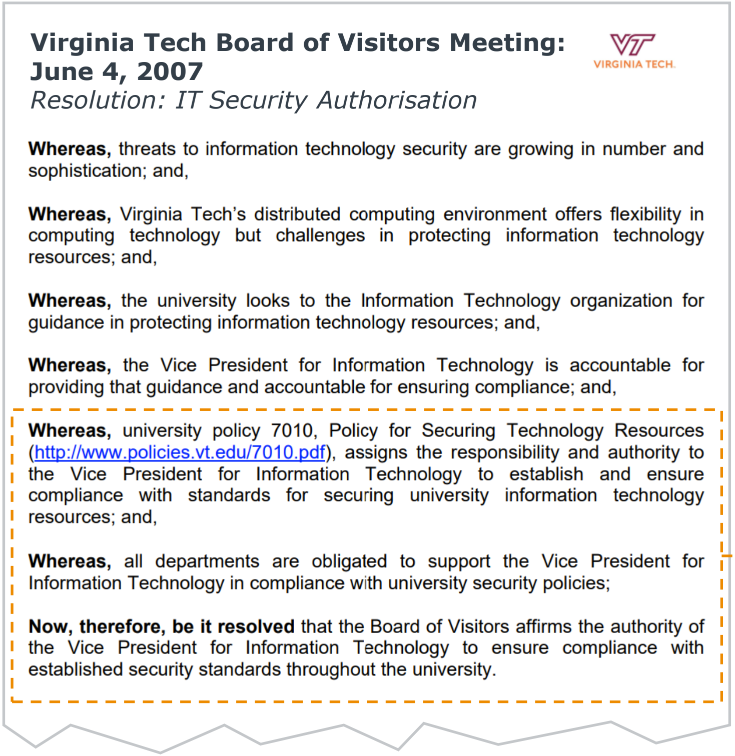
Key Imperative

1. **Empower IT to Enforce Security Standards Across Campus**
2. **Apprise Leadership of High-Priority Risks to Determine Response Options**
3. **Practice Decision-Making Pathways for Responding to Security Events**

Source: EAB interviews and analysis.

Empower CIO/CISO to Ensure Compliance

VTech Board Codifies Ultimate Authority to IT Executive in Minutes



Virginia Tech Board of Visitors Meeting: June 4, 2007

Resolution: IT Security Authorisation

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.

Translate Cyber Risks into Business Risks

Vanderbilt University's Enterprise-Wide Risk Register Template

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.

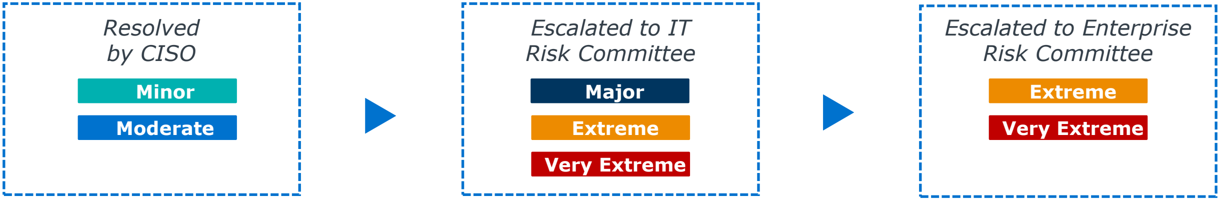
Triage Risks for Leadership Assessment

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

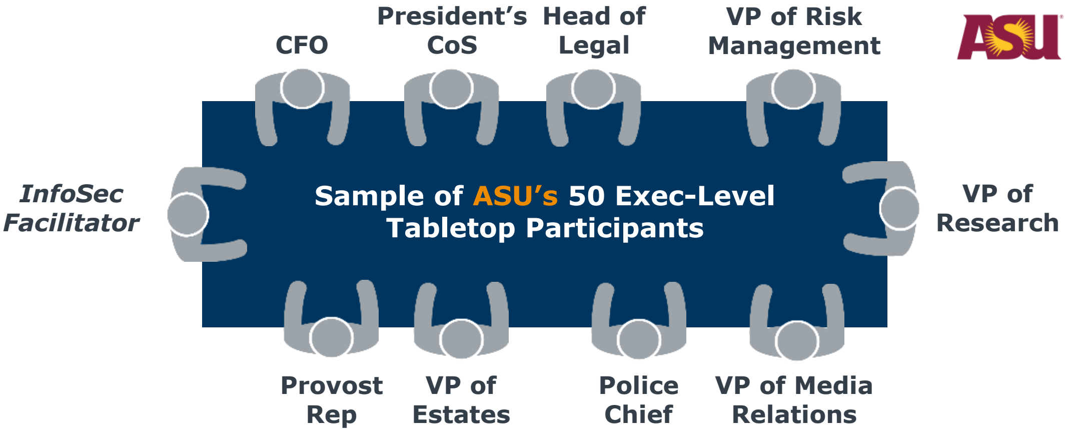
Escalated to Enterprise Risk Committee

- Extreme
- Very Extreme

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

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 **organisational 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, Academic Staff 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 prioritise 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.

EAB

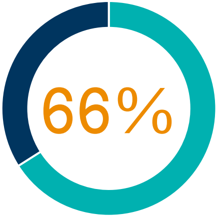
Enforce Aggressive Training Standards

SECTION 3

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

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.

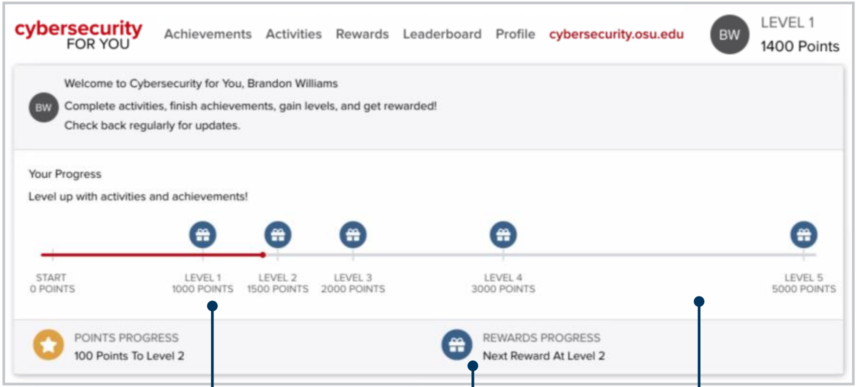
Traditional Training Strategies No Longer Sufficient

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 instructors, staff, and students	**Department-tailored trainings** optimises 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.

Gamified Security Platform

Ohio State's Cybersecurity4You Security Awareness Platform



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!

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 utilisation across year

THE OHIO STATE UNIVERSITY

Instructors 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 programme **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

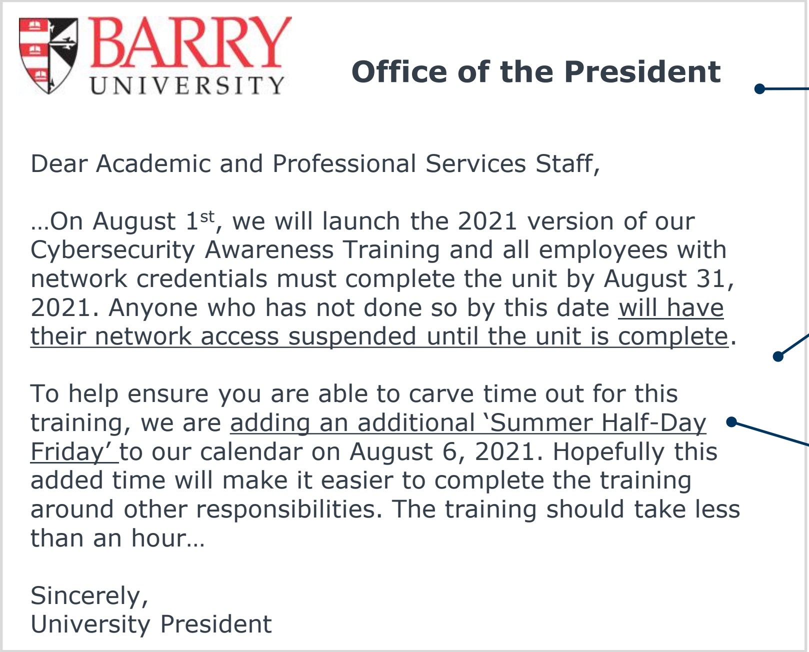
- Yubico YubiKey
- $15 to the James Fund for Life

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

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 Academic and Professional Services Staff,

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

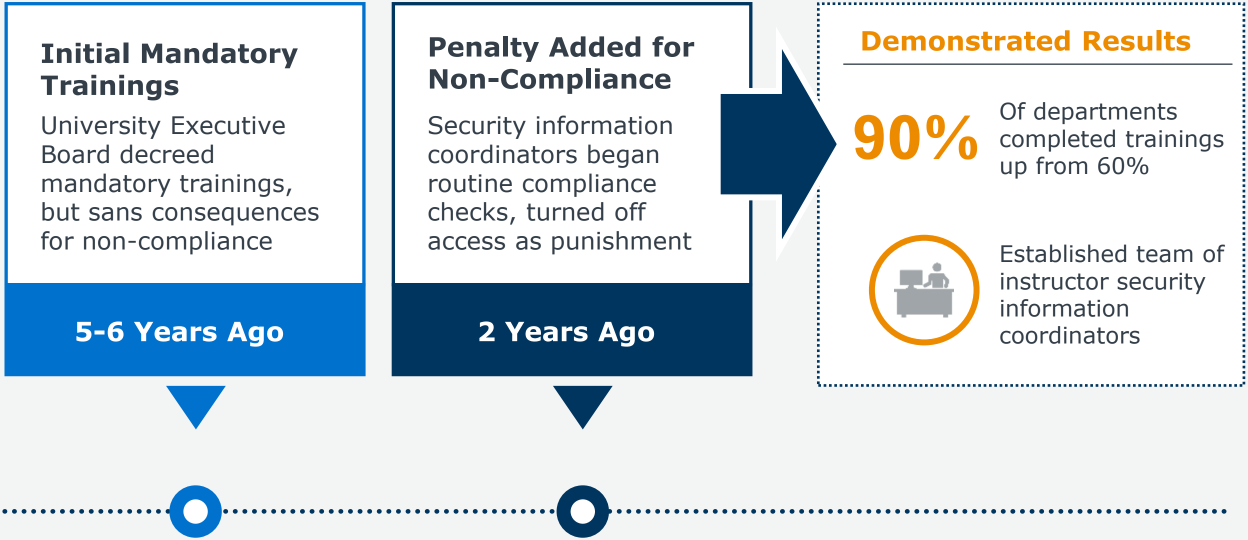
Inducements incentivise compliance and mitigate complaints about training burden or inconvenience

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

Consequences Drive Results in Mandatory Training

University Sees Rise in Completion After Implementing Penalties

The University Of Sheffield.



Initial Mandatory Trainings

University Executive Board decreed mandatory trainings, but sans consequences for non-compliance

5-6 Years Ago

Penalty Added for Non-Compliance

Security information coordinators began routine compliance checks, turned off access as punishment

2 Years Ago

Demonstrated Results

90% Of departments completed trainings up from 60%

Established team of instructor security information coordinators

Source: EAB interviews and analysis.

Three Must-Dos to Improve Security

1

Invest in Safety

Ensure cybersecurity budget reflects recurring needs like greater staffing and ongoing services—not just one-time expenses.

2

Make Security Everyone’s Job

Set the cyber ambition in collaboration with IT, define acceptable risk, and then distribute accountability across the institution.

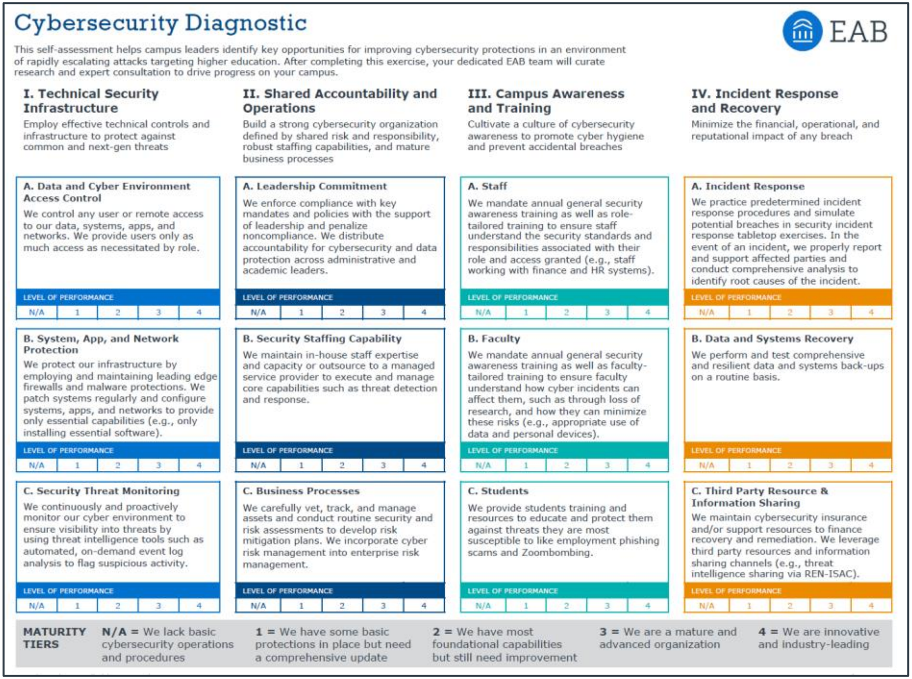
3

Enforce Aggressive Training Standards

The most effective trainings are mandatory, tested with self-phishing exercises and enforced with leadership backing.

Source: EAB interviews and analysis.

How Mature Is Your Cybersecurity Posture?



Cybersecurity Diagnostic

EAB

This self-assessment helps campus leaders identify key opportunities for improving cybersecurity protections in an environment of rapidly escalating attacks targeting higher education. After completing this exercise, your dedicated EAB team will curate research and expert consultation to drive progress on your campus.

I. Technical Security Infrastructure

Employ effective technical controls and infrastructure to protect against common and next-gen threats

A. Data and Cyber Environment Access Control

We control any user or remote access to our data, systems, apps, and networks. We provide users only as much access as necessitated by role.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

B. System, App, and Network Protection

We protect our infrastructure by employing and maintaining leading edge firewalls and malware protections. We patch systems regularly and configure systems, apps, and networks to provide only essential capabilities (e.g., only installing essential software).

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

C. Security Threat Monitoring

We continuously and proactively monitor our cyber environment to ensure visibility into threats by using threat intelligence tools such as automated, on-demand event log analysis to flag suspicious activity.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

II. Shared Accountability and Operations

Build a strong cybersecurity organization defined by shared risk and responsibility, robust staffing capabilities, and mature business processes

A. Leadership Commitment

We enforce compliance with key mandates and policies with the support of leadership and penalize noncompliance. We distribute accountability for cybersecurity and data protection across administrative and academic leaders.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

B. Security Staffing Capability

We maintain in-house staff expertise and capacity or outsource to a managed service provider to execute and manage core capabilities such as threat detection and response.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

C. Business Processes

We carefully vet, track, and manage assets and conduct routine security and risk assessments to develop risk mitigation plans. We incorporate cyber risk management into enterprise risk management.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

III. Campus Awareness and Training

Cultivate a culture of cybersecurity awareness to promote cyber hygiene and prevent accidental breaches

A. Staff

We mandate annual general security awareness training as well as role-tailored training to ensure staff understand the security standards and responsibilities associated with their role and access granted (e.g., staff working with finance and HR systems).

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

B. Faculty

We mandate annual general security awareness training as well as faculty-tailored training to ensure faculty understand how cyber incidents can affect them, such as through loss of research, and how they can minimize these risks (e.g., appropriate use of data and personal devices).

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

C. Students

We provide students training and resources to educate and protect them against threats they are most susceptible to like employment phishing scams and Zoombombing.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

IV. Incident Response and Recovery

Minimize the financial, operational, and reputational impact of any breach

A. Incident Response

We practice predetermined incident response procedures and simulate potential breaches in security incident response tabletop exercises. In the event of an incident, we properly report and support affected parties and conduct comprehensive analysis to identify root causes of the incident.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

B. Data and Systems Recovery

We perform and test comprehensive and resilient data and systems back-ups on a routine basis.

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

C. Third Party Resource & Information Sharing

We maintain cybersecurity insurance and/or support resources to finance recovery and remediation. We leverage third party resources and information sharing channels (e.g., threat intelligence sharing via REN-ISAC).

LEVEL OF PERFORMANCE				
N/A	1	2	3	4

MATURITY TIERS

N/A = We lack basic cybersecurity operations and procedures

1 = We have some basic protections in place but need a comprehensive update

2 = We have most foundational capabilities but still need improvement

3 = We are a mature and advanced organization

4 = We are innovative and industry-leading

Source: EAB interviews and analysis.

EAB

Washington DC | Richmond | Birmingham | Minneapolis

202-747-1000 | **eab.com**

@eab **@eab_** **@WeAreEAB** **@eab.life**