EAB

Elevating Security Awareness

Increasing the Relevance and Scalability of
End-User Education

IT Forum

IT Forum

Project Director

Laura Whitaker

Contributing Consultant

Ben McGuire

Design Consultant

Haley Chapman

Executive Director

Chris Miller

LEGAL CAVEAT

The Advisory Board Company has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and The Advisory Board Company cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, The Advisory Board Company is not in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. Neither The Advisory Board Company nor its officers, directors, trustees, employees and agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by The Advisory Board Company or any of its employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by The Advisory Board Company, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

The Advisory Board is a registered trademark of The Advisory Board Company in the United States and other countries. Members are not permitted to use this trademark, or any other Advisory Board trademark, product name, service name, trade name and logo, without the prior written consent of The Advisory Board Company. All other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names and logos or images of the same does not necessarily constitute (a) an endorsement by such company of The Advisory Board Company and its products and services, or (b) an endorsement of the company or its products or services by The Advisory Board Company. The Advisory Board Company is not affiliated with any such company.

IMPORTANT: Please read the following.

The Advisory Board Company has prepared this report for the exclusive use of its members. Each member acknowledges and agrees that this report and the information contained herein (collectively, the "Report") are confidential and proprietary to The Advisory Board Company. By accepting delivery of this Report, each member agrees to abide by the terms as stated herein, including the following:

1. The Advisory Board Company owns all right, title and interest in and to this Report. Except as stated herein, no right, license, permission or interest of any kind in this Report is intended to be given, transferred to or acquired by a member. Each member is authorized to use this Report only to the extent expressly authorized herein.
2. Each member shall not sell, license or republish this Report. Each member shall not disseminate or permit the use of, and shall take reasonable precautions to prevent such dissemination or use of, this Report by (a) any of its employees and agents (except as stated below), or (b) any third party.
3. Each member may make this Report available solely to those of its employees and agents who (a) are registered for the workshop or membership program of which this Report is a part, (b) require access to this Report in order to learn from the information described herein, and (c) agree not to disclose this Report to other employees or agents or any third party. Each member shall use, and shall ensure that its employees and agents use, this Report for its internal use only. Each member may make a limited number of copies, solely as adequate for use by its employees and agents in accordance with the terms herein.
4. Each member shall not remove from this Report any confidential markings, copyright notices and other similar indicia herein.
5. Each member is responsible for any breach of its obligations as stated herein by any of its employees or agents.
6. If a member is unwilling to abide by any of the foregoing obligations, then such member shall promptly return this Report and all copies thereof to The Advisory Board Company.

Table of Contents

Unlimited Copies for Members

Security Resources for You and Your Staff

Elevating Security Awareness

Best practices to help the IT function streamline breach response, make risks relevant to end users, demonstrate vulnerability, and incentivize secure behavior.

IT Breach Preparation and Response Toolkit

Get IT Forum guidance on preparation and planning steps that will expedite response, reduce cost, minimize risk, and protect institutional reputation.

Driving Phishing Awareness Across Campus

Learn how to raise awareness of phishing through dedicated blogs and deliver timely and targeted education to end users through phishing simulations.

Copies of EAB publications associated with the IT Forum are available to members in unlimited quantity and without charge. Additional printed copies of studies can be ordered through our website, by email, or by telephone. Electronic copies of all resources are also available for download by IT Forum members from our website.

TO ORDER VIA EAB.COM

Publications can be ordered at eab.com

TO ORDER VIA EMAIL

Please address your email to research@eab.com with one of the titles above in the subject line, or reach out to your Dedicated Advisor.

In your email please include the number of publications desired, your name, your institution, a contact phone number, and your shipping address. We apologize that we cannot ship materials to a P.O. Box.

TO ORDER VIA PHONE

Please call 202-266-5920 to speak with a Delivery Services associate.

About the IT Forum

Our Parent Firm: The Advisory Board Company

Founded in 1979 to serve hospitals and health systems, The Advisory Board Company is one of the nation's largest research and consulting firms serving nonprofit, mission-driven organizations. With a staff of over 2,300 employees worldwide, including 1,150 in Washington, D.C., we serve executives at about 3,000 member organizations in more than two dozen countries, publishing 150 major studies every year on progressive management practices.

Our Work in Higher Education: The Education Advisory Board

Encouraged by leaders of academic medical centers that our model and experience serving nonprofit institutions might prove valuable to colleges and universities, The Advisory Board Company launched The Education Advisory Board, our higher education practice, in 2007. We are honored to serve over 800 college and university executives through our EAB memberships.

Research and Insights

Academic Affairs Forum

Strategic advice for provosts to elevate performance in teaching, research, and academic governance

Student Affairs Forum

Research helping student affairs improve student engagement and perfect the student experience

Continuing and Online Education Forum

Research on continuing and online education program growth, revenues, and academic quality

Enrollment Management Forum

Guidance and support for chief enrollment officers to overcome today's enrollment challenges

Business Affairs Forum

Research and support helping CBOs improve administrative efficiency and lower costs

Community College Executive Forum

Strategic advice for community college leaders on strengthening student success, workforce development, and institutional planning

IT Forum

Research for CIOs on leveraging information and technology to further higher education

Advancement Forum

Research and performance analytics for development officers to elevate fundraising performance

Performance Technologies

University Spend Collaborative

Business intelligence and price benchmarking to help institutions better manage procurement and outside spend

University Student Success Collaborative

Predictive modeling and academic milestone tracking to help universities improve completion and time to degree

Community College Student Success Collaborative

Student support tool for college navigation and career pathing to help colleges improve graduation and employment outcomes

Advisors to Our Work

We are extremely grateful to those who generously contributed their time, expertise, and insight to our research.

American University
Cathy Hubbs
Chief Information Security Officer

Anne Arundel Community College
Marcelle Lee
Cybersecurity Instructional Specialist

Aon Risk Solutions
Leta Finch
National Practice Leader, Higher Education

Kevin Kalinich
Global Practice Leader, Cyber Risk Insurance

Arthur J. Gallagher
John McLaughlin
Managing Director

Boston College
David Escalante
Director of Computer Policy and Security

David Millar
Principal Information Security Analyst

Brown University
David Sherry
Chief Information Security Officer

California State Polytechnic University, Pomona
John McGuthry
Chief Information Officer

Central Michigan University
Roger Rehm
Vice President and Chief Information Officer

Eric Lorenz
Director of Infrastructure & Security

CynergisTek, Inc.
Lori McElroy
Senior Compliance Consultant

Eastern Michigan University
Rocky Jenkins
Director of IT Services

George Washington University
Amy Butler
Assistant Vice President, Information Security and Compliance Services

ID Experts
Christine Arevalo
Vice President, Healthcare Fraud Solutions

Indiana University-Bloomington
Brad Wheeler
Vice President for IT and Chief Information Officer

Daniel Calarco
Chief of Staff to the Office of the Vice President for Information Technology

Ithaca College
Kris Monroe
Information Security Officer

Lafayette College
John O'Keefe
Vice President and Chief Information Officer

Metropolitan State University of Denver
James Lyall
Chief Information Officer and Associate Vice President of Academic and Student Affairs

Mike Hart
Director of IT Security, Networking, Asset Management, and Procurement

North Dakota State University
Theresa Semmens
Chief IT Security Officer

Ohio State University
Helen Patton
Chief Information Security Officer

Purdue University
Gerry McCartney
System Chief Information Officer and Vice President for Information Technology

Rochester Institute of Technology
Ben Woelk
Policy and Awareness Analyst

San Jose State University
Terry Vahey
Associate Vice President and Chief Information Officer

Mike Cook
Identity and Information Security Manager

Advisors to Our Work (continued)

Tennessee Technological University
Reid Christenberry
Chief Information Officer

University of California-Berkeley
Lyle Nevels
Assistant Vice Chancellor–IT, Deputy Chief Information Officer

Paul Rivers
Interim Chief Information Security Officer

University of Florida
Rob Adams
Chief Information Security Officer

University of Georgia
Brian Rivers
Associate CIO for University Information Security

University of Maryland-Baltimore County
Jack Suess
Vice President for IT and Chief Information Officer

University of Maryland-University College
Alan Carswell
Chair of Cybersecurity and Information Assurance Program

University of Michigan
Sol Bermann
Interim Chief Information Security Officer

University of North Carolina at Wilmington
Zachery Mitcham
IT Security Officer

University of Pennsylvania
Josh Beeman
Information Security Officer

University of Pittsburgh
Jay Graham
Enterprise Architect

Sean Sweeney
Information Security Officer

University of Toronto
Robert Cook
Chief Information Officer

Martin Loeffler
Director of Information Security

Top Lessons from the Study

The Challenge: Elevating Information Security Awareness

Getting Campus to "Threshold Awareness" the Biggest Leverage Point

Small to medium-sized breaches are a question of when, not if, because higher education institutions, highly decentralized and full of diverse information sets, are a data-rich soft target.

Often-cited reputational risks are arguably overstated in the mainstream media; little evidence exists that data breaches risk student enrollment, but a stronger case can be made for research, advancement, and state legislature oversight.

The more significant and likely cost is recurring expense from small breaches (i.e., less than 10,000 records) creating business distraction and remediation expense.

The biggest opportunity to reduce an institution's risk profile is not by strengthening controls against malicious actors, but instead by educating faculty, students, and staff to stop being "unintentionally unsecure" and to practice basic security hygiene.

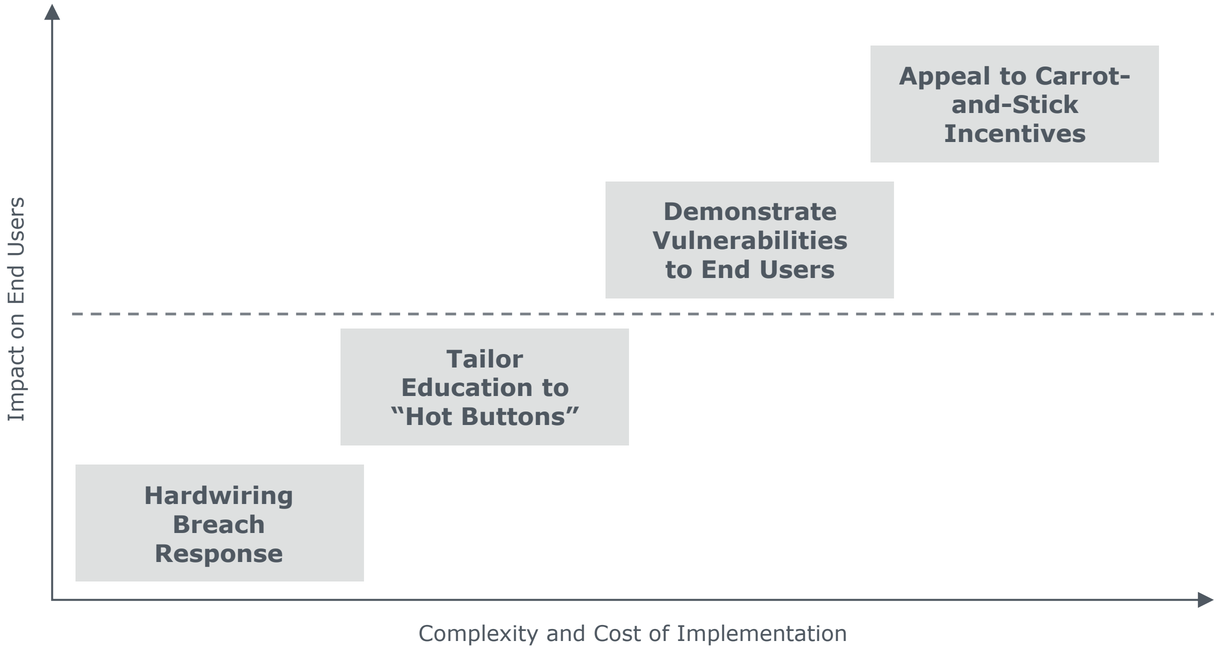
Why Do Current Security Awareness Efforts Fall Short?

Most security education programs have a mass-marketing bias; they use ubiquitous cues, humor, and shock value to "get noticed" by busy constituents rather than trying to sustain behavior changes.

In addition, awareness efforts lack relevance for end users; they come from the central IT office and focus on institutional consequences, rather than originating from managers or colleagues and focusing on individual work and department risks.

Finally, security awareness efforts are episodic and reactive; delivered as a campaign or in the hurried aftermath of a breach event, campaigns have to start all over again every term with new students and staff.

How Are the Best Making End-User Education Scalable and Relevant?


Appeal to Carrot-and-Stick Incentives
Demonstrate Vulnerabilities to End Users
Tailor Education to "Hot Buttons"
Hardwiring Breach Response
Impact on End Users
Complexity and Cost of Implementation

Top Lessons from the Study

The Challenge: Elevating Information Security Awareness

Foundational Requirement: Hardwiring Breach Response (p. 23-28)

The single biggest preventable security management problem is not having well-defined processes in place for triaging, escalating, and communicating security breaches. Schools lacking such processes have to educate a broad range of stakeholders in moments of crisis, incurring unnecessary remediation expenses and bad PR.

To combat this issue, some institutions are not only creating breach response processes, they are also appointing a Breach Response Leader: a single owner who temporarily drops everything to focus on response, and who is tasked with correctly and quickly executing process.

Tailor Security Risk Education to Different End Users' "Hot Buttons" (p. 29-35)

Security teams are finding success by creating replicable processes for making security education relevant to the different incentives of boards, faculty, students, and staff.

One successful practice is to link board education to high-profile stories in trade press. Private-sector incidents can be used for just-in-time education about the nature of threats and adequacy of current institutional protections. Security teams can also create unit-level security profiles referencing "live" faculty projects, illustrating how unsecure behaviors can threaten individual faculty grant funds, research data validity, and ongoing scholarship. Existing security trainings can be repurposed to teach employees and students better security practices for their personal devices and information; the habits they learn for their own digital safety will encourage them to employ better security behaviors at all times.

Demonstrate Vulnerabilities: Show End Users "This Could Happen to You" (p. 37-44)

Creative security teams are reusing existing security monitoring efforts to educate units and individuals about avoiding vulnerabilities. Sharing results of DLP monitoring and board security heat maps, and showing units how they fare against university norms are low-risk, high-value practices. Just sharing the information can change behavior, as no one wants to perform worse than their peers.

Demonstration hacks and self-phishing provide even more individualized evidence of vulnerabilities by showing end users the tangible things they could lose through unsecure behavior. While there can be downside risks of employing such practices—end users may feel tricked and react negatively—successful programs say these risks can be mitigated with proper "pre-wiring."

Incentivize Secure Decisions: Appeal to Carrot-and-Stick Incentives of Leaders (p. 45-51)

Our research did not find many IT groups charging back the costs for security breaches to units. Most breaches result from multiple points of failure and innocent, first-time offenses, and it's not worth disrupting relationships with charge-backs. Those who do charge back for breaches do so sparingly, only for incidents traceable to individual units and repeat offenders who have consistently failed to adhere to basic security practices. The purpose is not to recover costs, but to get deans' attention and encourage them to personally enforce standards going forward.

Successful programs get positive buy-in from deans and department chairs for new cyber risk mitigation policies by appealing to financial and mission incentives alongside reduced department-level vulnerabilities. In addition, security teams can offer perks to academic leaders to get them on board.

Security Awareness Diagnostic

Hardwiring Breach Response	Yes	No
Has your institution designated a role with clear operational responsibility during an information security breach?		
Does IT know which distributed applications in academic departments are necessary for business continuity and which could be easily quarantined during a breach?		
Does IT collect granular metrics on the efficiency and effectiveness of data breach response, allowing for department and data comparisons, as well as benchmarks for improvement?		

If you answered "No" to any of these questions, please turn to pages 23-28.

Making Risks Relevant	Yes	No
Are the board of trustees and cabinet informed about data breach risks, and are they proactive about risk mitigation?		
Do academic department leaders and staff treat information security as a task relevant to their own daily work?		
Do end users without access to sensitive data (e.g., SSN) understand why security rules apply to them?		

If you answered "No" to any of these questions, please turn to pages 29-36.

Security Awareness Diagnostic

Demonstrating Vulnerability	Yes	No
Does IT use centrally tracked information about unit vulnerabilities to inform education for local managers?		
Can department business and academic leaders benchmark their security posture against peer units or over time?		
Do non-technical academic leaders understand the mission-related relevance of information security vulnerabilities?		
Do end users and administrative support offices understand the purpose and value of self-phishing campaigns?		

If you answered "No" to any of these questions, please turn to pages 37-44.

Incentivizing Secure Practices	Yes	No
Does central IT assess financial penalties for "self-inflicted" breaches at the departmental level, to be paid by deans or administrative leaders from local budgets?		
Does IT facilitate centralization of distributed servers and computing to generate stronger campus security, capture economies of scale, and allow departments to reinvest in local mission?		

If you answered "No" to any of these questions, please turn to pages 45-51.

EAB

The Challenge

Elevating Security Awareness

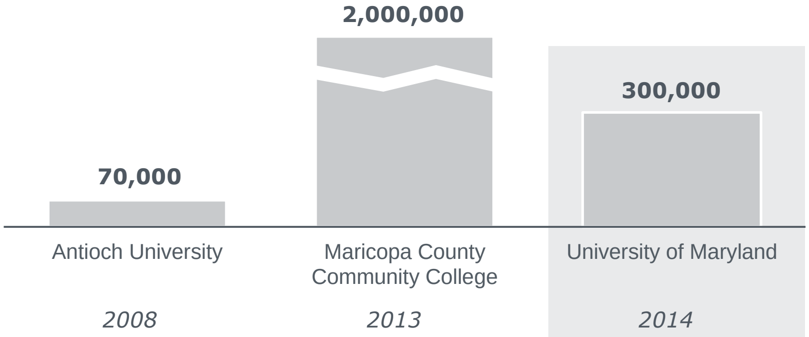
INTRODUCTION

Security Breaches Making Headlines

Modern higher education institutions generate and use large, complex data sets to shepherd students and research missions. At the same time, they share data in partnership with third parties, vendors, and private-sector research collaborators; all of this creates more threats and vulnerabilities, faster than ever before. Higher education institutions of all types have been the target of new threats; small private schools, community colleges, and research flagships are all at risk.

High-Profile Incidents Across Institutional Types

Compromised Records in Recent Data Breaches



University of Maryland’s Postmortem

≈280,000 records of current and former students, faculty, and staff compromised

Credit monitoring expense*:* **$2.6 million**

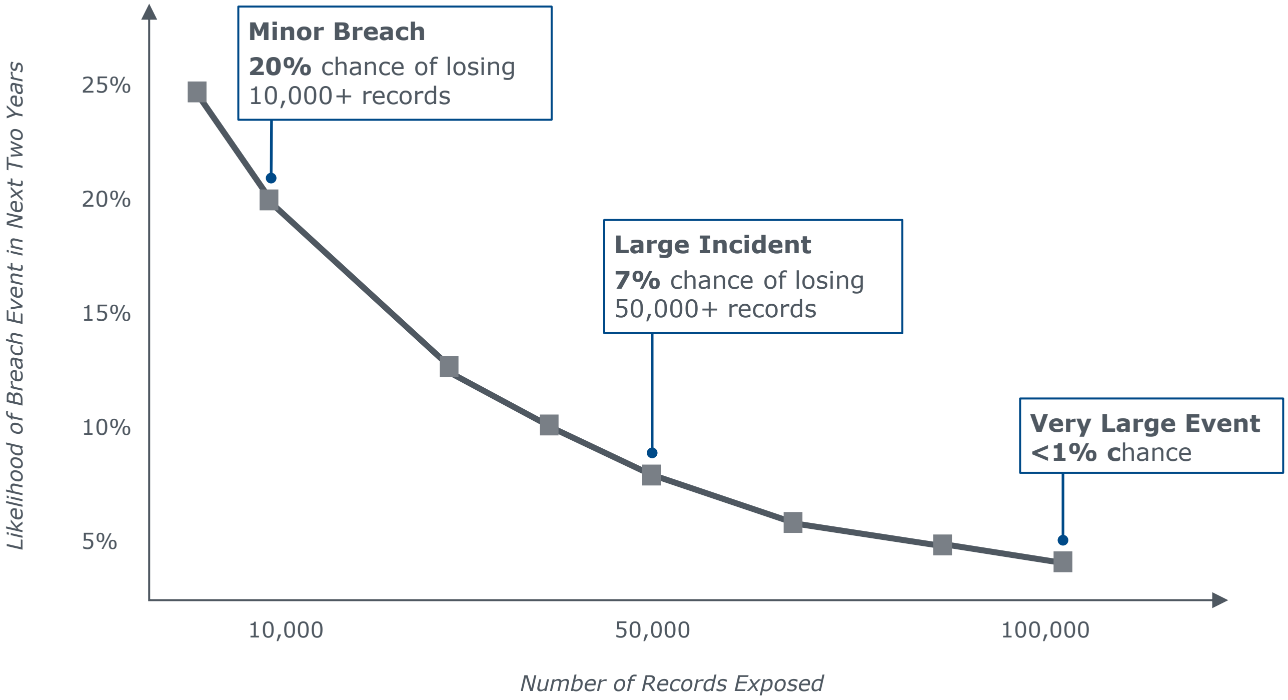
Estimated cost of reorganization and new security protections*:* **$20 million**

Source: EAB interviews and analysis.

A Question of When, Not If

CISOs from various industries around the world estimated the probability of data breaches at their own institutions in the next two years and indicated that major losses involving hundreds of thousands of records are likely to remain very rare. However, one in five organizations expects to experience a breach involving at least 10,000 records in the next two years.

CISOs' Educated Guess on Probability and Size of Data Breaches in the Next Two Years



Source*:* Ponemon Institute LLC, 2014 Cost of Data Breach Study: Global Analysis, May 2014.

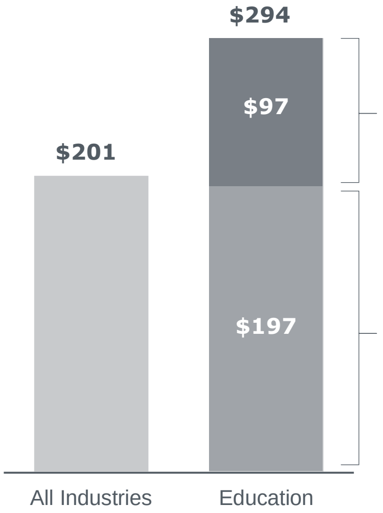
Education Breaches Carry High Costs

The average cost per compromised record is higher in education breaches than the average in other industries. Across global industries, only health care had a higher cost per record in breaches. Two-thirds of breach costs are associated with indirect expenses like victim notification, reorganization, and business interruption—losses that are rarely covered by insurance. Only one-third of average costs are direct crisis services, legal penalties, and government fines.

Across industries, breaches were more expensive if they involved lost or stolen devices, third-party data, or if the breached organization engaged with consultants. Organizations reported lower per capita expenses when they had a CISO appointed, a business continuity plan, and an incident response plan in place.

CISOs, Response Plans Reduce Indirect Breach Costs

Breach Cost per Capita, 2014



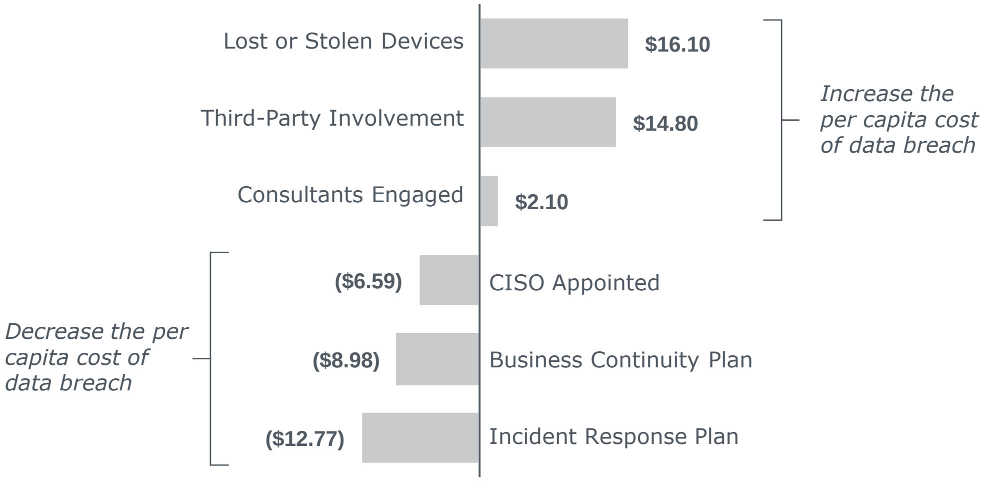
Direct Costs

- Crisis Services
- Defense
- Settlement
- Fines/Penalties
- Insurance

Indirect Costs

- Detection
- Victim Notification
- Credit Monitoring
- Remediation
- Reorganization
- New Hiring
- Business Interruption

Factors Ranked by Impact on per Capita Costs of Data Breach



Increase the per capita cost of data breach

Decrease the per capita cost of data breach

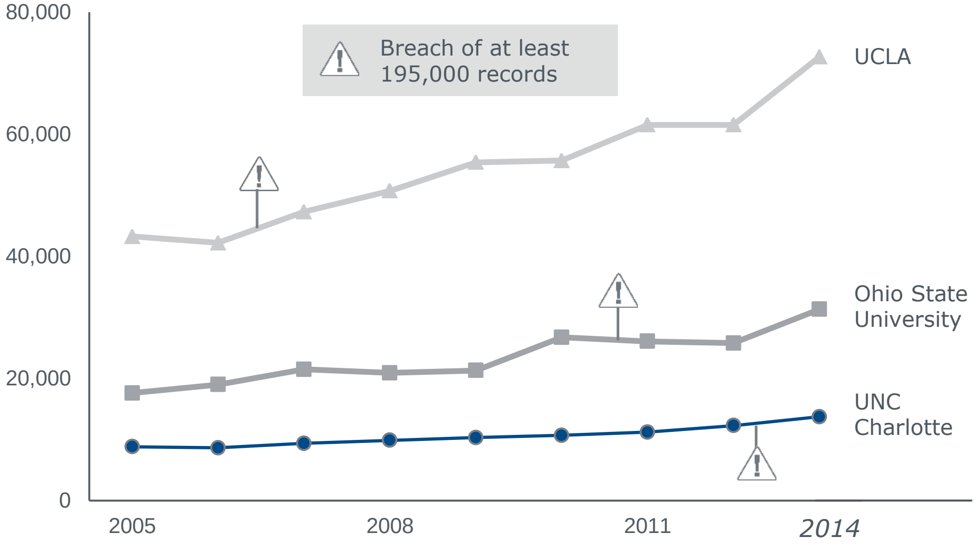
Source: Ponemon Institute and IBM, 2014 Cost of Breach Study, http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/.

What’s the Worst That Could Happen?

Student applications, yield, and retention do not show a significant correlation to large breach events across institutional types, indicating that fears about reputation loss with students may be unfounded.

Student Enrollments Likely Not at Risk from Breach

Undergraduate Applications After Major Breach Event



Revenue from major donors, private-sector research partners, and state governments could be at risk when a major breach occurs. In a constrained and competitive funding environment, a data breach could be the difference between winning and losing a major research project or large gift from a private donor.

Research, Advancement Revenue Streams at Risk

Revenue Sources	Why at Risk
Research funding from federal government agencies	Government agencies are increasing the expected security protections for federally sponsored research
Research funding from private and corporate sources	Corporate partners are extremely sensitive about losing valuable intellectual property
Funding approval from state governments	State governments skeptical of new investments in unsecure administration
Gifts from major donors	‘Mega-donors’ sensitive about anonymity or gift term secrecy may balk at perceived risks in institutional gifts

Looking for Reasons to Say “No”

“Corporate partners won’t work with people they think can’t protect their IP. My fear is that security and compliance perceptions will be grounds to put us out of the running.”

VPRA, Public Research University

Source: IPEDS Data Center and Privacy Rights Clearinghouse.

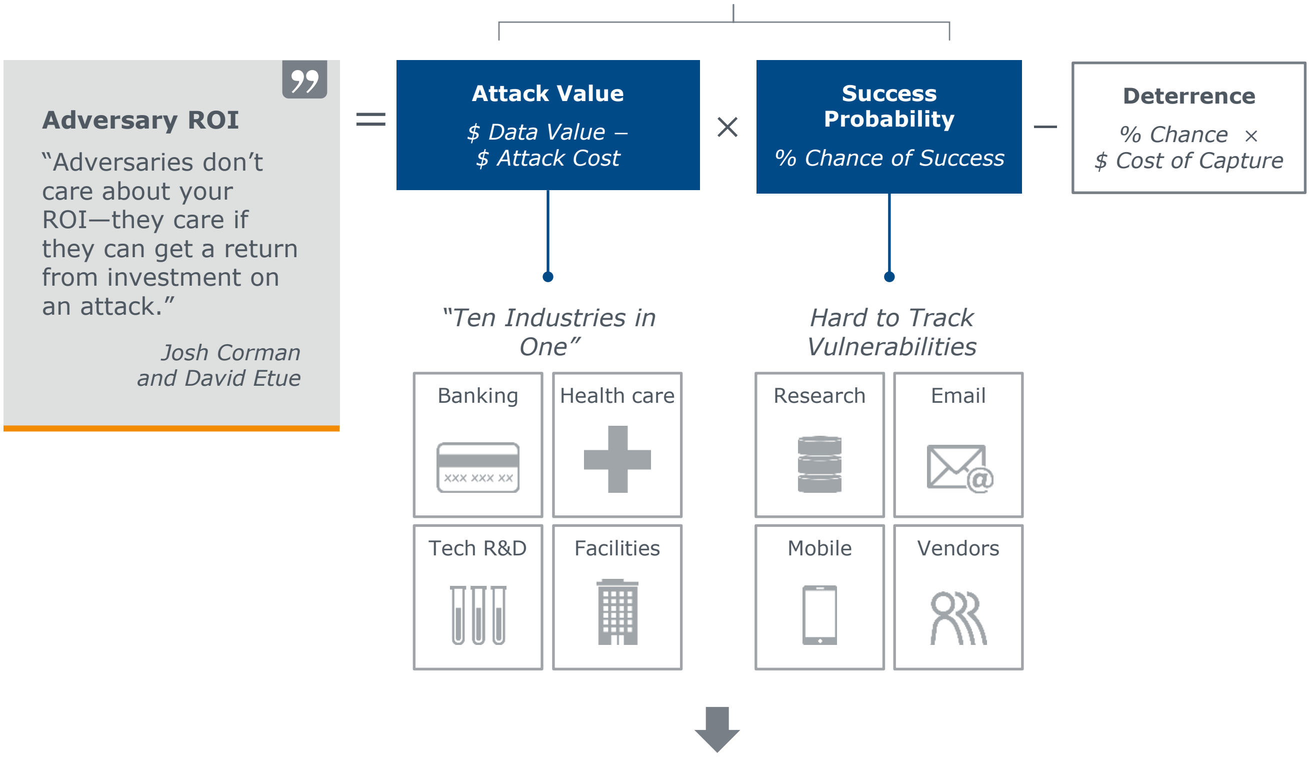
A Data-Rich 'Soft Target'

Private sector researchers developed a new formula to supplement traditional ROI analysis in assessing the value of new security controls. Traditionally, institutions have struggled to define the value of not being attacked versus the cost of implementing new controls. Security adversaries, on the other hand, from identity thieves to government-sponsored hackers, can easily identify their own ROI. The formula measures the ROI to the adversary, pointing the way for targets to decrease the potential return of an attack.

The formula also demonstrates why higher education is uniquely at risk; modern universities hold more types of valuable data than any industry, so a successful breach is akin to hitting 10 industries at once. At the same time, vulnerabilities are more distributed, and more opaque, than in any industry; higher education CISOs have immense difficulty in tracking and controlling all campus vulnerabilities.

Tantalizing, Vulnerable Resources

Higher Ed Inviting to Middle-Tech Adversaries



Adversary ROI

"Adversaries don't care about your ROI—they care if they can get a return from investment on an attack."

Josh Corman and David Etue

Elements Outside Institutional Control

- **Lower data value:** Not a viable option
- **Raise the chance of capture:** Possible (to a point) to improve through technology
- **Raise the cost of capture:** Determined by law enforcement

Elements within Institutional Control

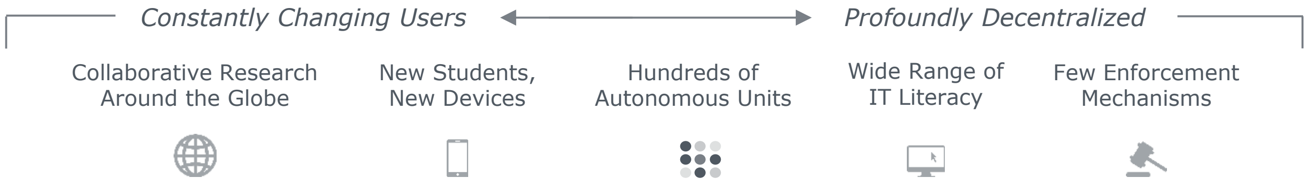
- **Raise the attack cost:** More training for end users, more perimeter protections
- **Lower the probability of success:** More training for end users, more consolidation of technology

Source: Corman, J. and Etue, D. "Adversary ROI: Why Spend $40B Developing It, When You Can Steal It for $1M?", RSA Conference 2012.

Higher Education Uniquely Difficult to Secure

To protect a transient and collaborative user base with a proudly decentralized academic culture focused on information sharing, higher education IT leaders face a unique and daunting task.

Openness = Academic Freedom + Shared Governance


Constantly Changing Users ↔ *Profoundly Decentralized*

Collaborative Research Around the Globe

New Students, New Devices

Hundreds of Autonomous Units

Wide Range of IT Literacy

Few Enforcement Mechanisms

Determined to Stay "Free"

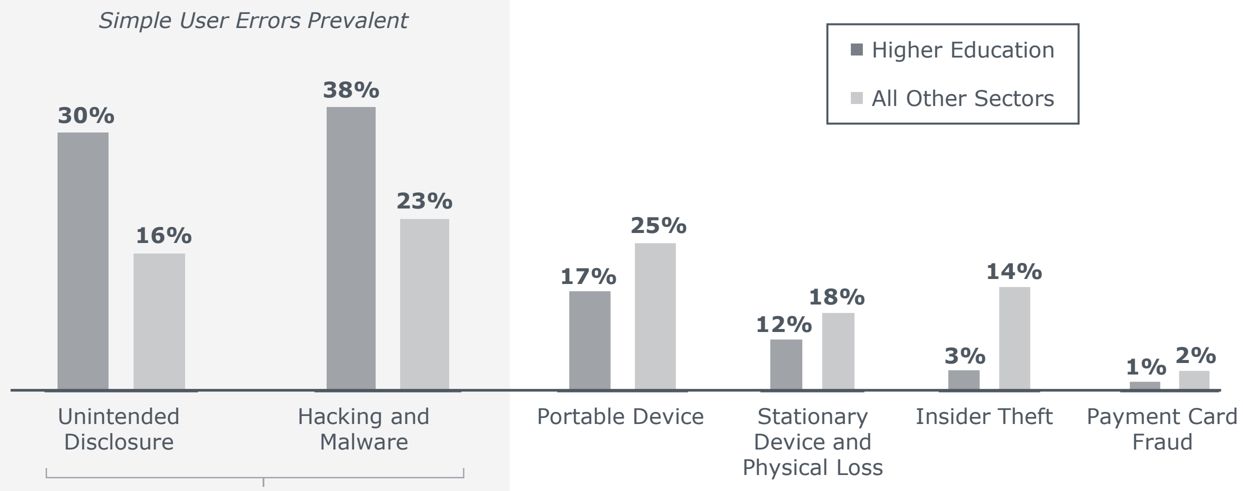
> "Higher ed is by design focused on transparency, with as few restrictions as possible to information sharing. The bedrock mind-set tilts toward academic freedom."
>
> *CIO, Regional Masters University*

Uniquely Risky

> "Higher education is one of the most heavily regulated industries in the U.S.—and it has more risk-producing constituencies than almost any other industry."
>
> *Leta Finch, Aon Risk Management Services*

The impact of higher education's security culture challenge is visible in the distribution of breach types in the industry; breaches that involve simple user errors (e.g., not patching servers, responding to phishing emails) are twice as common in higher education as they are in other industries.

Percentage of Total Breaches in Higher Education vs. All Other Sectors (2005-2014)



"Unhygienic" Behaviors

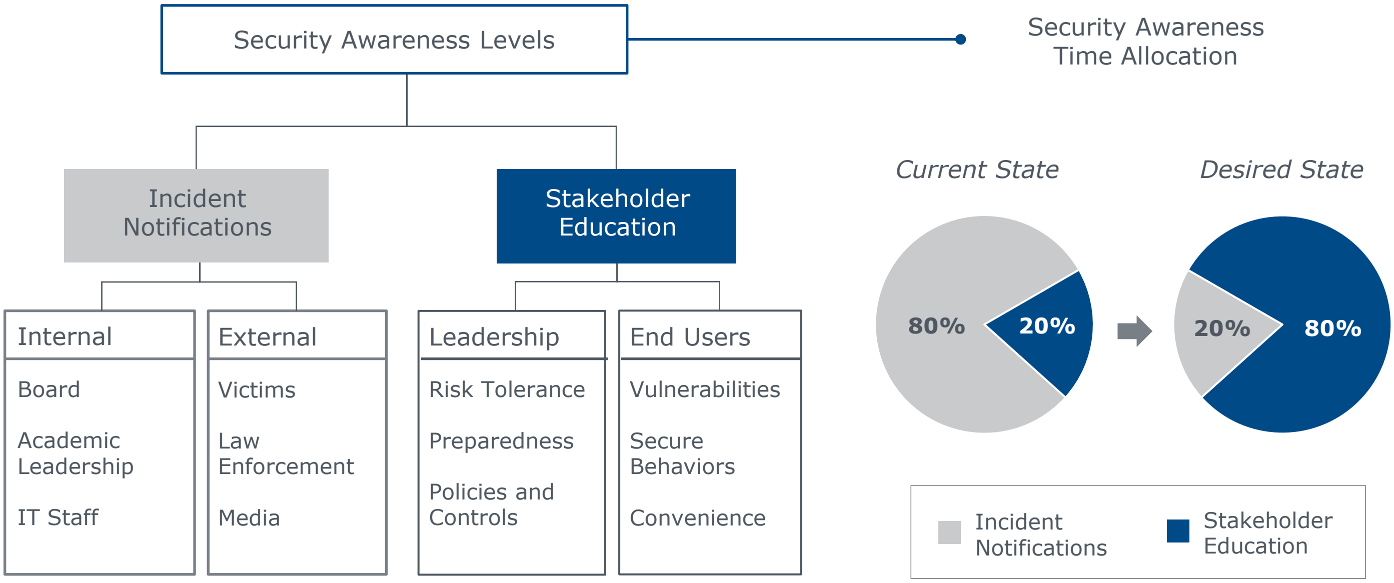
- Not patching software
- Downloading programs
- Unencrypted email
- Phishing response

Source: Privacy Rights Clearinghouse, http://www.privacyrights.org/

Reactive Crowds Out the Intentional

The need to respond to minor security lapses (e.g., compromised passwords) keeps IT from focusing education on secure behaviors and preparedness. In addition, proactive security awareness campaigns (described on the next page) are sent to everyone on campus without differentiation, using ubiquity and clever slogans that do not change long-term behaviors.

Complementary (Competing?) Levels of Awareness



No Time for Strategy

"We're supposed to be in the strategic realm, looking to future threats and challenges. The reactive work chews into my time and the strategic element of my job, putting me into a tactical focus, and we can't prepare for what's coming."

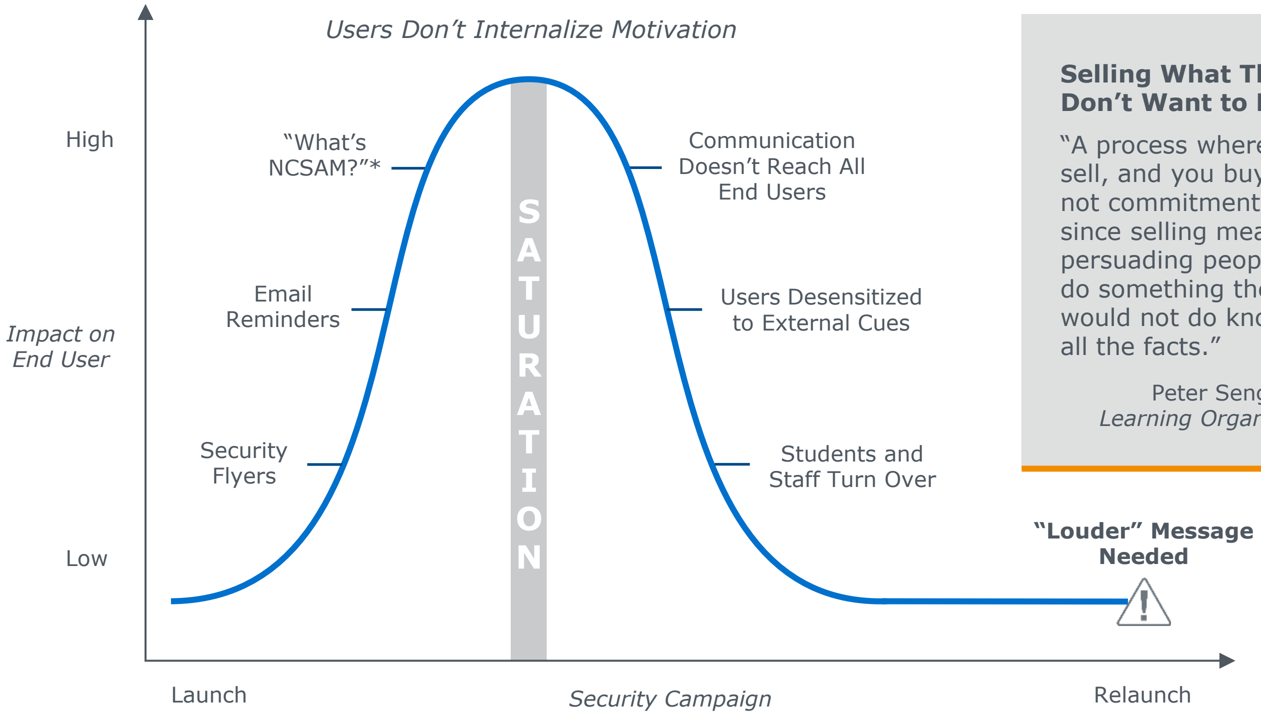
CISO, Public Research University

Source: EAB interviews and analysis.

The Predictable Fate of Security-as-Campaign

When institutions treat security awareness as campaign, messaging relies on shock value and ubiquity, to which end users get desensitized quickly. Email reminders and meetings with IT staff make an initial impact, but without buy-in from managers, users don't internalize the need to improve behavior. Soon enough, end-user turnover obviates the campaign's early success, and the institution ultimately fails to generate long-term commitment with students, faculty, and staff.

Impact of Security Campaigns on Behavior


Users Don't Internalize Motivation
High
Impact on End User
Low
"What's NCSAM?"*
Email Reminders
Security Flyers
SATURATION
Communication Doesn't Reach All End Users
Users Desensitized to External Cues
Students and Staff Turn Over
"Louder" Message Needed
Launch
Security Campaign
Relaunch

Selling What They Don't Want to Buy

"A process where 'I sell, and you buy', is not commitment, since selling means persuading people to do something they would not do knowing all the facts."

Peter Senge, *The Learning Organization*

* National Cyber Security Awareness Month

Source: New ITS Mascot Hooks Freshmen, http://yaledailynews.com/blog/2010/09/02/new-its-mascot-hooks-freshmen/
Source: Anti-Phishing Posters for Yale, 2010, https://www.behance.net/gallery/1030407/Anti-Phishing-Posters-for-Yale-2010.

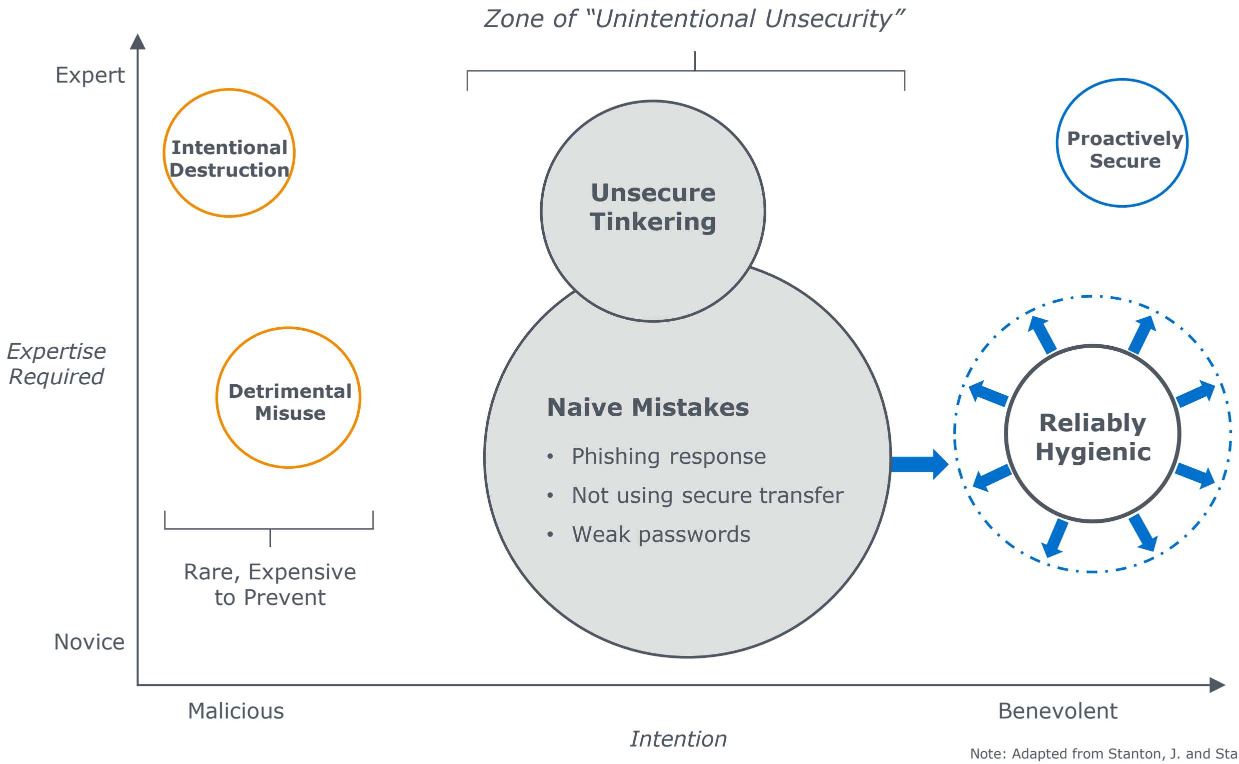
Biggest Opportunity: Elevating Awareness

A Taxonomy of End-User Security Behaviors

Malicious Intent ←	*Unintentionally Unsecure* →	*Secure and Benevolent*
Intentional Destruction Breaks in to protected file	**Unsecure Tinkering** Researcher sets up wireless gateway	**Reliably Hygienic** Changes passwords regularly
Detrimental Misuse Uses email system for spam	**Naive Mistakes** Responds to phishing attack	**Proactively Secure** Reports backdoor desktop program

The vast majority of campus constituents are neither proactive about security nor intentionally trying to harm the institution; most are simply unconcerned or naive about risks; this distribution is an opportunity to improve security through education, as a complement to investment in new technology. Our research identified tactics for moving naive and unaware students, staff, and faculty to reliably secure behaviors.

The Goal of Elevating Security Awareness



Note: Adapted from Stanton, J. and Stam, K.: *Analysis of End-User Security Behaviors*, Rochester, NY, Journal of Computers and Security, 2005.

EAB

Hardwiring Breach Response

PART 1

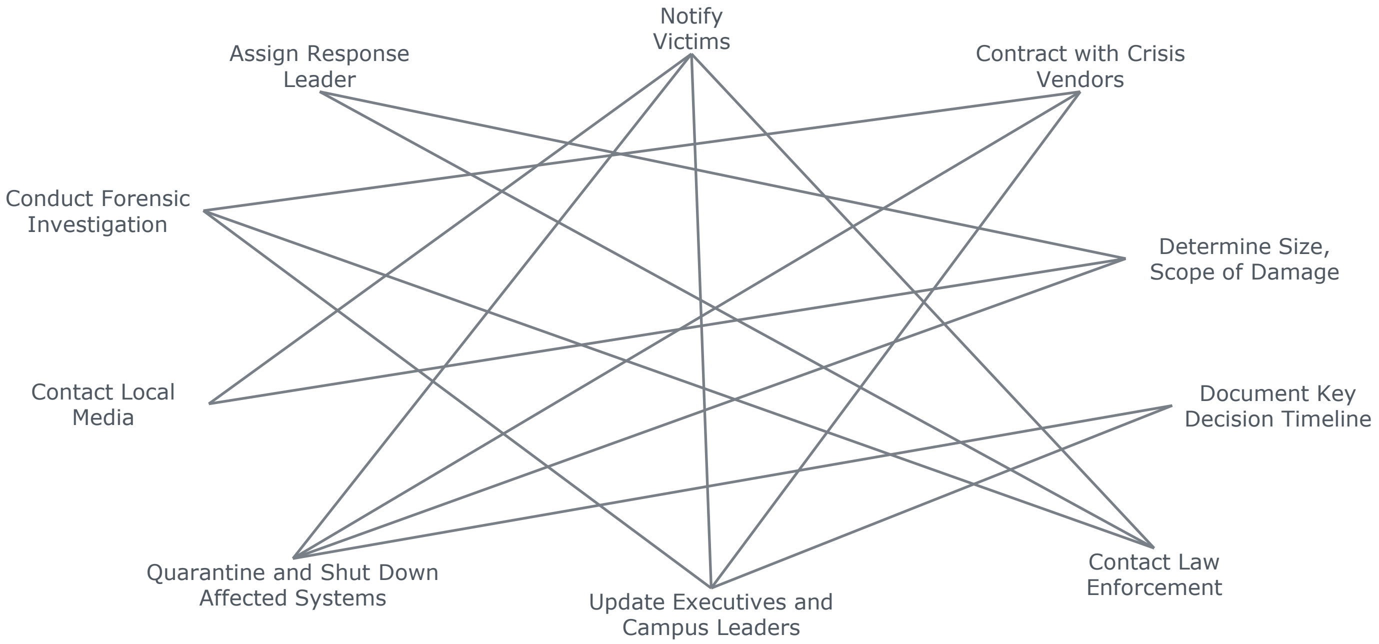
- Practice 1: Incident Managers
- Practice 2: Distributed Application Whitelisting
- Practice 3: Time-to-Response Tracking

Worst of Both Worlds

Increased security awareness on campus can support a more efficient and controlled response, and preparing campus for a breach event will lead to greater awareness of risks and acceptance of necessary changes to policy.

IT teams that have experienced a breach event know that the first hours after incident notification will be hectic and confusing. The institution must organize internal responders, secure systems, contact all appropriate parties, set up crisis services, and collect key data all at once. Without a clear plan and organization in place, mistakes are made.

Diagramming a Breach's Aftermath



Notify Victims

Assign Response Leader

Contract with Crisis Vendors

Conduct Forensic Investigation

Determine Size, Scope of Damage

Contact Local Media

Document Key Decision Timeline

Quarantine and Shut Down Affected Systems

Update Executives and Campus Leaders

Contact Law Enforcement

Big Decisions Too Quickly

- Free credit reports for X years
- Comprehensive security audit of IT systems
- Multiple revisions of breach details in media reports

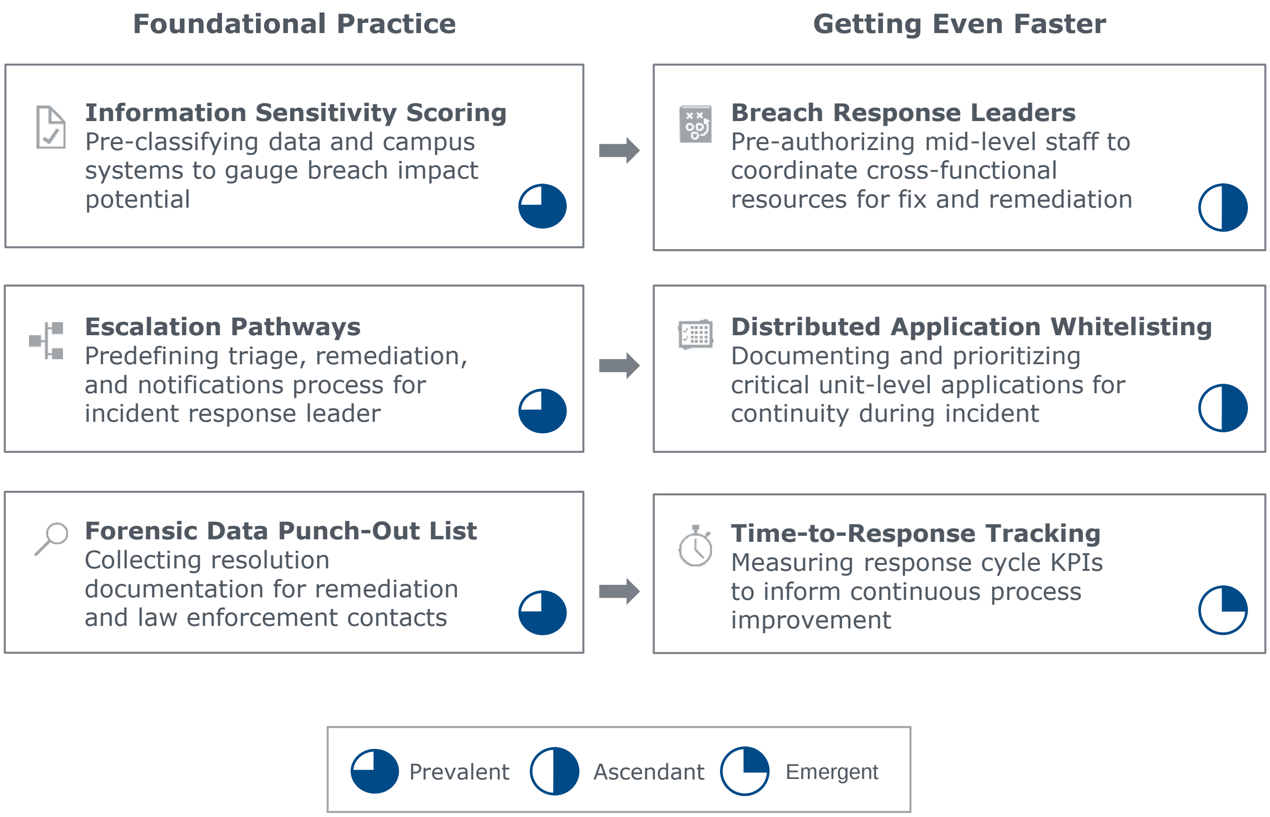
Routine Activities Too Slowly

- Confusion about priority and control of critical systems
- Can't find crisis vendor information
- Duplicative law enforcement requests

Source: EAB interviews and analysis.

Airbrush the Rapid-Response Playbook

Nearly all institutions have conducted basic preparation in segmenting data and assigning ownership over key systems; however, few have made key roles and processes part of their breach response plan. Designating breach response leaders, creating distributed application whitelists, and tracking time to response can help even advanced organizations improve the efficiency and effectiveness of breach response.



Foundational Practice		Getting Even Faster
Information Sensitivity Scoring Pre-classifying data and campus systems to gauge breach impact potential ◕	→	**Breach Response Leaders** Pre-authorizing mid-level staff to coordinate cross-functional resources for fix and remediation ◑
Escalation Pathways Predefining triage, remediation, and notifications process for incident response leader ◕	→	**Distributed Application Whitelisting** Documenting and prioritizing critical unit-level applications for continuity during incident ◑
Forensic Data Punch-Out List Collecting resolution documentation for remediation and law enforcement contacts ◕	→	**Time-to-Response Tracking** Measuring response cycle KPIs to inform continuous process improvement ◔

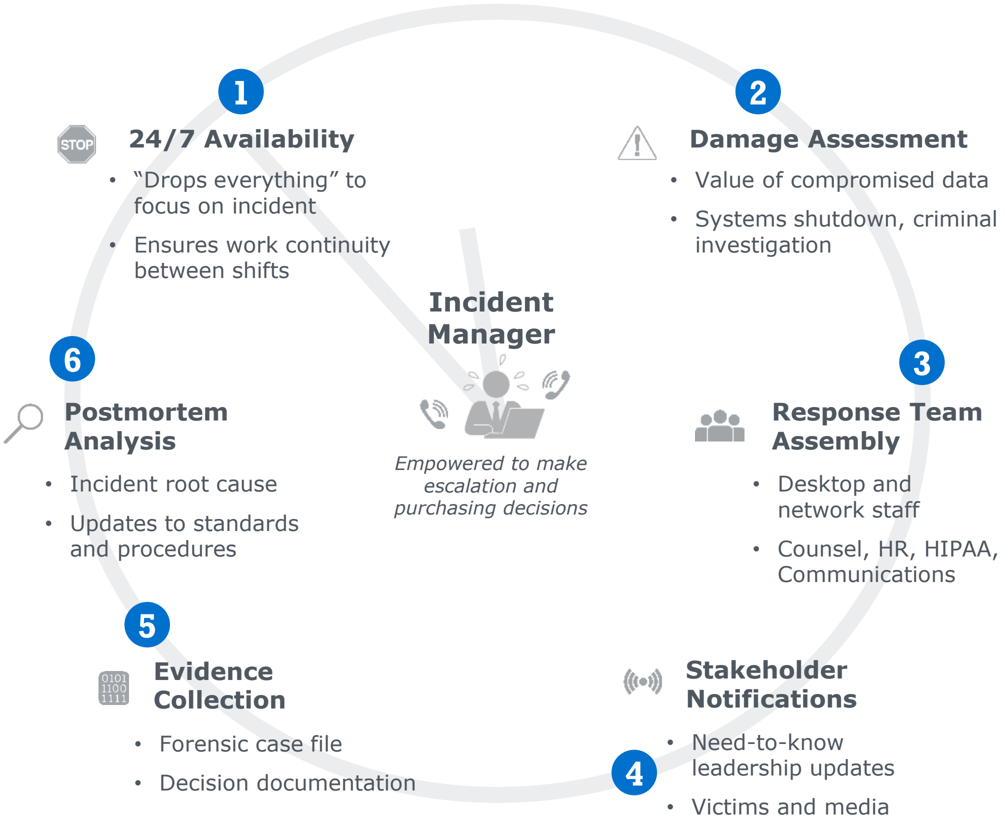
◕ Prevalent ◑ Ascendant ◔ Emergent

Source: EAB interviews and analysis.

Ensure Focus and Authority for Fast Decisions

To make breach response efficient, controlled, and predictable, identify a pool of staff who will be prepared to make escalation, purchasing, and quarantine decisions during a breach. These incident managers oversee the entire workflow around breach response and are responsible for shift continuity, damage assessment, response team assembly, stakeholder notification, evidence collection, and an initial postmortem analysis.

Single Owner Reduces Lag to Access Experts, Notify Stakeholders



Incident Manager

Empowered to make escalation and purchasing decisions

1 **24/7 Availability**
- "Drops everything" to focus on incident
- Ensures work continuity between shifts

2 **Damage Assessment**
- Value of compromised data
- Systems shutdown, criminal investigation

3 **Response Team Assembly**
- Desktop and network staff
- Counsel, HR, HIPAA, Communications

4 **Stakeholder Notifications**
- Need-to-know leadership updates
- Victims and media

5 **Evidence Collection**
- Forensic case file
- Decision documentation

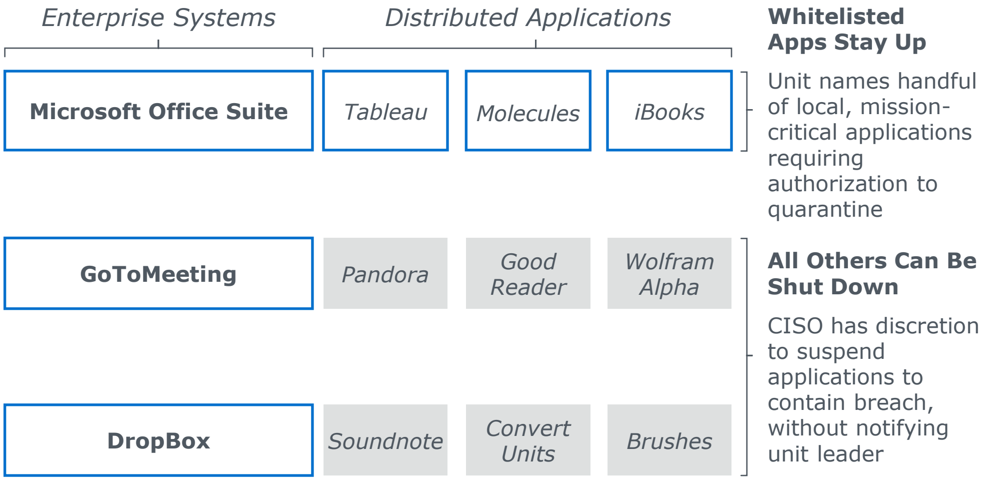
6 **Postmortem Analysis**
- Incident root cause
- Updates to standards and procedures

Source: EAB interviews and analysis.

Pre-wire Unit-Level Containment Decisions

Keep up with critical distributed applications without overburdening the security team by focusing on what will stay on during a breach instead of what will shut down. Compiling a list of top local applications outside of standard, enterprise-wide licenses can ensure continuity in local areas by insulating whitelisted applications from a system quarantine.

Focus on What Stays On Instead of What Shuts Down



Enterprise Systems	*Distributed Applications*		
Microsoft Office Suite	*Tableau*	*Molecules*	*iBooks*
GoToMeeting	*Pandora*	*Good Reader*	*Wolfram Alpha*
DropBox	*Soundnote*	*Convert Units*	*Brushes*

Whitelisted Apps Stay Up

Unit names handful of local, mission-critical applications requiring authorization to quarantine

All Others Can Be Shut Down

CISO has discretion to suspend applications to contain breach, without notifying unit leader

> **Sticking to What We Can Realistically Track**
>
> "Trying to know what every department's up to isn't realistic, and in the middle of a breach it's too much effort to inventory. What we can do is find out in advance what tools faculty and staff need to do their jobs, so we can keep the important stuff running."
>
> *CISO, Public Research University*

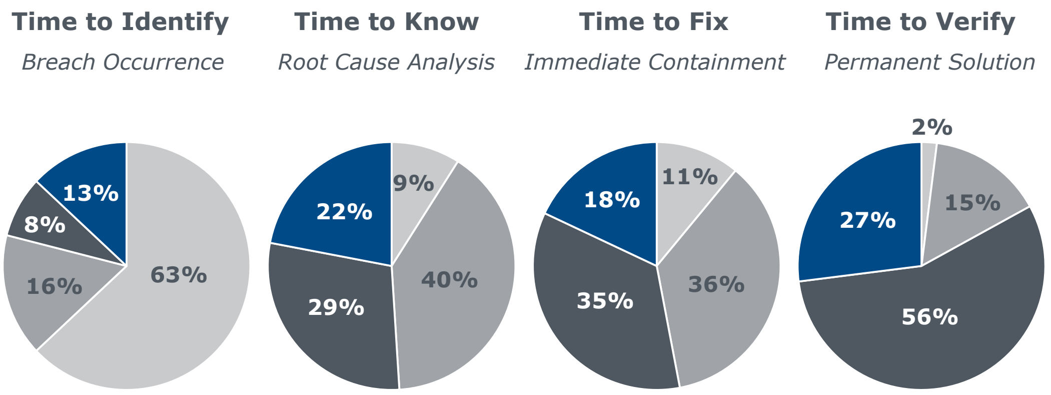
Note: Application examples are illustrative only.

Source: EAB interviews and analysis.

Measure Response to Reduce Breach Costs

Operational efficiency during a breach is a significant driver of indirect expenses. To save on breach costs, improve the time to know a breach has occurred, understand root cause vulnerability, contain damage, and create a permanent solution. Comparing granular performance metrics of breach response to set benchmarks allows identification of areas for improvement and discovery of how different data and parts of campus respond differently to security incidents.

Document Process Performance to Streamline Response



⬜	Hours
▨	Days
■	Weeks
🟦	Months

Parsing the Data

- *Are we getting faster?*
- *Are responses in some units slower than others?*
- *How does response time vary by information class?*

Compare performance metrics at the level of data type (e.g., FERPA versus HIPAA) and unit type (e.g., academic department versus administrative office) to prioritize remediation at the level of process and understand where the "indirect" costs of data breaches are clustered.

Representative Uses of Granular Time-Based Metrics

Data Type	Identify	Know	Fix	Verify	Recommendation
PCI*	15 Minutes	1.2 Hours	4 Hours	1 Day	**Controls Working Well** Continue monitoring activity for improvement
HIPAA*	1.4 Hours	7 Hours	8 Hours	1 Week	**Targeted Intervention** Rapid fix once cause discovered; focus on faster root-cause analysis
FERPA*	5 Days	2 Weeks	2 Months	Unknown	**Needs Significant Work** Process redesign and retraining may be necessary for unit IT

- Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA)
- Note: Performance benchmark examples are illustrative only.

Source: Ponemon Institute, "Cyber Security Incident Response – Are we as prepared as we think?", 2014.

EAB

Making Risks Relevant

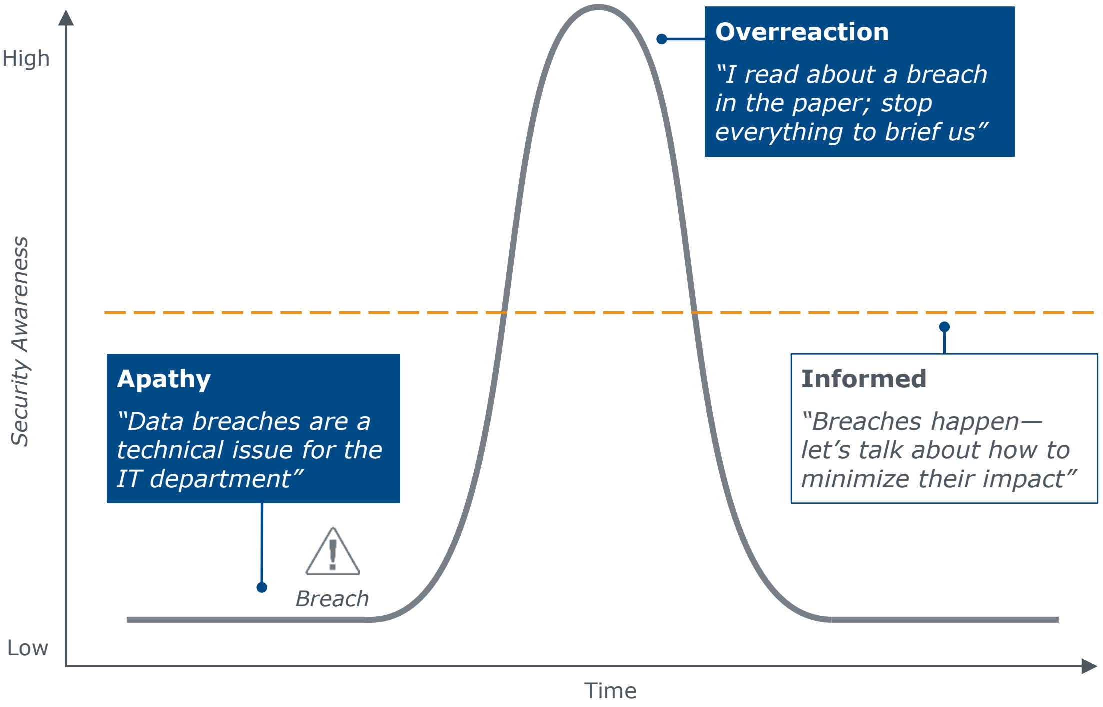
PART 2

- Practice 4: Board Education Memos
- Practice 5: Unit-Level Risk Profiles
- Practice 6: Personal Risk Audits

Infrequent Board Exposure to Security Issues

Security awareness among executives and boards tends to spike when mainstream media covers an incident or the institution suffers an attack, but some leaders may also misunderstand data security as a technical issue that is controlled by the IT function. CIOs and CISOs struggle to keep leadership engagement at an appropriate, constructive level that acknowledges the possibility of data losses and seeks the best ways to minimize the impact and cost of incidents.

Struggling to Keep Leaders at Appropriate Security Awareness Level



Overreaction

"I read about a breach in the paper; stop everything to brief us"

Apathy

"Data breaches are a technical issue for the IT department"

Informed

"Breaches happen—let's talk about how to minimize their impact"

Source: EAB interviews and analysis.

Ripped From the Headlines

At Brown University, the CISO takes news stories about data breaches and converts them into one-page education memos that the CIO distributes to the cabinet and board. Incidents that involve a real campus vulnerability or those that affect Brown directly are prioritized, but the CISO also writes memos (primarily for the president and provost) when peer institutions are affected and when breaches receive media attention in mainstream publications that trustees are likely to read.

Turning Mainstream News into Education Opportunity

"Target Now Says 70 Million People Hit in Data Breach"

-Wall Street Journal

Breach Memo TARGET

Summary: WSJ reports Target lost 70M customer records

Vulnerability: Vendor control, systems access

Impact: Millions in costs, loss of goodwill, share price decline

Protections: Agreements with vendors in critical systems

Exposure: Complete knowledge about all vendors?

Takeaway:

Not a Big Risk

"Data Breaches Put a Dent in Colleges' Finances as Well as Reputations"

-Chronicle of Higher Education

Breach Memo UNIVERSITY OF MARYLAND

Summary: Chronicle covers UMD data breach of 300,000 records

Vulnerability: External collaboration website, data storage

Impact: Millions in credit monitoring, reputation damaged

Protections: Data destruction policy, network monitoring

Exposure: Consistent campus adherence to collaboration rules?

Takeaway:

This Could Happen to Us

Brown's focus on getting relevant information to leaders as events occur saves time by keeping executives and trustees up to date, and also achieves a goal set by many CIOs: make sure executives are appropriately informed and educated about security, and approach new funding and initiatives proactively.

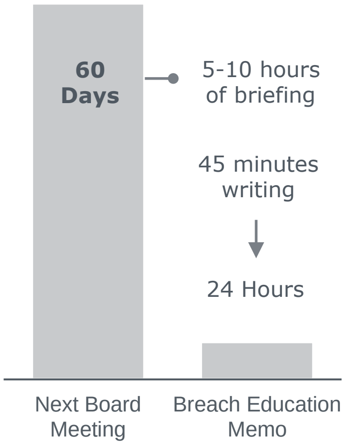
Proactive Education Keeps Focus Strategic, Not Reactive

Case Study: Getting Ahead of the Shellshock Bug

Shellshock

- Undetected bug goes live across millions of devices
- Student Macs vulnerable to malicious use
- Multiple rounds of patching and updates from central IT

Time to Brief Leadership



More Productive, Proactive Security Discussions

"Now, when we go to the cabinet with updates to our budget and requests for new protections, we don't have to start education from zero—we can immediately have an informed conversation about what needs to change in terms of security."

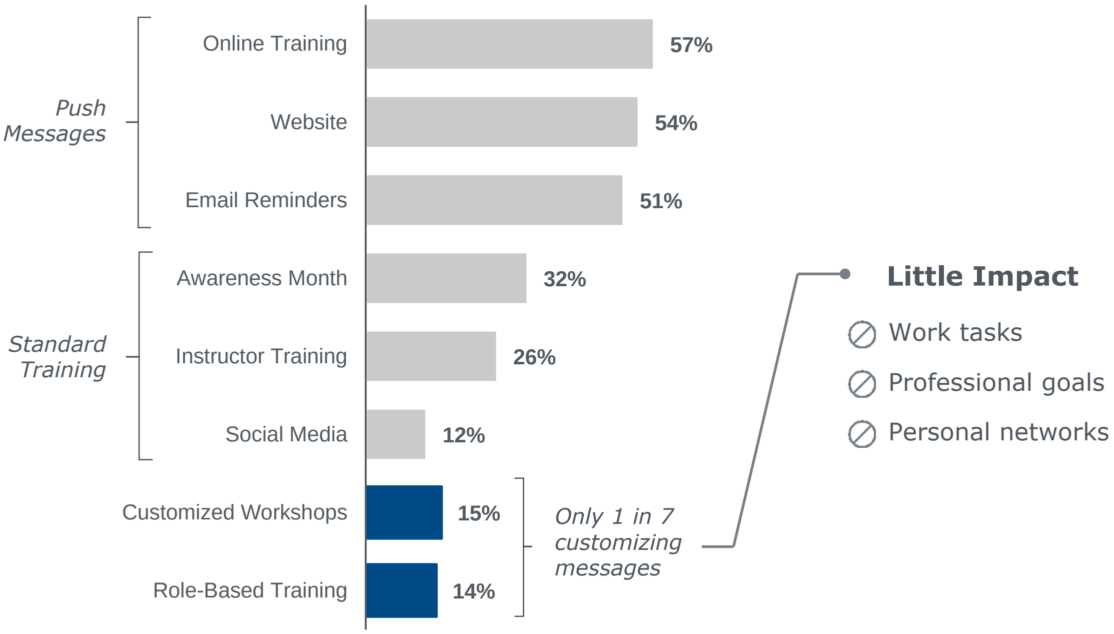
David Sherry
CISO, Brown University

Source: EAB interviews and analysis.

Not Investing in Tailored Awareness Education

Institutions use myriad channels to broadcast security messages across campus, but most communication is untargeted and unrelated to the personal priorities that drive end-user behavior; only one in every seven institutions customizes security messages through tailored workshops and role-based training. While push messages and standard training might reach all campus audiences without large expense, ineffective messaging can distract end users from important lessons and does little to enhance security.

Few Institutions Tailoring Education for End Users



Security's Posterization

"Sure it's cheap to hang up posters everywhere. But no one thinks it does much. And it keeps us from trying the kinds of targeted messaging that might do more good."

CIO, Public Research Institution

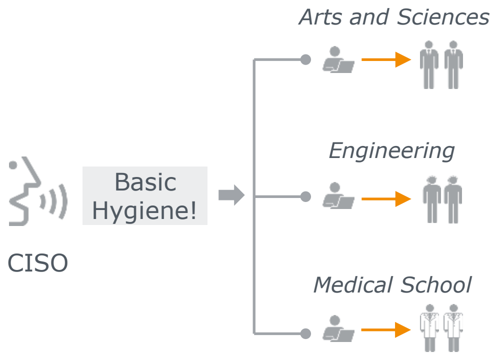
Source: McElroy, L. and Weakland, E. : Measuring the Effectiveness of Security Awareness Programs, EDUCAUSE Center for Analysis and Research, 2013. https://net.educause.edu/ir/library/pdf/ERB1310.pdf

Framing Policies in Terms Users Understand

When ordering units to comply with security policies in the abstract, IT typically invokes generic risks and institutional consequences. Before engaging with departments, ask for details about local projects involving data and devices that present risks. CISO meetings with academic departments will be more focused and productive when constituents discuss real department-level vulnerabilities.

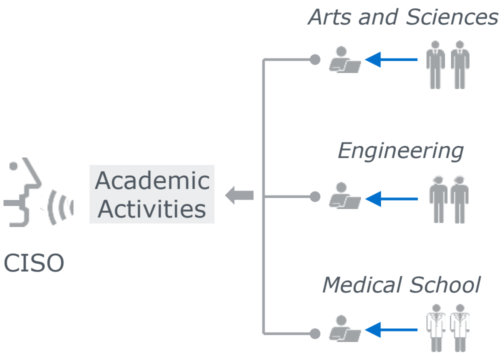
Work with Unit-Based IT to Itemize Academic Activity

CISO Exhorts Unit IT to Get Academy to Comply



- Local check-ins focus on messaging generic vulnerabilities
- Consequences described at institutional level

CISO Asks for Insight into High-Profile Academic Activity



- Check-ins focus on understanding academic research, scholarship, and collaborations
- CISO tailors risk messaging around project-specific vulnerabilities

Help end users understand the potential risks of data breaches by describing risks and potential consequences in the context of projects and missions close to academic and professional goals. A conversation tailored to concrete department activity will gain greater attention and long-term compliance than a presentation focused on generic institutional consequences.

Make Abstract Risks Relevant to Academic Goals

Security Profile: Medical School

Local Project	*Risk*	*Local Consequence*	*Vulnerability Check*
Federally funded study on medical device surgical impacts	**Grant Funding**	NIH requires payback of funds already spent	✓ *Data Management Plan* ✖ *Vendor Access* ✓ *Software Patching*
Longitudinal health outcomes data stored on flash drive	**Lost Data**	Research invalidated if data lost or tampered with	✓ *HIPAA Compliance* ✓ *Device Tracking* ✖ *Device Encryption*
Cutting-edge textbook on interventional radiology methods	**Pirated Scholarship**	Hackers steal textbook, post on Internet for free	✓ *Changing Passwords* ✖ *Strong Passwords* ✓ *Secure Data Transfer*
Pharmaceutical experiments conducted with international partners	**Risky Collaborators**	Devices connected to networks in China routinely compromised	✖ *Remote Mobile Wipe* ✓ *Mobile Containerization* ✓ *Email Encryption*

Source: EAB interviews and analysis.

Security Begins at Home

To raise the profile of cybersecurity on campus at Rochester Institute of Technology, staff converted existing security modules for students, faculty, and staff into a unit organized around "personal self-defense" rather than institutional protection. The focus of six in-person or online modules is how individuals can protect themselves in the course of their digital activity, and it is positioned as a service rather than a compliance responsibility.

A Personal Security Mini-MOOC

Digital Self-Defense Modules

- Passwords
- Patching
- Anti-Virus
- Firewall
- Spyware
- Physical Security

How Threats Work
Securing Devices
Spotting Adversaries

Self-Quiz

Key Facts

- Online curriculum developed by Security Manager
- Self-paced modules with self-quizzes
- Links to university, vendor, and government resources

After offering personal risk audits first for administrative staff through in-person courses, the IT team at RIT expanded the modules across campus. Today, the IT team offers self-defense services to incoming students, slots modules into onboarding for new faculty and staff, and will present in-person for a private department audience at the request of local administration or IT leaders.

Embedded in Orientation and Onboarding

New Student Orientation

90-minute session with incoming freshmen on personal security

New Employee Onboarding

Staff directed to Digital Self-Defense during desktop and email provisioning

On-Demand Teach-Ins

Managers request presentations to unit if persistent risky behaviors identified

Source: EAB interviews and analysis.

Tie Personal Habits to Institutional Policies

The key to the success of personal risk audits is that secure personal behavior is linked directly to institutional policy. Each module in the digital self defense course finishes with an explanation of campus policy, and reasons why additional controls are necessary to protect sensitive institutional data.

Self-Defense Practices Match University Policy

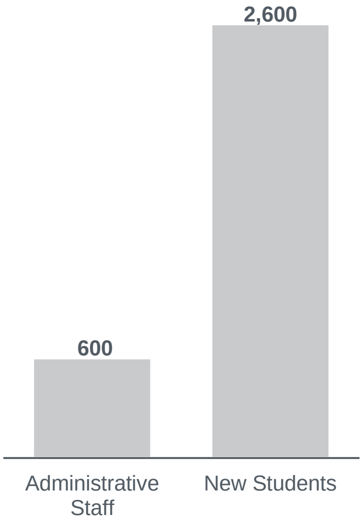
	Passwords	Patching	Spyware	Phishing
Securing Yourself	Use complex passphrases Vary usernames and passwords across accounts	Activate Windows auto-updates Weekly check for application updates	Confirm URLs and attachments Task manager for unfamiliar programs	Requests to "confirm" information Knockoff and masked URLs
Ties to Institutional Policy	Minimum complexity and automatic sunsets	Patch personal applications on work devices	Report suspicious URLs and attachments	RIT emails **never** request account information

Phishing attacks have increased across higher education in the last decade, and RIT has seen the volume and sophistication of attacks grow. However, the average number of campus constituents who fall for a phishing email (i.e., those who click on a link or reply) has dropped by 80% since the introduction of digital self-defense courses. Hygienic habits that support safe personal computing stay "on" when students, faculty, and staff come to campus.

Hygienic Habits Are "Always-On"

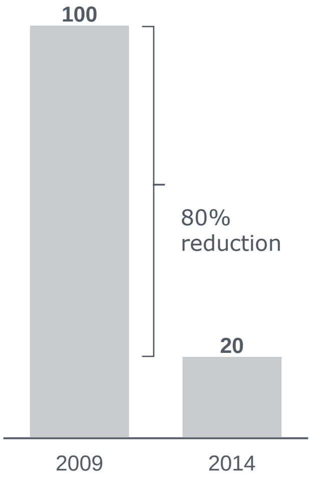
A Bigger Footprint

More Campus Constituents Trained



More Sophisticated Users

Fewer Victims per Phishing Attack



Proactive Alerts to CISO

2009 **Strange Email** "This doesn't look like my normal bank message"

2014 **Possible Malware** "I don't know why that program would use so much memory"

Source: Digital Self-Defense, http://www.rit.edu/security/tags/digital-self-defense.

EAB

Demonstrating Vulnerability

PART 3

- Practice 7: Vulnerability Consultations
- Practice 8: Security Scorecards
- Practice 9: Demonstration Hacks
- Practice 10: Self-Phishing

Repurposing Monitoring Data for Awareness

Non-technical staff may have trouble understanding why cyber risks affect them; leverage the data already collected through audit committees, penetration testing, phishing analysis, and tools like data loss prevention (DLP) to demonstrate real vulnerability and engage end users more effectively.

See Tool 1 in the appendix (page 56) for a compendium of key performance indicators for security awareness.

Numerous Sources of Potential Security Awareness Data

Audit Committee Frameworks

Campus-wide information risk assessments are kept for CISO and board eyes only

Penetration Testing

Compliance with PCI and HIPAA requires some testing, with results delivered in highly technical, IT-facing format

Phishing Postmortems

Successful external phishes compromise accounts and devices regularly, but IT rarely self-phishes to build immunity

DLP Tools

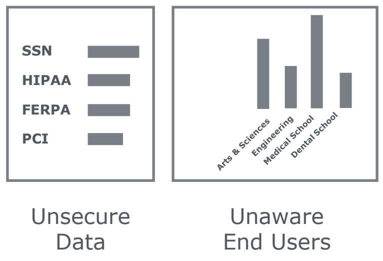
Email scanning and blocking software engaged to stop data loss with minimal education or explanation to units

A DLP tool monitors data transfers such as email for information that could be sensitive (e.g., a nine-digit code that could be a Social Security number) and can block outgoing communications. To make the most of a DLP investment, the CISO at Texas State University kept the tool in learn mode for six months, to discover where on campus sensitive information was moving and pinpoint root causes of unsecure behavior.

Making the Most of Monitoring Tools

TEXAS STATE UNIVERSITY SAN MARCOS

Email Traffic Analysis



Establishing Baselines for Unsecure Data Transfer

- Nature
- Volume
- Timing
- Source

Getting Our Message Straight

> "We wanted to understand why people send risky emails. Do they not know the data's sensitive? Do they really need to send this data? The baseline helped calibrate our message—if we had just started blocking out of the blue, it wouldn't have had any impact."
>
> *Former CISO, Texas State University*

Source: EAB interviews and analysis.

Using DLP to Fine-Tune Security Outreach

Analyzing the DLP information, Texas State's CISO visited unsecure departments one by one to discuss security rules and implement specific fixes for unsecure data transfers. The appropriate intervention is a factor of data type, location, and root cause; the CISO used a combination of campus-wide emails, one-on-one meetings, and process redesign to prevent the risky behavior identified through DLP monitoring.

Calibrating Interventions with Monitoring Data

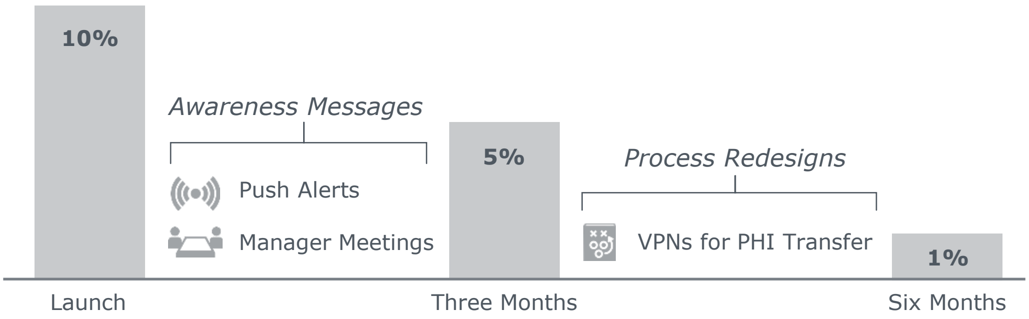
Unsecure Data	Location	Root Cause	Intervention
Social Security Numbers	Entire Campus	W-2 forms emailed during tax season	**Annual Reminders**: April email alerts linked to secure transmission instructions
Personal Health Information	Medical Center	PIs sending patient notes to personal accounts	**Manager Meeting**: CISO meets with Medical Center Director and PIs
PHI and Financials	Medical School	Staff finds encrypting data too cumbersome to perform daily tasks	**Process Redesign**: IT funds secure VPN facilitating safe, convenient traffic

Monitoring (Unsecure Data, Location) — *Analysis* (Root Cause) — *Remediation* (Intervention)

DLP analysis allowed the CISO to focus valuable in-person conversation time on departments where there were real, recognizable issues. Bringing actual data of vulnerability focused and grounded discussion. Using real data to prioritize interventions paid off; within six months, the percentage of emails containing sensitive data decreased by 90%.

A 90% Decrease in "Bad" Emails

Percentage of Emails Containing Sensitive Data



Making the Most of Our Resource-Intensive Interventions

"Everyone agrees face-to-face meetings and tailored trainings are the most effective awareness levers. But no one has enough time to do them with every unit or individual across campus. This approach allows us to 'spend' that resource in the way that's most likely to resolve ongoing risks, and measure the impact once we're done."

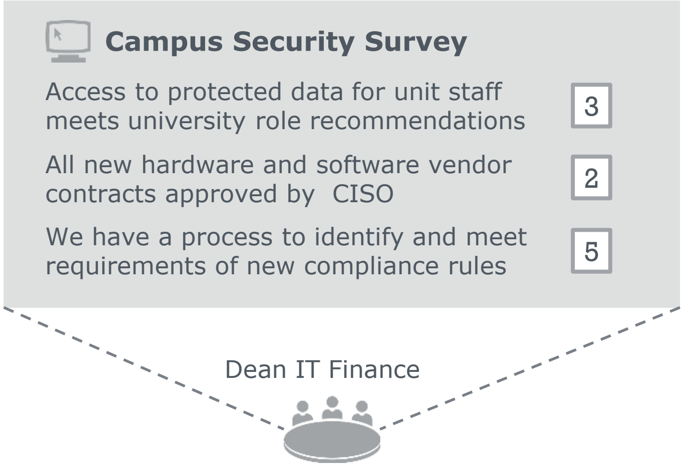
Former CISO, Texas State University

Source: EAB interviews and analysis.

Making the Most of Required Board Reporting

When the board of trustees at Ohio State University sought increased reporting from IT, the CISO developed a simple self-grading survey mechanism for campus. The annual survey is based on a standard National Institute of Standards and Technology (NIST) framework, with 100 questions developed in cooperation with campus experts (e.g., general counsel). The local academic, finance, and IT leaders are required to sign off on scores before the survey is sent back to the CISO.

A Bottom-Up Summary of Risks for the Board



Campus Security Survey

Access to protected data for unit staff meets university role recommendations 3

All new hardware and software vendor contracts approved by CISO 2

We have a process to identify and meet requirements of new compliance rules 5

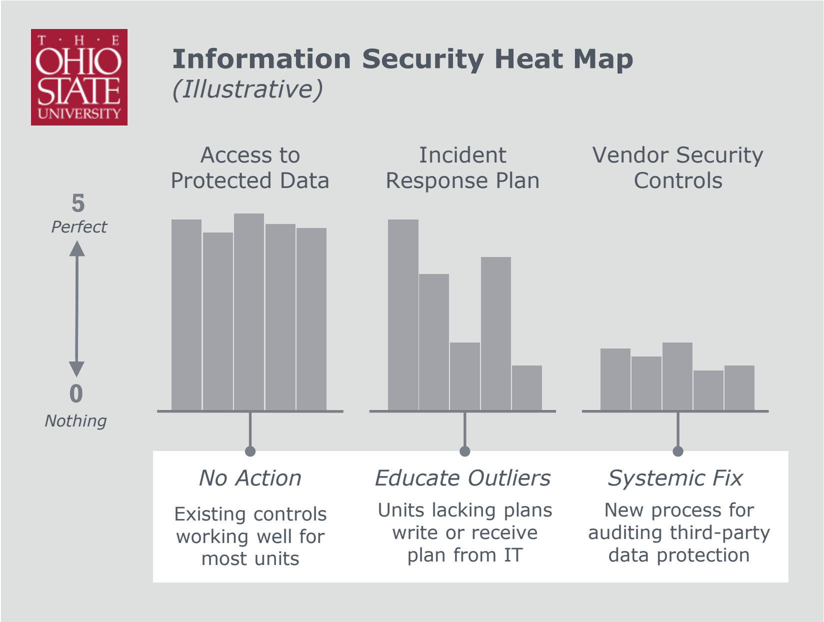
Dean IT Finance

How Are We Doing?

- 160 "auditable" units
- 30 risk categories, 100 self-ratings
- Academic, business, and IT directors must sign off

For the board of trustees, the CISO builds a university-wide heat map with 160 columns representing units and 30 rows representing risk areas. The board can easily identify which categories have security controls that are working well, where there are outliers that need additional help, and where problems across campus could prompt a systemic fix.

Security "Heat Map" for Board of Trustees



Information Security Heat Map *(Illustrative)*

No Action
Existing controls working well for most units

Educate Outliers
Units lacking plans write or receive plan from IT

Systemic Fix
New process for auditing third-party data protection

Source: EAB interviews and analysis.

Scorecards Show Units’ Relative Security

To maximize the impact of campus surveys and help units understand their own vulnerability, the CISO produces department-level scorecards that compare units to peers (e.g., academic departments, research centers) and the institution as a whole. The scorecards help local academic and finance staff set benchmarks for improvement, understand peer comparisons, and identify key areas for remediation in the coming year.

See Tool 5 in the appendix (page 74) for advice on how to implement security scorecards on campus.

No One Wants to Be Last

Department Security Scorecard

	Your Unit	*Units Like You*	*Institution*
Data Management			
Information Classification	4.3	3.6	3.2
Archiving and Destruction	**3.5**	3.8	2.9
Incident Management			
Response Leaders	**1.5**	**3.6**	2.7
Business Continuity	3.2	3.1	2.8
Applications and Devices			
Malicious Software Monitoring	2.8	2.9	3.1
Mobile Development	**2.1**	**2.4**	**3.2**

Annual Awareness Briefings

Are We Improving? Longitudinal trends show correction of identified risks

Are We Lagging Peers? Humanities with humanities, STEM with STEM, administrative with administrative

Are We Far Outside Norms? Units and peers lagging reasonable “hygiene” security expectations

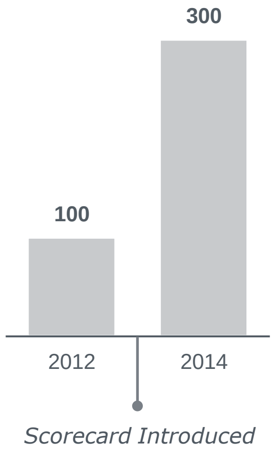
Attention from the board and new visibility into risks for business and academic leaders has already generated positive results for Ohio State. In its second year, the survey gained 100% participation from units, and instead of pushing units to accept cybersecurity policies, there is overwhelming department demand for CISO involvement with security consultation and policy writing.

Visibility Sustains Engagement

100% Participation

> “We told units we couldn’t force them to participate in the surveys and scorecarding, but we’d report on who wasn’t participating to the trustees. No one wants to be the department in front of the board for not playing ball.”
>
> *Helen Patton*
> *CISO, Ohio State University*

CISO “Teach-In” Attendance



Security Consultation Requests

Asset Tracking
Initiate tracking of devices under $5,000

Response Plans
Import existing roles and policies from similar unit

Vendor Screening
Procurement vets data for security in RFP process

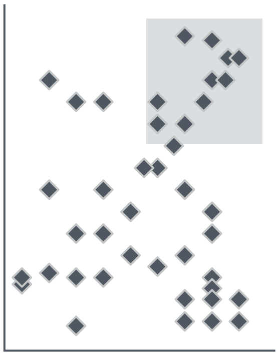
Source: EAB interviews and analysis.

A Warning Units Can't Ignore

While most leaders are practical about risks and willing to take guidance from the CISO on how to protect data, CIOs suggest that sometimes more drastic action is needed. At one large, public university, the CIO partners with a private- sector firm annually to scan the institution's network for vulnerabilities. The riskiest quintile is composed of IP addresses in departments with historically poor risk management, and the IT team guides the vendor toward demonstrative penetration tests that will make an impact with unit leadership.

Vividly Illustrating "This Could Happen to You"

1 Identify Riskiest Quintile



2 Rank Vulnerabilities in Top 20% IP Ranges

3 Design Demonstration Hack

- ⚠ Change Grades
- ⚠ Remove Salary Information
- ⚠ Pirate Research Publication

While non-technical staff might not understand the complexity of information security risks, a visual demonstration of real vulnerability to mission-critical priorities will generate action and new attention to risk mitigation. Demonstrations should be extremely private and non-punitive; the conversation around vulnerability is a valuable teaching moment for deans and administrators previously unfamiliar with new cyber-threats.

Targeted Hacks Show Dangers to "Local" Data

	Academic Dean	**Administrative Director**	**Center Director**
	C+ → A+	Routing Number XXXXXXX	
You Are Vulnerable	*"We were able to change a grade in five minutes"*	*"Paychecks for your employees could be diverted"*	*"Data on your patients are at risk of release"*
Here's How to Protect Yourself	Schedule reminders for patching servers	Secure data transfer training	Encryption tools and services

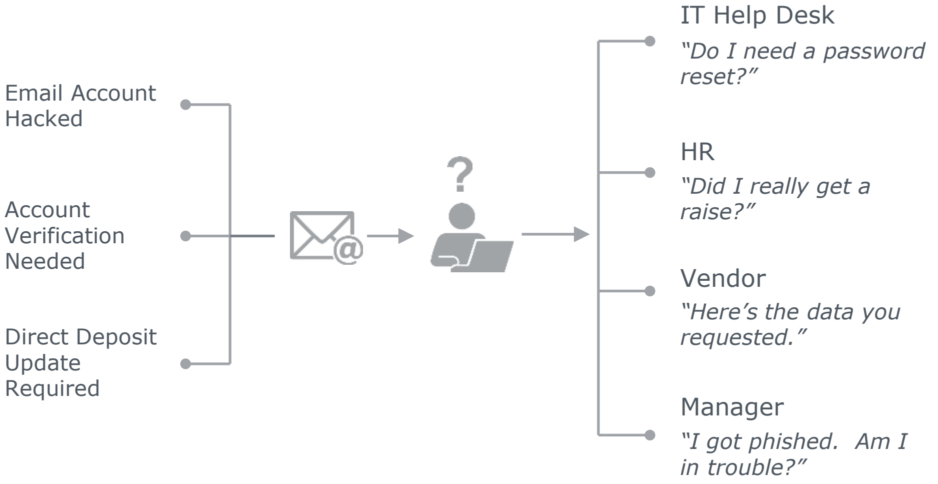
Source: EAB interviews and analysis.

Pre-wiring Is the Key to Self-Phishing Success

Self-phishing is a controversial tactic for many CIOs and their teams, and for good reason: a self-phishing campaign sent out without notification of end users and key stakeholders can cause confusion, anger, and wasted time across campus.

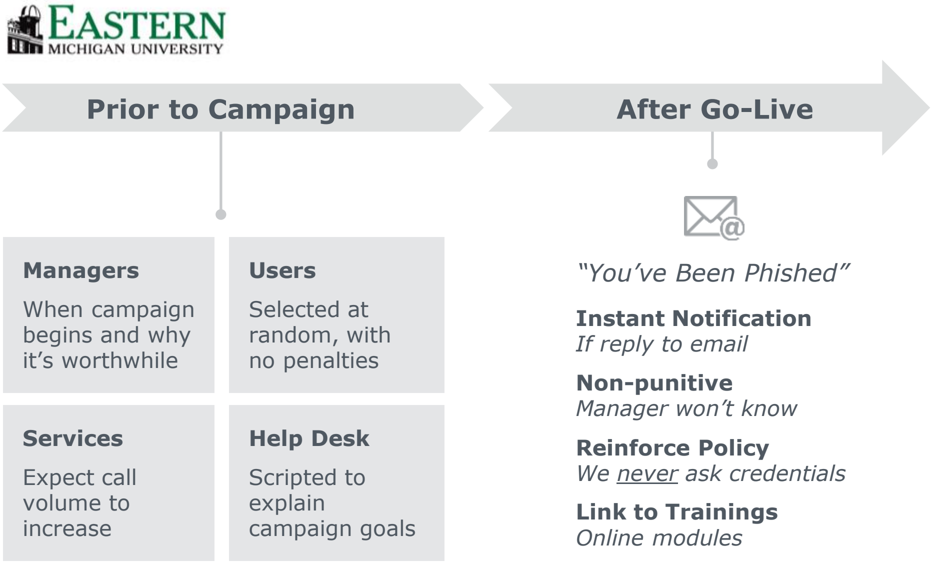
Great in Theory, Distracting in Practice

"Stealth" Self-Phishing Courts Time-Consuming Confusion


Email Account Hacked
Account Verification Needed
Direct Deposit Update Required
?
IT Help Desk
"Do I need a password reset?"
HR
"Did I really get a raise?"
Vendor
"Here's the data you requested."
Manager
"I got phished. Am I in trouble?"

Successful self-phishing begins with extensive pre-wiring that clarifies the intention, scope, and ramifications of the campaign. The core message for all those affected by self-phishing is that the campaign is a service on behalf of campus to protect their data and the institution, not an attempt to expose or punish users that may be vulnerable.

Targeted Preparation Maximizes Campaign Benefits



Managers
When campaign begins and why it's worthwhile

Users
Selected at random, with no penalties

Services
Expect call volume to increase

Help Desk
Scripted to explain campaign goals

"You've Been Phished"

Instant Notification
If reply to email

Non-punitive
Manager won't know

Reinforce Policy
We never ask credentials

Link to Trainings
Online modules

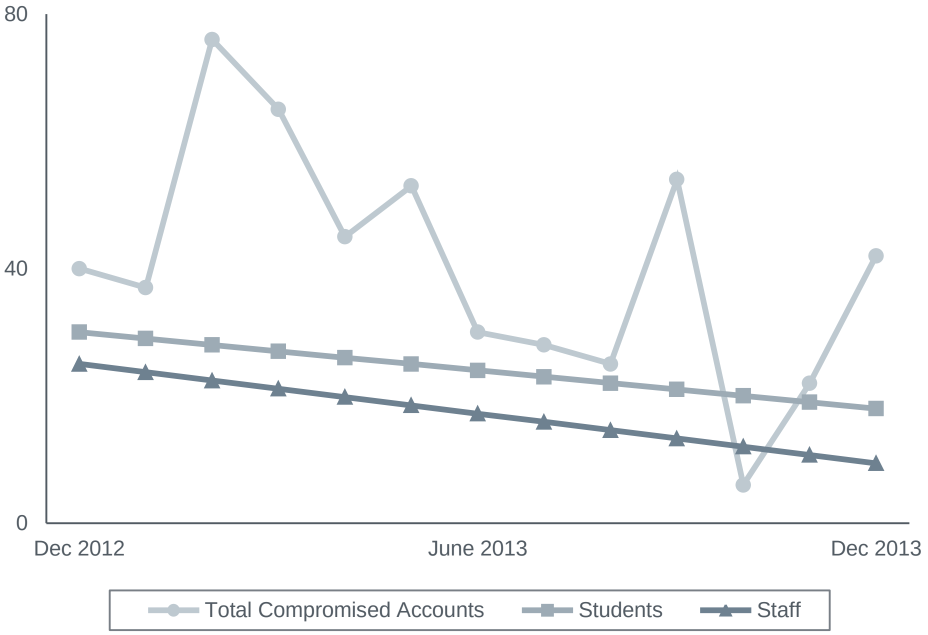
Source: Driving Phishing Awareness on Campus, http://www.eab.com/research-and-insights/it-forum/studies/2014/driving-phishing-awareness.

Moving in the Right Direction

At Eastern Michigan University, effective pre-wiring with campus partners before the self-phishing campaign helped reduce the account compromise rate month over month for students and employees, delivering real savings to the IT help desk and internal units. Rather than the campaign meeting with campus opposition, the IT team found that staff and faculty were gratified to learn about their vulnerability and wanted to know how they could be safer in the future.

Students and Faculty Better Prepared After Being Self-Phished

Accounts Compromised per Month



Hug-Worthy?

"One colleague walked up to me outside and hugged me. She said she thought she was insulated from phishing attacks and understood them, until she got caught."

Rocky Jenkins
IT Director, Eastern Michigan University

Source: Summary Report: Cyber Security Awareness Committee 01/15/2015, http://www.emich.edu/it/security/initiatives/cybersac/reports/summary_report.pdf; Driving Phishing Awareness on Campus, http://www.eab.com/research-and-insights/it-forum/studies/2014/driving-phishing-awareness

EAB

Incentivizing Secure Practices

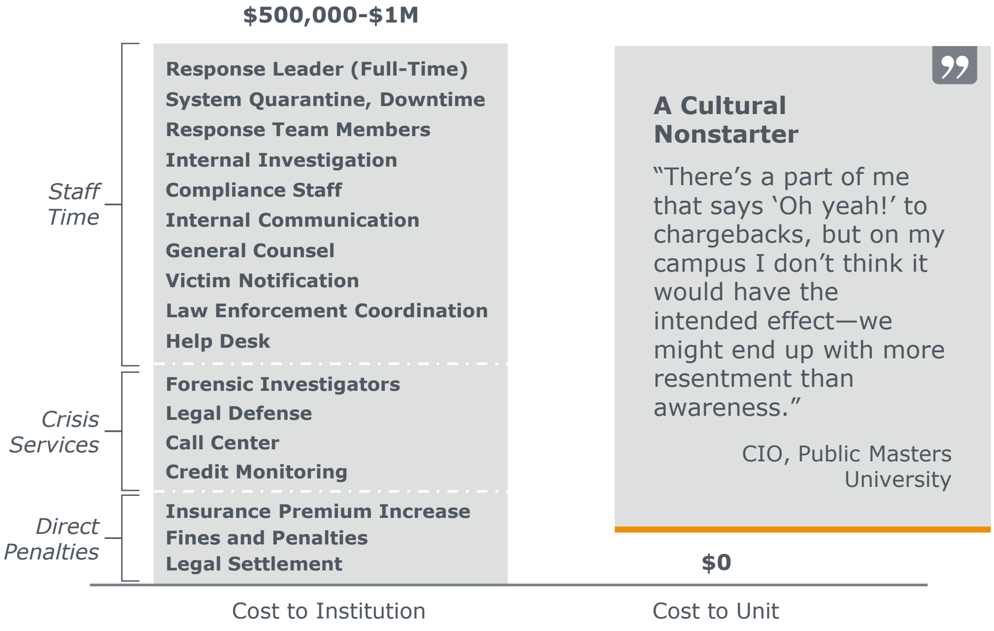
PART 4

- Practice 11: Breach Chargebacks
- Practice 12: Cyber Risk Mitigation Incentives

Breach Costs Largely Invisible to End Users

Even as data breaches have increased in severity and frequency across higher education, managers outside of central IT have stayed mostly immune to the consequences. A dean who is engaged in cybersecurity will be a strong ally for the IT security team, but simply charging departments a penalty for security breaches could generate significant tension between IT and the academy.

Charging Back Remediation to Units Almost Unheard Of



$500,000-$1M

Staff Time
- Response Leader (Full-Time)
- System Quarantine, Downtime
- Response Team Members
- Internal Investigation
- Compliance Staff
- Internal Communication
- General Counsel
- Victim Notification
- Law Enforcement Coordination
- Help Desk

Crisis Services
- Forensic Investigators
- Legal Defense
- Call Center
- Credit Monitoring

Direct Penalties
- Insurance Premium Increase
- Fines and Penalties
- Legal Settlement

$0

Cost to Institution | Cost to Unit

A Cultural Nonstarter

"There's a part of me that says 'Oh yeah!' to chargebacks, but on my campus I don't think it would have the intended effect—we might end up with more resentment than awareness."

CIO, Public Masters University

At Purdue University, breach chargebacks are not intended to punish misbehavior, but rather to provide deans and administrators with a clear reason to adhere to reasonable security standards. Engaging academic administrators through chargebacks allows the CIO to deliver education to the person with most relevant authority, in the language they best understand.

Breach Chargebacks Get Deans Listening and Talking

Gerry McCartney

System Chief Information Officer and VP for Information Technology

Purdue University

"Why are chargebacks worth the uncomfortable conversation?"

Deans Listen When Budget Involved

"People don't care if the CIO gets mad; they care about laws and regulations, but they really come to attention when they have to pay for the consequences."

Riskiest End Users Listen to Deans

"Academic faculty can feel immune to consequences if there is only IT sending the message—a dean is someone they can't ignore."

Deans Talk to Each Other

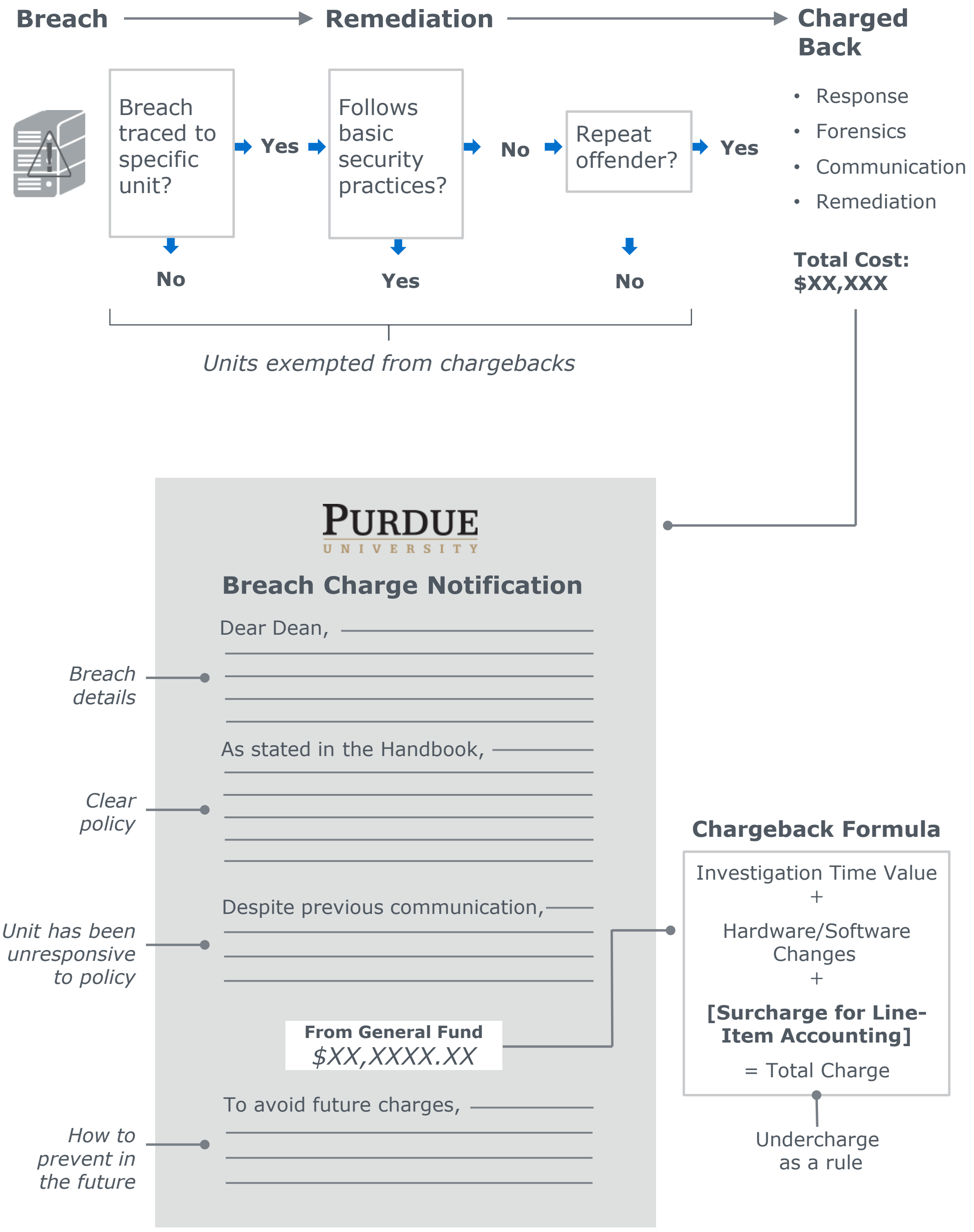
"Once the word gets out you don't need to do additional education; the informal networks in the academy are far stronger than a memo from your office."

Source: EAB interviews and analysis.

Use Breaches As Education Opportunity

Breach chargebacks are not intended to recoup the true costs of a data breach; instead, use the incident as an opportunity to educate responsible managers (e.g., academic deans) about what happened, why it is necessary to improve behavior, and how to prevent future incidents. A simple letter explaining the breach cause, campus policy, previous reminders, and explanation of future prevention should accompany the bill for academic departments, and the CIO should also offer to meet in person to discuss the charge.

Go for Signal Value, Not Cost Recovery



Breach Charge Notification

Dear Dean,

As stated in the Handbook,

Despite previous communication,

From General Fund
$XX,XXXX.XX

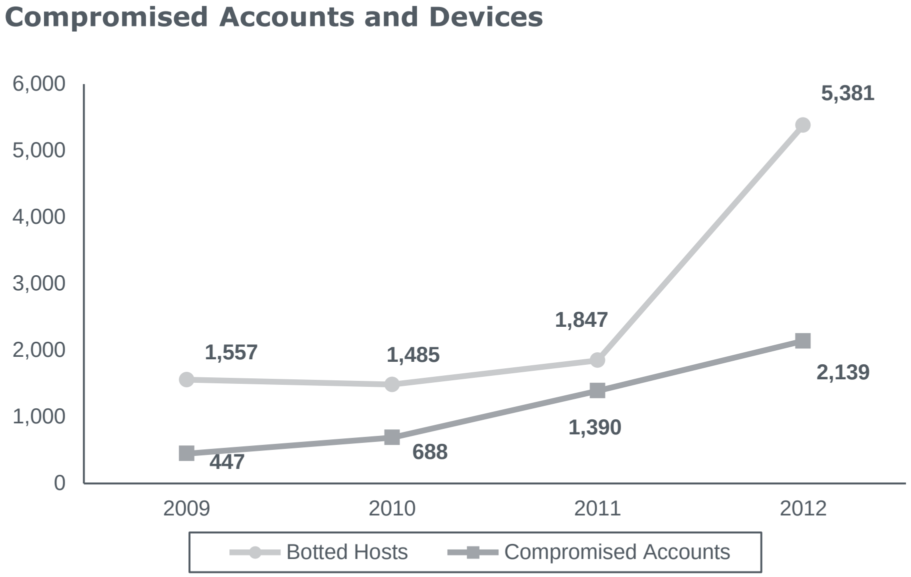
To avoid future charges,

Source: EAB interviews and analysis.

Distributed Systems at Risk

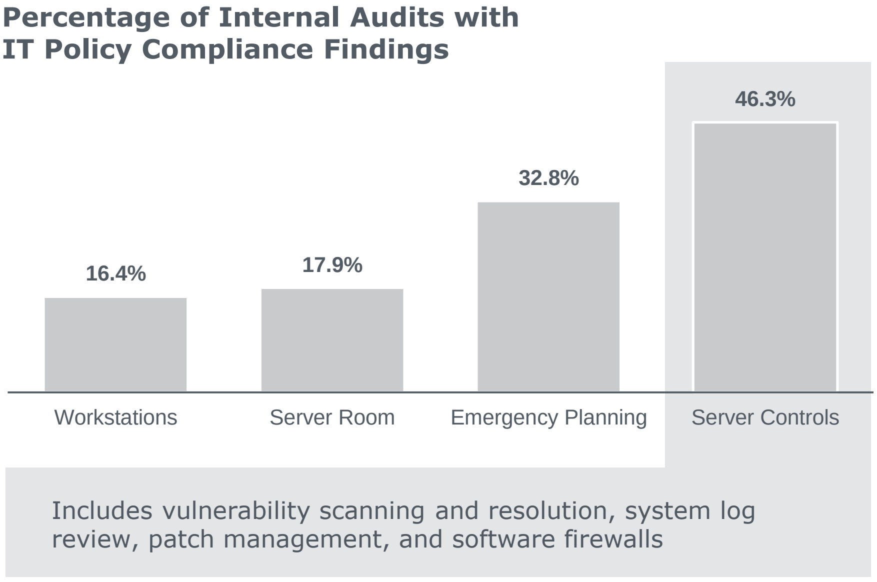
Like many institutions of higher education, Indiana University has faced increased cyber attacks in the last several years. When the IT team at IU analyzed the history of attacks, they discovered that the fastest-growing segment of attacks involved botted hosts, or servers that had been taken over by a third party and used for external attacks under the guise of IU computing.

Increasing Attacks on Indiana University Computing



A review of five years of internal audits revealed recurring gaps in unit-level compliance with existing cybersecurity policies. IU had already constructed a highly secure data center, but the institution's decentralized culture left many servers without effective security controls. With the board of trustees' support, the institution rolled out a Cyber Risk Mitigation Policy that included unit-level reviews and dean sign-offs.

Routine Audits Reveal a Pattern of Policy Compliance Gaps



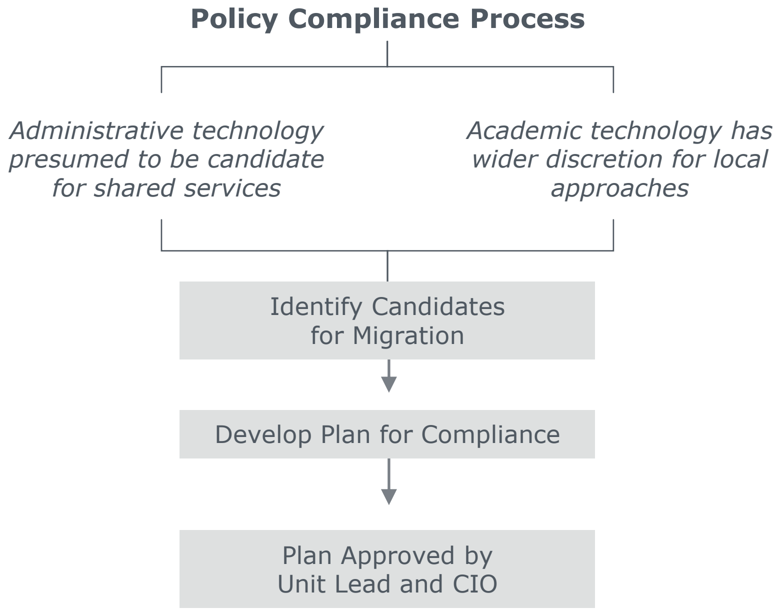
Includes vulnerability scanning and resolution, system log review, patch management, and software firewalls

Source: EAB interviews and analysis.

Treating Cyber Risk Like Financial Risk

IU's IT reduced friction with departments by segmenting acceptable risk mitigation approaches for administrative and academic uses. Administrative technologies (e.g., website HTML servers) are presumed to be candidates for shared services, but the policy gives greater latitude to academic technologies for research and instruction. In either case, deans and researchers can use differentiated, unit-based services if they demonstrate how local security controls provide an ongoing and appropriate level of risk mitigation.

Allowing Units Greater Discretion for Academic Uses



Policy Compliance Process

Administrative technology presumed to be candidate for shared services

Academic technology has wider discretion for local approaches

Identify Candidates for Migration

Develop Plan for Compliance

Plan Approved by Unit Lead and CIO

Schools, administrative departments, and central IT codesigned the implementation rules, which drew on existing approaches for financial policies with the CFO. Policy compliance begins with each unit conducting a self-review and planning their path to policy compliance. Exception requests are peer reviewed, and if the dean provides an alternate means to mitigate cyber risks per security policies, the CIO is not likely to push for further centralization.

Peer Review of Exception Requests Increases Buy-In

Unit Self-Review → **Exception Peer Review** → **CIO Sign-Off**

Unit Self-Review

- Unit IT and leader verify that department meets eight groups of security controls; together they identify technology candidates for secure, shared services
- Review time commitment ranges from 10-150 hours; mean time is 33 hours

Exception Peer Review

- Cross-functional IT managers review requested technology exceptions; peer-group analysis reduces pushback
- Most exceptions requested for research and classroom technology in select departments
- Higher scrutiny on administrative technology than academic tools

CIO Sign-Off

- Central IT team reviews final recommendations after peer group denies or approves exceptions
- CIO and school dean or dept. head sign off on risk mitigation
- Central IT helps unit identify targets for risk remediation and technology migration

Source: EAB interviews and analysis.

Incentivizing Cyber Risk Mitigation

The key to policy success is making deans and administrators aware of the potential costs of cyber threats and the unit benefits available through centralization of servers and technology. In town hall meetings, online broadcasts, and in-person meetings at the department level, the CIO and CISO spent three months educating departments about reduced costs, insulation from risks, increased staff specialization, and space reclamation.

While some local IT staff and researchers did not like the new rules, face-time with the CIO and leadership team helped explain the nuances of the policy and the multiple ways to achieve cyber risk mitigation. Support of the deans and vice presidents was crucial.

CIO Offers Deans Reduced Risks, Lower Costs

- 4%

Accelerated Cost Reduction

IT lowered pricing for shared server space by about 12%, a further decrease past the standard annual decrease (8%)

Insulation from Cyber Risks

Department servers moved to a tornado-proof, secure facility to shield local data and constituents from cyber risks (e.g., attacks, physical damage)

Increased Staff Specialization

Reduced need for generalists at department level allows more local investment in mission-focused services and technology

Reclaimed Space and Energy

Central services gain economies of scale in heating, cooling, and powering servers; deans reclaim needed academic space

"Run into the Fire" to Minimize Pushback from Faculty

- Initial rollout of the new policy provoked some confusion and strong reactions among academic researchers and unit-level IT staff; to quickly move the conversation forward, the CIO asked for a face-to-face engagement to personally brief the entire department on:
  - The risks to departments and the institution from new cyber threats
  - Benefits to be gained from moving more servers to secure facilities
  - How to achieve and demonstrate effective, local security controls for academic and research technologies
- By immediately addressing concerns in person and fully explaining the new cyber risk policy, the CIO helped department leadership and faculty recognize the need for change and comply with the new policy.

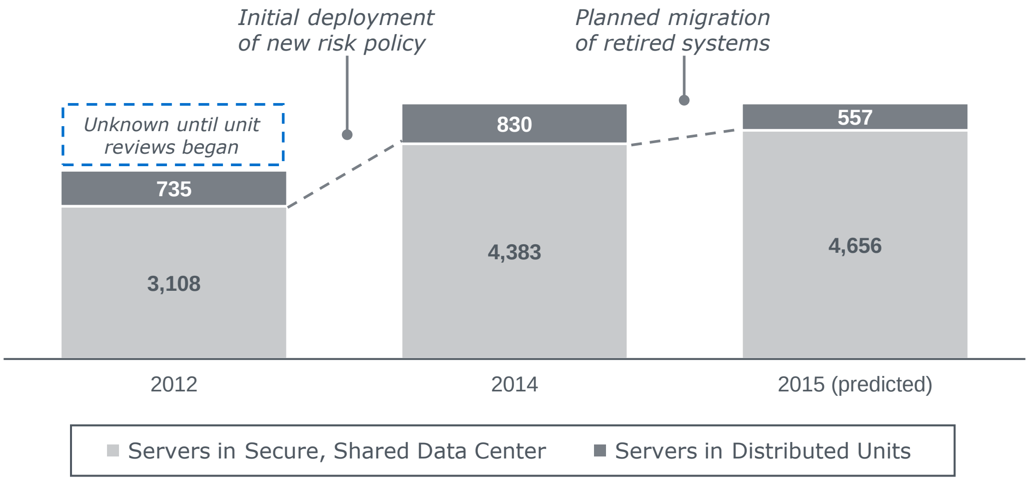
Source: EAB interviews and analysis.

Reducing the 'Surface Area' of Vulnerability

Since the introduction of the new cyber risk mitigation policy, hundreds of servers have been virtualized or physically moved into the secure server space; there are fewer physical servers to attack, and 9 out of 10 servers on campus are now within the secure data center. The vast majority of administrative units have moved all servers into shared services, and only a handful of units still maintain internal servers. For units that recently purchased administrative computing systems, and would thus "lose" their investment if departmental servers were migrated immediately, the CIO offers to set up a future date for planned migration—and as systems retire, most are moved into the secure facility.

Administrative Focus Helps IT Collect 90% of All Servers in Secure, Cost-Effective Facility

Servers in Central Data Center and Distributed Units



> **Trustees Very Pleased with Strong Security Progress**
>
> "A trustee said that he wanted to take me out to dinner over the numbers we've moved using this new policy."
>
> *Brad Wheeler*
> *CIO, Indiana University*

Source: EAB interviews and analysis.

EAB

Implementation Resources

APPENDIX

Implementation Resources

Member Challenge	Security Need	EAB Resources
IT is not using metrics *to track or evaluate our awareness efforts, and we're not sure what to measure.*	Metrics for Awareness	**Security Awareness KPI Compendium** page 56
If a breach happened today, ***we aren't sure who would be in charge*** *of escalation and communication; we aren't prepared.*	Breach Response Roles	**Incident Manager Role Template** page 62
Boards and executives are uninformed about cyber risks or too worried; we ***need a balanced reaction from leaders*** *to guide strategy.*	Pass-through Education Documents	**Board Education Memo Template** page 64
IT struggles with ***vulnerability education*** *for department leadership, and establishing* ***security controls benchmarks*** *for remediation is too difficult to do campus-wide.*	Department Leadership Engagement Tools	**Risk Framework for Department Education** page 69 **Department Security Scorecard Template** page 74
We think self-phishing is a great way to show campus why security matters, but we are ***worried about pushback from end users****.*	Self-Phishing Support Documents	**Self-Phishing Pre-Wire Templates** page 83
We're not sure ***where to start with policy development*** *for cyber risk mitigation.*	Draft Policy Language	**Cyber Risk Mitigation Policy Language** page 92

Visit the IT Forum Webpage for More Tools and Resources

Find native-format tools and implementation resources at eab.com/itf.

Security Awareness KPI Compendium

Use Proactive Security Metrics to Drive Behavior Changes

Without an accurate tracking mechanism for results, security teams struggle to define the goals and expectations for new investments and changes in policy to executives and the rest of campus. This makes communication more difficult and forces security teams to rely on fear, uncertainty, and doubt (FUD) campaigns that are known to be deficient but difficult to replace without better data.

In the following five pages, we lay out some of the more progressive and proactive measures used by IT security teams to understand and track the behavioral drivers of cybersecurity risk. Using metrics tied to awareness and behavior will allow security teams to measure improvement with a leading indicator (awareness) rather than a lagging indicator (compromised accounts).

!

Warning: Tracking Only the "Lagging Indicator" of Actual Compromises May Not Be Enough to Discover and Remediate Vulnerabilities

The number of compromised accounts and devices per year is relatively easy to track and is tied to real consequences and operational costs (e.g., the cost in staff time and resources). However, using this metric might fail to drive change on campus because:

- **It is reactive** (i.e., it tells the security team only after something has already gone wrong).
- **It is difficult to disaggregate the causes of compromise** (e.g., poor password choice, poor password protection, weak physical security).

While changing components of security policy and education might address certain causes, no change will address each root behavioral or technical cause, which obfuscates the true drivers of increasing or decreasing compromise volumes.

Getting Started with Proactive Security Awareness KPIs

□ Assess capability to track each metric

□ Select limited set of metrics to pilot on campus

□ Incorporate chosen metrics into security dashboard

□ Refine training and technology deployment based on data collected on proactive metrics

□ Assess impact, communicate to partners, and change or add metrics for future years

Tool 1

Security Awareness KPI Compendium

Phishing Vulnerability

Measurement details: Security team works with help desk to track the number of compromised accounts and devices caused by phishing attacks

Metrics to Track	What IT Can Do with Metrics
• Number of victims per attack	• Adjust campus-wide phishing education targets and timing to the areas on campus most at-risk in a phishing attack • Refine training module structure to address the most common and effective types of phishing messages • Review campus email protections and firewall rules to find out if more phishing attacks could be screened out before reaching end users
• Number of victims per month	
• Number of victims per year	
• Population most affected	
• Total number of people notifying help desk	
• Most common phishing messages	
• Most effective phishing messages	

Self-Phishing Vulnerability

Measurement details: Security team tracks vulnerability directly, coordinates with help desk, administrative offices to track qualitative responses

Metrics to Track	What IT Can Do with Metrics
• Percentage successfully phished per attempt	• Adjust the location, duration, and message of next self-phishing campaign based on previously identified constituency click and training activity • Improve the targeting and timing of phishing education modules delivered to campus • Refine coordination and communication with local managers and campus administrative partners (e.g., help desk) to strengthen buy-in for awareness
• Percentage deleting message per attempt	
• Percentage reporting message per attempt	
• Percentage clicking on training module	
• Percentage completing training module	
• Most vulnerable constituency	
• Most effective time of day	
• Most effective times of year	
• Most effective phishing messages	

Tool 1

Security Awareness KPI Compendium

Training Completion

Measurement details: Security team works with web team to track click rates, completion, and scoring on assessments

Metrics to Track	What IT Can Do with Metrics
• Percentage and number completing general (i.e., non-tailored) training modules	• Adjust the training module structure, content, and modality based on highest completion rates • Consider creating new incentives (both positive and negative) tied to compliance with training rules if departments or individuals do not complete training in consecutive terms
• Percentage and number completing targeted (i.e., tailored) training modules	
• Completion rate by college and department	
• Completion rate by role (e.g., students, faculty, staff, executives)	
• Most effective placement (e.g., course registration, website)	
• Most effective timing (e.g., onboarding)	

Physical Security Compliance

Measurement details: Qualitative walk-through by security team for unsecure physical assets

Metrics to Track	What IT Can Do with Metrics
• Volume of vulnerability types by department	• Refine the content of security awareness messages delivered to end users to reflect the most common unsecure behaviors and vulnerabilities identified • Adjust placement of posters and other physical advertisements to campus areas identified as common sites for unsecure behavior • Update training priorities for face-to-face conversations with academic leaders, managers, and end users
• Most common vulnerabilities and unsecure behaviors	
• Most common vulnerabilities by device type	
• Most common vulnerabilities by campus group (e.g., students, faculty)	
• Reasons for physical security lapses (e.g., unit process, convenience)	

Tool 1

Security Awareness KPI Compendium

Sensitive Data Transfer

Measurement details: Detected through monitoring tool like data loss prevention (DLP) solution, owned and operated by security team

Metrics to Track	What IT Can Do with Metrics
• Volume of emails with sensitive data	• When patters in unsecure transfer are identified, design local education campaign to ensure end users are aware of secure data transfer options • Refine targets for face-to-face, department-level education • Gain buy-in from executives and department leadership (e.g., deans, department chairs, directors) by showing real evidence of vulnerability tied to sensitive data
• Percentage of emails with sensitive data	
• Common sensitive data types (e.g., SSN, credit card number) transferred	
• Share of sensitive transfers by department	
• Share of types of sensitive data sent by department	
• Share of types of sensitive data by time of year sent	
• Reasons for unsecure transfer (e.g., tax season) to calibrate education	

Security Website Traffic

Measurement details: Security team asks web team to track web traffic to security portal after department presentations and events

Metrics to Track	What IT Can Do with Metrics
• Daily site traffic average for month and year	• Adapt content and resources available online to meet end-user demand • Based on popularity and download rates, refresh content that remains applicable but has slow demand and consider retiring material with very low activity and relatively low applicability • Prioritize content to archive online for easy access or reformat for face-to-face presentations
• Download volume for security resources	
• Content download popularity (e.g., poster versus FAQ)	
• Change in traffic and download pattern around NCSAM and campus events	
• Change in traffic and downloads after CISO presentations to units	

Tool 1

Security Awareness KPI Compendium

Department Demand for Security Training

Measurement details: Security team keeps track of ad hoc and formal requests for services

Metrics to Track	What IT Can Do with Metrics
• Volume of formal presentation requests by month and year	• Update modality of future trainings to match the content preferred by active departments • Archive popular content and re-format less-popular resources to streamline education role • Prioritize face-to-face conversations with managers in departments with declining or no requests for direct education
• Most common request types (e.g., in-person presentation versus consultation)	
• Change in request type and volume around security events and communications	
• Departments or units that do not make any requests from security team	
• Most common ad hoc resource requests to convert into scalable services	

Self-Rating on Central Framework

Measurement details: Security team collects self-scores through survey mechanism and sets high-level view and benchmarking (e.g., Tool 5: Department Security Scorecards on page 74)

Metrics to Track	What IT Can Do with Metrics
• Percentage of units filling out survey	• Prioritize targets for institution-wide remediation (e.g., if one security control has low scores across the institution) • Prioritize targets for department-level remediation (e.g., if one academic unit has security control scores below the average for their peer units) • Help departments develop risk remediation and management plans for the coming year by focusing efforts on controls behind peer or institutional norms
• Average scores across institution	
• Average scores within functional groups (e.g., academic units, administrative units)	
• Number of units requesting help to complete survey form	
• Average time for units to fill out survey	
• Year-over-year improvement in scores	

Security Awareness KPI Compendium

Implementation Tips for Proactive Security Metrics

Recording and tracking new kinds of metrics will require additional work from the security team or CISO, as well as asking unit staff to self-score or provide new kinds of behavioral data. These metrics will help the security team understand and prioritize risks more effectively, but the metrics will create substantial value only when they are effectively understood by line-level staff, faculty, and students. When introducing these metrics on campus, remember to:

- **Choose a Limited Set of Metrics to Start Tracking and Reporting**
  - Tracking all of the metrics on the previous pages will overwhelm the security team, and each metric will not be applicable to the root causes of risk on campus.
  - An initial scan of qualitative assumptions within central and distributed IT will guide the security team to a narrow list of known problems. Cross-check those assumptions with any quantitative data on the location and nature of previous compromises or breaches to select the final list.
- **Establish a Baseline Before Making Changes and Reporting to Campus**
  - Begin by tracking metrics on an internal document (e.g., Excel spreadsheet) and establish a baseline before making adjustments to training or reporting results to leadership and campus.
  - Set internal goals based on initial measurements, but do not publicly set goals for metric improvements until campus members have had a chance to see the new data and understand baseline expectations.
- **Use New Metrics to Refine Training, Technology Deployment**
  - Define the activities performed by the security team that could be refined with better metrics, and match potential findings with potential actions (e.g., if a department is more vulnerable to phishing emails than others, increase face-to-face training for local staff and speak with managers directly about risks).
- **Focus Communications on the Importance of Human Vulnerability**
  - An informed and skeptical end user is the best line of defense against the majority of digital security threats; increasing attention to the behavior and attention of users is the logical counterpart to the surging spend around technology prevention and detection tools.
- **Remind Users that Measurement Is a Service, Not Punitive**
  - Some users may feel that physical and digital checks of security policy compliance and self-phishing constitute a breach of privacy or a “trick”; the theme of communication around behavioral metrics must be that the security team is collecting new awareness metrics to better protect and enable end users.
- **Set Clear, Public Goals Tied to New Metrics**
  - Use existing communications and events (e.g., National Cyber Security Awareness Month) as opportunities to describe current practice, explain the drawbacks of weak awareness, and set both short-term goals (e.g., decrease the number of constituents that succumb to self-phishing) and long-term goals (e.g., increase average self-reported scores on asset management by 20% in two years).
  - Include progress on chosen metrics in established, regular communications with the deans’ council, faculty senate, cabinet, or board.

Incident Manager Role Template

Consolidate Authority and Expertise for Agile Response

Most breaches are not resolved quickly or easily, and many require months of reporting, analysis, and testing to verify resolution. Staff and contractors involved in these tasks are often highly paid and resources spent on this process could drive value in many other areas of the IT project portfolio. To strengthen, coordinate, and streamline the incident process, EAB highly recommends temporarily granting a designated role of incident manager to an individual or group of individuals.

Critical Responsibilities for the Incident Manager

- **Ensure Continuity and 24/7 Availability**
  - Put all other project responsibilities on hold for duration of incident
  - If incident lasts more than 12 hours, designate alternate to cover duties overnight
  - Document tasks and work plans; coordinate handoffs between shifts
- **Conduct Damage Assessment and Escalation Decision**
  - Determine if the incident affects critical institutional systems
  - Estimate potential losses and report impact to CIO (CIO makes final determination of incident classification, based on incident manager recommendation)
  - Declare critical incidents and follow quarantine protocol
- **Serve as Communication Waypoint**
  - Connect internal response team and department staff with CIO and deputies
  - If the CIO declares that some details are embargoed for public and media (a gag order), inform staff and ensure private information remains safe
  - Explain incident response details and rules to internal governance committees
  - Determine the external notifications that will be necessary; contact external stakeholders with approval of CIO and relevant internal staff
- **Form Incident Response Team**
  - Activate necessary individuals from central and distributed IT teams that will complete technical breach tasks (e.g., initial forensics)
  - When necessary, recruit staff from other campus units (e.g., general counsel, HIPAA compliance, communications office) to support response activities
- **Collect and Document Evidence**
  - Record initial details of discovery and location, all individuals notified
  - Document decisions and staff involvement throughout all response activities
  - Begin case file with all information; if criminal investigation is warranted, hand off case file and support law enforcement authorities
- **Conduct Postmortem Analysis and Recommend Process Improvement**
  - As appropriate, coordinate retention and destruction of materials after incident
  - Determine root cause of vulnerability and incident
  - Estimate costs of staff and vendor time for incident response and continuing remediation activities
  - Compile report on response effectiveness and efficiency for CIO and internal IT committee structures; recommend changes to protocol as necessary

Incident Manager Role Template

Implementation Tips for Creating an Incident Manager Role

Designating an incident manager does not create a new full-time role, nor does it imply that only one person will be responsible for key functions during an incident. Instead, one or more IT staff members are granted new authority when an incident is detected, to ensure that response is coordinated, fast, and effective.

- **Designate an Individual Below the CIO to Serve as Incident Manager**
  - The CIO should not be incident manager because the 24/7 responsibility and granular decisions required of an incident manager will detract from the CIO’s strategic responsibilities.
  - An entry-level staff person should also not become an incident manager, because the definition of critical systems and coordination of complex internal and external communications requires significant institutional knowledge.
  - Ideally, a CISO or member of the regular security team who is familiar with the technologies and protocols that protect institutional data can be designated as the incident manager when a breach event occurs.
- **Allow Incident Managers to Escalate, Communicate Mostly Independently**
  - While the CIO and other senior leaders must still have final decision-making authority for victim notification, law enforcement involvement, and gag orders over incident details, the incident manager should be empowered to make most internal team decisions and communicate internally without CIO approval.
  - When the CIO’s authority is required for decisions (e.g., designating a critical incident or disaster, approving final notification documents), senior leaders should defer to the recommendations of the incident manager, who is most familiar with breach details.
- **Use Process Documentation to Improve Internal and Vendor Operations**
  - The incident manager’s case file on breach response will help the IT organization know what to expect in a future breach; just as importantly, the IT team can study past events to find sources of inefficiency, remove bottlenecks, and improve the speed of activities.
  - This will help save internal staff time, but also improve the organization’s requests for vendor and expert help, and ensure that RFPs and vendor relationships are bounded and as clear as possible.

Board Education Memo Template

Helping Executives Connect Risks with Policy

Boards of trustees and cabinet members may not understand the technical details of modern information security, but they are very aware of the reputational, financial, and operational consequences that can occur after a security breach. The media's treatment of breach events in higher education and other industries keeps executives informed that adversaries and risks exist, but it does not explain how security risks are relevant to the missions and projects that they care about.

Without a connection between breach news and institutional risks, executives might struggle to contextualize the protections and policies proposed by IT with the real risks the institution faces from unsecure end users and adversaries.

Getting Started with Board Education Memos

- □ Align template with institution brand
- □ Select recent, public breach to adapt for first memo
- □ Security team compiles details; CIO finalizes language
- □ CIO sends Board and Cabinet members final memo; CIO makes time available to explain details and answer questions
- □ When new, relevant breaches occur, CIO and security team decide if events warrant memo treatment

Tool 3

Board Education Memo Template

Template with Recommendations

Your Institution Name Here

Executive Security Memo

Month DD, YYYY

Don’t wait for final details; try to send a memo within a week of initial news.

Incident Title (parallel to media headline)

- **Incident Summary**

  Identify the breached institution’s location and industry; describe the incident in plain (i.e., non-technical) language to give simple, three- to five-sentence summary that explains the most relevant details. Always describe information as “what has been reported so far” in case details change.

- **Incident Root Cause Vulnerability**

  Describe the human and technology failures that put data at risk. When appropriate, include technical details and describe granular processes in place at the breached institution.

- **Impact to Date**

  Use media or institutional estimates to describe potential. Be sure to always describe losses as current estimates and “what is known so far” to avoid confusion if incident details are adjusted later.

- **Our Institutional Protections**

  Pivot to describe how the policies, protections, and technologies in place at your institution address the vulnerability described in the second section. If the risk does not affect your institution (e.g., involves a technology that your institution does not use) make that clear in this section.

- **Our Remaining Exposure**

  Describe the ways in which your institution may still be at risk from a similar attack or exposure, and estimate the potential repercussions from a similar breach at your institution. Be aware that many executives might move straight from the summary to this section; the remaining exposure information should inform future investment and policy discussions.

Tool 3

Board Education Memo Template

Representative Completed Document

Alpha University

Executive Security Memo

January 15, 2014

Target Loses 70 Million Customer Records in Data Breach

- **Incident Summary**
  - On December 19, 2013, retail giant Target Corporation publicly acknowledged that credit and debit card information had been accessed by criminals, and announced a hotline and customer service line for questions.
  - Initial reports indicated that few customers were affected and PIN numbers were secure; a January 10 press release confirmed that at least 70 million customers had information lost, including CVV security codes and expiration dates.
- **Incident Root Cause Vulnerability**
  - Criminals breached customer data by first stealing credentials from a refrigeration and HVAC vendor used by Target in its retail stores.
  - Because the HVAC accounts were not cordoned off from access to the payment system network, the criminals then pushed malware to point-of-sale devices (cash registers) at local retailers to actively collect information.
  - Attackers tested the malware during the Black Friday weekend (November 28, 2013) and collected information during the entire month of December.
- **Impact to Date**
  - Profits in Q4 of 2013 were down 50% from Q4 2012 from lost holiday shopping
  - Share prices fell 9% between December 2013 and February 2014
  - Based on known revenue losses, Target could lay off hundreds of line staff
  - Target executives, including the CIO and CEO, might resign
- **Our Institutional Protections**
  - No vendor accounts for enterprise-wide systems have access to internal financial data.
  - IT staff in the networking team monitor access to personally identifiable information; if any account accesses sensitive data outside of established protocols, IT investigates and shuts down the account if necessary.
  - Institutional policy XX.123 defines the access which vendors can have to internal systems; if all units are in compliance, the breach of a vendor will not expose sensitive internal information.
- **Our Remaining Exposure**
  - A significant number of academic departments partner with various vendors for classroom technology and computing tools; central IT does not always know about those relationships prior to purchase and integration.
  - The University Theatre works with several third-party vendors to process credit card transactions over the Internet; central IT has not been able to determine the access those vendors have to internal systems.
  - A breach of financial data similar to Target’s could damage our relationships with local vendors and lead to additional pressure and scrutiny on central administrative costs from the state legislature.

Board Education Memo Template

Implementation Tips for Board Education Memo

To maximize the effectiveness of memos without putting an undue burden on IT staff to research and write reports for executives, security teams should be selective about generating these documents.

- **Prioritizing Events for Response**
  1) Relevant to Institution (Board and Executives)
     - Incidents that involve a vulnerability or data type that is particularly important for institutional security
     - Incidents that involve aspirant peers, nearby institutions, and others within athletic conference or other networking group
     - All members of the board and cabinet can benefit from more knowledge about events that are relevant to institution; plan to educate as many leaders as possible about
  2) High-Profile Media Treatment (Board Members)
     - Any large incident covered in outlets that board members are likely to read regularly (e.g., *New York Times*, CNN, *Chronicle of Higher Education*)
     - An incident involving a very large or high-profile entity (e.g., Target, Home Depot, Federal Bureau of Investigation)
  3) Local Concerns (Executives Only)
     - Local incidents involving small businesses and cybercrime in the community
     - Most relevant for the chief business/financial officer, chief administrative officer, and senior staff involved directly in procurement and purchasing
- **Send Between One and Six per Semester**
  – If the IT department does not send at least one memo per semester about a relevant breach, executives will not remain sensitized to the reality of digital risks and may go back to old behaviors; however, too many memos can dilute the value of education and give the impression that IT leaders are too worried about outside events

  – As a rule of thumb, send no more than six memos per semester, and no more than one per month

  – Maintain multiple distribution lists; the board of trustees should see only very high-profile, public breaches explained, while the provost will be more interested in peer or aspirant peer impacts, and the chief business officer needs information on local businesses and vendors

Engaging Department Leadership on Security

Two Tools to Educate and Enable Department Leaders

Central information security teams should aim to engage department leaders in security tasks and allow local managers to become proactive about security in their own units. Tools 4 and 5 from pages 69-82 enable security teams to support departments that may be disengaged from security as a priority or that struggle to mitigate risks because of high complexity and decentralization.

Opportunity: Department Education

Academic and administrative leaders do not have a clear understanding of why security policies are important; security is routinely a last priority for department leaders.

Tool 4: Risk Framework for Department Education

Pages 69-73

- **Purpose**: Identify the consequences related to unsecure data that are most important to department constituents. The central security team can focus education conversations on most relevant, top-of-mind risks.
- **Components**: Central security team asks local IT or academic leader to fill in basic template, dividing consequences between reputational, operational, regulatory, and financial, related to the academic, financial, advancement, medical, and research data within department systems.
- **Requires support from**: Local IT or academic staff willing to fill out template (most departments will need only minutes to fill out framework completely).

Risk Framework for Department Education may be more appropriate for your institution if deans and department chairs don't always understand the local consequences that can result from data breaches and lack incentives to change local policy.

Opportunity: Control Benchmarks

Department leaders may understand risks but lack a framework to prioritize remediation; unsafe behaviors proliferate because deciding on goals is difficult.

Tool 5: Department Security Scorecard Template

Pages 74-82

- **Purpose***:* Benchmark department security controls against peer departments as well as institutional averages to guide high-level strategy and local cyber risk mitigation activities.
- **Components***:* Security team asks department to self-score readiness of 29 security local controls culled from NIST/ISO framework. Department academic and financial representatives sign off on scores, and central security team uses results to build campus-wide heat map and department scorecards.
- **Requires support from***:* Local IT, academic, and financial leadership that will complete and sign off on templates (may require significant communication for larger units).

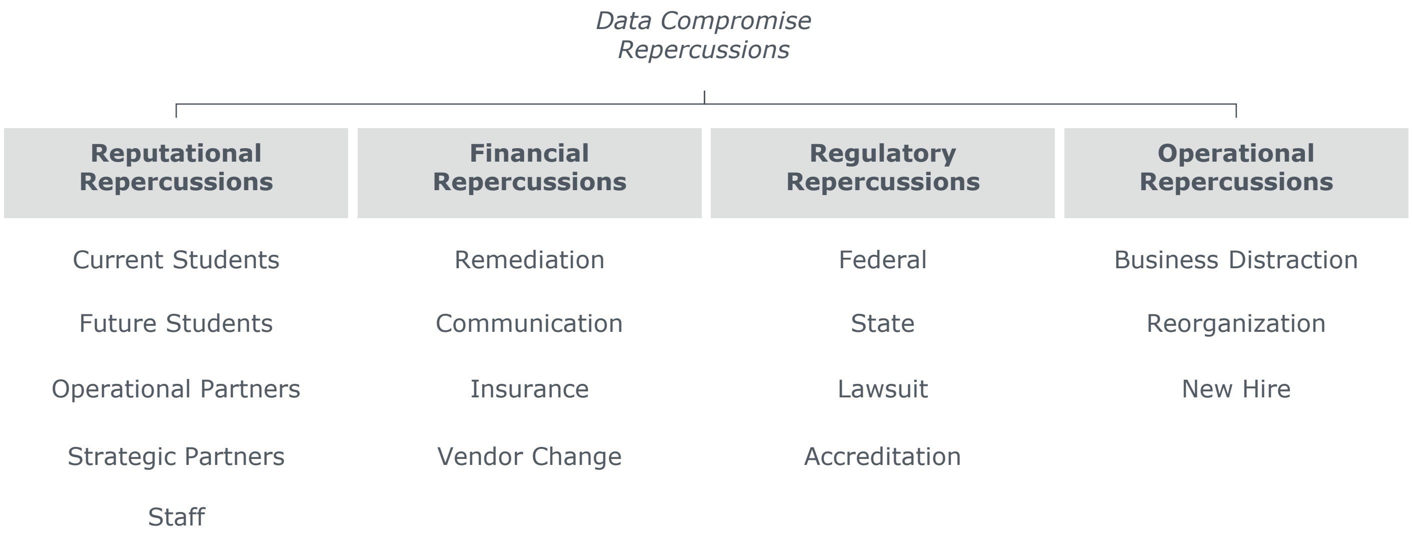
Department Security Scorecards may be more appropriate for your institution if cabinet and board members support stronger security controls, but complex, decentralized structures make it difficult for departments to prioritize risk-mitigation strategy.

Risk Framework for Department Education

Define the Full Range of Risks to Properly Educate Constituents

Even faculty and staff that are well-educated about the likelihood and technical aspects of breaches may not realize the breadth of specific potential consequences that can follow exposure or loss of protected data. Make the CISO’s presentation to line-level staff in departments more effective by filling out a simple risk framework document (either centrally or in the department) that prioritizes the breach consequences faced by the unit.

Framework of Breach Impacts by Repercussion Type



Data Compromise Repercussions

Reputational Repercussions	Financial Repercussions	Regulatory Repercussions	Operational Repercussions
Current Students	Remediation	Federal	Business Distraction
Future Students	Communication	State	Reorganization
Operational Partners	Insurance	Lawsuit	New Hire
Strategic Partners	Vendor Change	Accreditation	
Staff			

Getting Started with the Department Risk Framework

- □ Ask local department leader or IT staff to help fill out framework template specific to unit vulnerabilities before security team presentation
- □ During department presentation, security representative should start with focus on high-risk areas, then individual “hot spots”
- □ Describe how unit’s identified risk profile compares to institution and other similar units
- □ As appropriate, use self-identified areas of high risk to propose risk-mitigation strategy

Note: Adapted from “The Financial Impact of Breached Health Information: A Business Case for Enhanced PHI Security.” American National Standards Institute/Santa Fe Group/Internet Security Alliance, 2012

Tool 4

Risk Framework for Department Education

Prioritize Education by Local Data and Vulnerability

While all departments may face some level of reputational, financial, regulatory, and operational risk, the size of risk depends on the nature of data and behavior within the department. Before delivering in-person presentations to teams and departments, the security team should reach out to local staff to learn what kinds of data and activities are most critical to strategy and how a breach in those areas would affect ongoing operations.

Data Type	Example Information
Academic	• Directory information • Course records • Student PII
Administrative	• Credit card number • Bank routing number • Bank account logins
Advancement	• Anonymous donors • Donor PII • Gift terms
Medical	• Patient records • Patient notes • Patient PII
Research	• Material for publication • Collaborative data set • Sponsored research

Rating Potential Impact of Breach

0 **Not Applicable**
Data or compromise is irrelevant to department

1 **Minor Risk**
Little or no consequence to department from data loss

2 **Some Risk**
Breach will require remediation but effects are highly limited

3 **Moderate Risk**
Breach will require significant staff time, effort, and communication

4 **High Risk**
Compromise will create costs and inhibit operations for several years

5 **Catastrophic Risk**
Devastating, long-term consequences for department staff and constituents

Tool 4

Risk Framework for Department Education

Local IT or Academic Staff Fill Out Risk Estimates

Before the security team visits a department for education, ask local IT, business, or academic staff to estimate the 0-5 range of risks for data types within the unit; provide a template for their use and offer IT’s consultation services for this step. Calculate average individual risks in the “Overall” row to streamline risk identification.

Impacts for the College of Arts		Data Type				
		Academic	Administrative	Advancement	Medical	Research
Reputational	Current Students					
	Future Students					
	Operational Partners					
	Strategic Partners					
	Staff					
	Overall					
Financial	Remediation					
	Communication					
	Insurance					
	Vendor Change					
	Overall					
Regulatory	Federal					
	State					
	Lawsuit					
	Accreditation					
	Overall					
Operational	Business Distraction					
	Reorganization					
	New Hire					
	Overall					

Reputational risks may be difficult to estimate, as they reflect subjective attitudes about trust and risk tolerance. Local staff should consider how the loss of trust with regular customers (e.g., vendors) might complicate their ability to function effectively in day-to-day work.

Local staff fill in a number 0-5 to estimate the potential repercussions of a relevant breach in their unit.

Financial risks are a function of real breach response costs in staff time and technical operations, but also potential changes in insurance premiums.

Average all the reputational, financial, regulatory, or operational risks within one data type to fill in the “Overall” risk cells.

Regulations and laws that affect data types will vary across units and states; compliance staff within units can help to explain which risks are most relevant.

Units may underestimate the staff time and organizational changes that a breach event will necessitate; units may need help initially to understand how operational costs will affect them.

Risk Framework for Department Education

Example Completed Risk Table for College of Arts Presentation

Complete Table Serves As Heat Map to Guide Discussion

Rather than talk through a litany of institutional risks that may not be relevant to unit operations, a security representative can use the completed table (sample below) and the identified "hot spots" to focus conversation around risks most consequential for the unit.

Impacts for the College of Arts		Data Type				
		Academic	Administrative	Advancement	Medical	Research
Reputational	Current Students	3	2	4	0	2
	Future Students	2	0	2	0	3
	Operational Partners	2	0	2	0	5
	Strategic Partners	5	1	2	0	4
	Staff	4	2	1	0	4
	Overall	3.2	1	2.2	0	3.4
Financial	Remediation	1	1	1	0	1
	Communication	1	2	1	0	1
	Insurance	1	0	0	0	0
	Vendor Change	2	3	0	0	0
	Overall	1.25	1.5	0.5	0	0.5
Regulatory	Federal	3	1	0	0	1
	State	2	0	0	0	1
	Lawsuit	2	3	2	0	1
	Accreditation	5	0	0	0	2
	Overall	2.75	1	0.5	0	1.25
Operational	Business Distraction	2	2	2	0	3
	Reorganization	3	2	1	0	3
	New Hire	4	3	3	0	3
	Overall	3	2.3	1.3	0	3

Risk Framework for Department Education

Implementation Tips for Department Education Framework

Using a risk framework table imposes a new initial cost for the security team before making education presentations to academic departments and administrative units. However, the value of these presentations, and the usefulness of security team time spent in direct education, is increased significantly through this simple preparation tool. Consider the following recommendations to maximize the effectiveness of framework use:

- **Work with Local IT or Academic Leader to Fill Out Framework Document**
  - The risk framework document will be most effective when it reflects the opinions of department stakeholders, whether in the distributed IT staff or in faculty and administrative ranks.
  - However, given some knowledge about the unit's research and teaching missions, central IT security staff should be able to complete most of the document without further help.
- **Focus on Sections of High Average Risk, Then on Individual Areas of High Risk**
  - When presenting to department staff, begin the conversation with the department by discussing the areas where overall (i.e., average) risk is highest; this ensures that initial attention and conversation is built around the places where the department's greatest perceived risks are.
  - After that, point out places where individually high risk (e.g., for the previous page example, 'Customers' impact for Advancement data) should be called out for mitigation.
- **Describe How Unit Risk Profile Compares to Institution and Other Units**
  - While the unit's individual risk profile should be instructive about strategy and goals, and allow the security team to have a much more focused conversation about challenges, units will also benefit from knowing how they are similar or divergent from the institution at large and other departments.
  - For example, when speaking with constituents in the nursing or dental school, the high risks associated with medical data protected under HIPAA could usefully be compared to the medical School, which may have implemented policies and procedures for data protection that constituents in nursing and dentistry could implement in their own unit.
- **Use Risk Framework to Clarify Dangers and Propose Mitigation Strategies**
  - Helping units understand the breadth of risks they truly face, and engaging them with comparisons to institutional and peer unit vulnerability, gives the security team a better opportunity to teach department leadership and staff what needs to change.
  - Use the risk framework document to highlight where the greatest dangers lie, outline where current protections are strong and where they may fall short, and use the conversation grounded in department mission to propose necessary changes.
  - Even without comprehensive coverage, recognition of patterns in "like" departments (e.g., history and political science) can inform security conversations and help the security team make a greater impact during face-to-face education.

Tool 5

Department Security Scorecard Template

Security Teams Not Enfranchising Unit Leadership in Security

Cybersecurity awareness and defense are enterprise-wide processes, not tasks and responsibilities performed entirely within central IT. However, department staff may not always understand the technical nature of cyber threats and the positive role that they can play in preventing and mitigating breaches. Without a common framework to guide discussion and prioritize change, security teams can struggle to gain buy-in from department administrators, financial leaders, and local IT staff.

A simple self-rating tool, accompanied by a targeted conversation with the security team and clear benchmarking targets, helps department leaders understand the critical gaps in local defenses and prioritize remediation strategy.

A Lightweight Tool for Self-Assessment and Benchmarking

While many security teams have used a publicly available framework for internal assessments, these tools gain significant value when they enable both institutional and departmental leaders to understand and act on security gaps. In the following pages, we offer a basic framework based on NIST categories and a Capability Maturity Model Integration (CMMI) process improvement model, suggest practices for internal surveying on these categories, and provide templates for strategic, high-level analysis tools and department level scorecards.

The purpose of these tools is not to supplant existing audit frameworks, but rather to drive additional value from the auditing activities that many security teams already conduct and enfranchise department leadership in their own data protection.

Getting Started with Department Security Scorecards

- □ Divide departments by primary data usage; ask department leaders to self-identify peer groups if multiple data types used
- □ Department leaders self-score security controls inside department; academic, financial representatives sign off on scores
- □ Departments share self-scores with security team; security team inputs all data into central repository
- □ Security team generates campus-wide heat map based on peer group deviations from institutional averages for security governance groups
- □ Security team generates department-level scorecards based on department deviation from peer and institutional averages
- □ Security governance groups use campus-wide scores to set institutional strategy; departments use scorecards to prioritize local risk mitigation

Department Security Scorecard Template

Dividing Departments by Primary Data Usage

To help the security team and board of trustees focus strategic efforts, while giving departments a better set of benchmarks against peers, divide campus units into one of five categories (Academic, Administrative, Advancement, Medical, Research).

These categories should not be understood to capture all of the department's activities; when departments control multiple kinds of data, the category choice should be determined primarily by the potential risks involved with each category, but also by the kinds of units that department leaders (e.g., deans, department chairs, even end-user faculty) view as their peers.

- **Academic**: Primarily a teaching unit that holds FERPA-protected data about students; can include researchers, but primary risks are tied to student data, not intellectual property loss (i.e., most academic departments)
- **Administrative**: Auxiliary, administrative, and other central units holding financial and other personal information about students, faculty, and staff (e.g., registrar, division of academic affairs, facilities)
- **Advancement**: Units with sensitive information about donors and alumni, loss of which could damage long-standing relationships (e.g., division of alumni affairs, advancement office)
- **Medical**: Units that might teach and conduct internal research, but primary vulnerability is tied to the loss of HIPAA-protected medical patient data (e.g., medical school and dental school clinical units, campus clinic)
- **Research**: Units that primarily conduct research and where the most significant risk is the loss or compromise of intellectual property (e.g., any research institutes or centers on campus, units with large research grants tied to federal or corporate partners)

Department Security Scorecard Template

Survey Design, Data Collection, and Data Analysis

Design, Execute Survey Through Secure, Internal Channels

To collect departmental security scores from across campus, we suggest using one of the following collection options:

- **Spreadsheet Data Collection**
  - Details: Send department leadership teams a short Excel or Word file to fill in line-by-line scores. Collect and synthesize results in a single file.
  - Pros: Easy to copy and paste data into aggregated form for analysis and scorecard production. Personalized notes should generate higher response rates than broadcast survey.
  - Cons: Requires additional staff time to send, collect, and validate spreadsheet files.
- **Manual Written Form or Interview**
  - Details: Security team delivers physical copies of security categories for written self-scores or works with IT and department leaders to assign self-scores in-person.
  - Pros: Highly personalized data collection should generate highest possible buy-in and understanding from department stakeholders.
  - Cons: Requires significant staff time to transcribe and compile data to build heat map and scorecard information.
- **Note: Department Results Must Remain Confidential**
  - Whether the institution uses a spreadsheet or manual process to find out the security posture of departments, the results in the campus-wide map could allow malicious actors to target vulnerable assets.
  - *Only the central IT security team and IT governance groups should have access to the campus-wide heat map and raw data from departments.*

Regardless of Survey Method, Require Leadership Team Sign-Off

Whether using the spreadsheet, or manual written form, each department must secure approval of the local IT leader, business leader, and academic leader before sending the final report to the security team.

- **Department Leaders Are Aware of Risks and Security Team Efforts**
  - One of the primary benefits of the scorecard tool is helping department leaders outside of IT understand cybersecurity threats; requiring all department leaders to sign off is the first step to building a broader knowledge base around institutional vulnerabilities.
- **Provides Context for Future Scorecard Benchmarks and Recommendations**
  - Early sign-off serves as a pre-wire for the delivery of department-level scorecards, and allows security staff to show leaders how their self-scores compare to peers and to the institution without new education.
  - Security scorecards should be the catalyst for more productive discussions about risks, security policies, and potential changes. Early communication and sign-off from department leaders should provide a stronger foundation for security team analysis and recommendations to department leaders.

Department Security Scorecard Template

Self-Scoring Rubric for Department Leaders

Use a Basic CMMI Rubric for Department Self-Scores

Ask departments to self-score their security for the previous pages' risk areas on a standard CMMI scale of 1-5, while providing some guidance and explanation to ensure accuracy.

The following definitions and EAB commentary are meant to explain the maturity levels and describe them qualitatively. Note that higher levels are not always optimal; leaders must make prioritization and trade-off decisions based on the assets, risks, and policies unique to their unit.

- **Maturity Level 1: Initial**
  - The process is not performed or is poorly controlled, largely ad hoc, and reactive.
  - Most academic departments might find that their self-scores fall into the "initial" stage; assure leaders that many of their peers could be in a similar situation, and that they should wait to see how they perform against similar departments before worrying about relative risks.
- **Maturity Level 2: Managed**
  - The process occurs and is managed, but is tied to specific projects rather than being integrated into strategy or process.
  - If security measures are implemented unevenly (e.g., for the most important or high-profile projects), the process is probably "managed."
- **Maturity Level 3: Defined**
  - The process is defined in writing for the unit and is conducted as a matter of policy rather than only in response to events.
  - Ask departments if the process has a defined owner or if the function exists in a job description—if so, the component is probably "defined" rather than "managed."
- **Maturity Level 4: Quantitatively Managed**
  - The unit measures the effectiveness of the process using monitoring technology, dedicated tools, or specific metrics.
  - Ask departments to describe how they know they are doing well in categories; if they can cite measures of effectiveness, the process is "quantitatively managed."
- **Maturity Level 5: Optimizing**
  - The unit focuses on process improvement and learning lessons from process deployment.
  - Few if any academic units will be in position to optimize cybersecurity processes; only those units with very high risks associated with exposure (e.g., PCI compliance, lawsuit, loss of accreditation) should aim for "optimizing" status on more than a handful of categories.

Department Security Scorecard Workbook Online

- Find a native-format version of this tool and additional resources at eab.com/itf.

Note: Adapted from the Capability Maturity Model Integration Institute; http://cmmiinstitute.com/

Tool 5

Department Security Scorecard Template

Risk Area	Definition	NIST and ISO/IEC Reference
Security Governance	Information security policy is established and codified across the unit, and governance and risk management processes address cybersecurity risks.	• NIST SP 800-53 Rev. 4 -1 controls from all families, PM-9, PM-11 • ISO/IEC 27001:2013 A.5.1.1
Security Roles and Responsibilities	Information security roles and responsibilities for IT leaders, line-level staff, and any relevant third parties are established.	• NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11, PM-1 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1
Critical Asset Management	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	• ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
Risk Management and Strategy	Risk management processes are established, managed, and agreed to by organizational stakeholders. Organizational risk tolerance is determined and clearly expressed.	• NIST SP 800-53 Rev. 4 PM-9, PM-8, PM-11, SA-14
Institutional Data Risk	Threats to the institution emanating from institutional data are identified and documented.	• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
Unit Data Risk	Threats to the unit emanating from unit data are identified and documented.	• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
Risk Assessment	Potential business impacts and likelihoods are identified.	• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14
Risk Prioritization	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk .	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
Legal Risk Management	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	• ISO/IEC 27001:2013 A.18.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)
System and Network Monitoring	The network is monitored to detect potential cybersecurity events, and vulnerability scans are performed.	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, RA-5
Malicious Software Detection	Unit staff can detect, identify, and appropriately respond to discovery of malicious and unauthorized software and code.	• ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3
Identity and Access Management	Identities and credentials are managed for authorized devices and users, and IT actively manages access permissions.	• ISO/IEC 27001:2013 A.6.1.2, A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4 • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16, IA Family
Information Security Awareness	Security awareness demonstrates relevance for end users using local rather than institutional risks. Privileged users and senior executives understand roles and responsibilities.	• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, AT-3, PM-13
Information Security Training	All users undergo regular (e.g., at least annual) training related to cybersecurity risks, responsibilities, and are tested on knowledge.	• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, AT-3, PM-13
Data Protection	Data-at-rest and data-in-transit are protected.	• ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8, SC-28

Note: Adapted from the Framework for Protecting Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

Tool 5

Department Security Scorecard Template

Risk Area	Definition	NIST and ISO/IEC Reference
Data Storage Management	Technologies and processes to store and access sensitive data (e.g., through virtualization) include appropriate data encryption and protections.	• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 SC-28, CM-8, MP-6, PE-16
Data Destruction	Data is destroyed according to policy.	• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6
Incident Response Planning	Response plans and recovery plans (incident and disaster recovery) are in place and managed.	• ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8
Incident Management	Personnel know their roles and order of operations when a response is needed. The impact of the incident is understood, and incidents are categorized consistent with response plans.	• ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
Server Management	Department servers have appropriate protections, encryption, and access privileges as stated in policy.	• ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family
Incident Communication	Events are reported consistent with established criteria; information is shared consistent with response plans.	• ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR 4, IR-8, PE-6, RA-5, SI-4
Business Continuity Planning	Business continuity plans are in place and managed.	• ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8
Disaster Recovery Planning	Disaster recovery plans are in place and managed.	
Continuous Response Improvement	Newly identified vulnerabilities are mitigated or documented as accepted risks, response plans incorporate lessons learned, and response strategies are updated.	• ISO/IEC 27001:2013 A.12.6.1, A.16.1.6 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5, CP-2, IR-4, IR-8
Software Asset Management	Software platforms and applications within the organization are inventoried.	• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
Physical Asset Management	Physical devices and systems within the organization are inventoried.	• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
Development Process Management	The development and testing environment(s) are separate from the production environment.	• ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2
Vendor Management	Third-party stakeholders (e.g., suppliers, customers, partners) understand cybersecurity roles and responsibilities.	• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9
Communication Tools	Communications and control networks are protected.	• ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

Note: Adapted from the Framework for Protecting Critical Infrastructure Cybersecurity, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

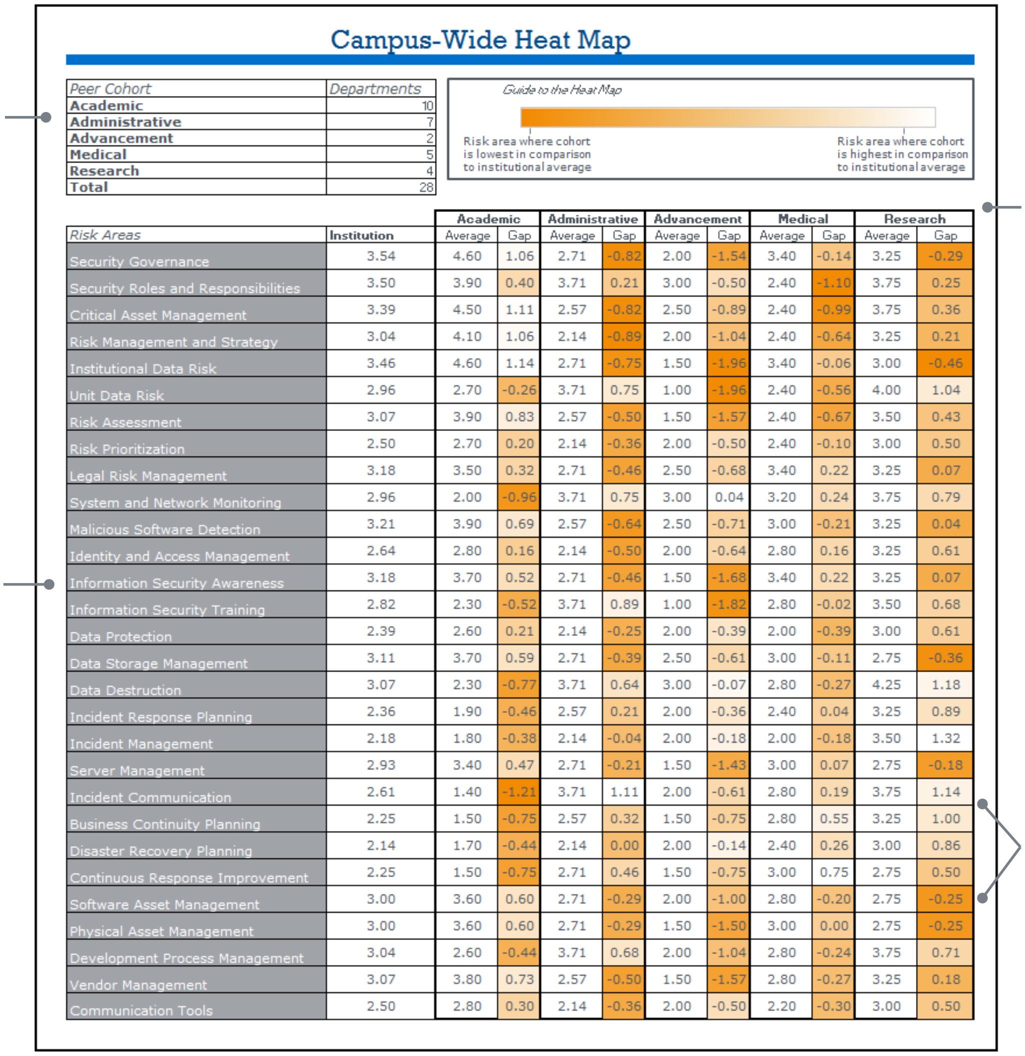
Department Security Scorecard Template

Build a Campus-Wide Heat Map of Risks

The primary purpose of collecting self-scores from departments is to populate a heat map of the entire campus that the security team and relevant leadership groups (e.g., board of trustees, IT governance teams) can use to set strategy moving forward.

To gain the buy-in from the maximum number of departments, notify all leaders that the survey mechanism will be used to generate information for the board, and that IT will report to the board of trustees on which units did not participate.

An example of a fully populated campus-wide heat map follows, below.



Overview of department cohorts

Average and gap scores organized by department type

Each row includes one risk area

Low and high scores easy to recognize and call out for discussion

Campus-Wide Heat Map

Peer Cohort	*Departments*
Academic	10
Administrative	7
Advancement	2
Medical	5
Research	4
Total	28

Guide to the Heat Map

Risk area where cohort is lowest in comparison to institutional average

Risk area where cohort is highest in comparison to institutional average

		Academic		Administrative		Advancement		Medical		Research	
Risk Areas	**Institution**	Average	Gap	Average	Gap	Average	Gap	Average	Gap	Average	Gap
Security Governance	3.54	4.60	1.06	2.71	-0.82	2.00	-1.54	3.40	-0.14	3.25	-0.29
Security Roles and Responsibilities	3.50	3.90	0.40	3.71	0.21	3.00	-0.50	2.40	-1.10	3.75	0.25
Critical Asset Management	3.39	4.50	1.11	2.57	-0.82	2.50	-0.89	2.40	-0.99	3.75	0.36
Risk Management and Strategy	3.04	4.10	1.06	2.14	-0.89	2.00	-1.04	2.40	-0.64	3.25	0.21
Institutional Data Risk	3.46	4.60	1.14	2.71	-0.75	1.50	-1.96	3.40	-0.06	3.00	-0.46
Unit Data Risk	2.96	2.70	-0.26	3.71	0.75	1.00	-1.96	2.40	-0.56	4.00	1.04
Risk Assessment	3.07	3.90	0.83	2.57	-0.50	1.50	-1.57	2.40	-0.67	3.50	0.43
Risk Prioritization	2.50	2.70	0.20	2.14	-0.36	2.00	-0.50	2.40	-0.10	3.00	0.50
Legal Risk Management	3.18	3.50	0.32	2.71	-0.46	2.50	-0.68	3.40	0.22	3.25	0.07
System and Network Monitoring	2.96	2.00	-0.96	3.71	0.75	3.00	0.04	3.20	0.24	3.75	0.79
Malicious Software Detection	3.21	3.90	0.69	2.57	-0.64	2.50	-0.71	3.00	-0.21	3.25	0.04
Identity and Access Management	2.64	2.80	0.16	2.14	-0.50	2.00	-0.64	2.80	0.16	3.25	0.61
Information Security Awareness	3.18	3.70	0.52	2.71	-0.46	1.50	-1.68	3.40	0.22	3.25	0.07
Information Security Training	2.82	2.30	-0.52	3.71	0.89	1.00	-1.82	2.80	-0.02	3.50	0.68
Data Protection	2.39	2.60	0.21	2.14	-0.25	2.00	-0.39	2.00	-0.39	3.00	0.61
Data Storage Management	3.11	3.70	0.59	2.71	-0.39	2.50	-0.61	3.00	-0.11	2.75	-0.36
Data Destruction	3.07	2.30	-0.77	3.71	0.64	3.00	-0.07	2.80	-0.27	4.25	1.18
Incident Response Planning	2.36	1.90	-0.46	2.57	0.21	2.00	-0.36	2.40	0.04	3.25	0.89
Incident Management	2.18	1.80	-0.38	2.14	-0.04	2.00	-0.18	2.00	-0.18	3.50	1.32
Server Management	2.93	3.40	0.47	2.71	-0.21	1.50	-1.43	3.00	0.07	2.75	-0.18
Incident Communication	2.61	1.40	-1.21	3.71	1.11	2.00	-0.61	2.80	0.19	3.75	1.14
Business Continuity Planning	2.25	1.50	-0.75	2.57	0.32	1.50	-0.75	2.80	0.55	3.25	1.00
Disaster Recovery Planning	2.14	1.70	-0.44	2.14	0.00	2.00	-0.14	2.40	0.26	3.00	0.86
Continuous Response Improvement	2.25	1.50	-0.75	2.71	0.46	1.50	-0.75	3.00	0.75	2.75	0.50
Software Asset Management	3.00	3.60	0.60	2.71	-0.29	2.00	-1.00	2.80	-0.20	2.75	-0.25
Physical Asset Management	3.00	3.60	0.60	2.71	-0.29	1.50	-1.50	3.00	0.00	2.75	-0.25
Development Process Management	3.04	2.60	-0.44	3.71	0.68	2.00	-1.04	2.80	-0.24	3.75	0.71
Vendor Management	3.07	3.80	0.73	2.57	-0.50	1.50	-1.57	2.80	-0.27	3.25	0.18
Communication Tools	2.50	2.80	0.30	2.14	-0.36	2.00	-0.50	2.20	-0.30	3.00	0.50

Department Security Scorecard Template

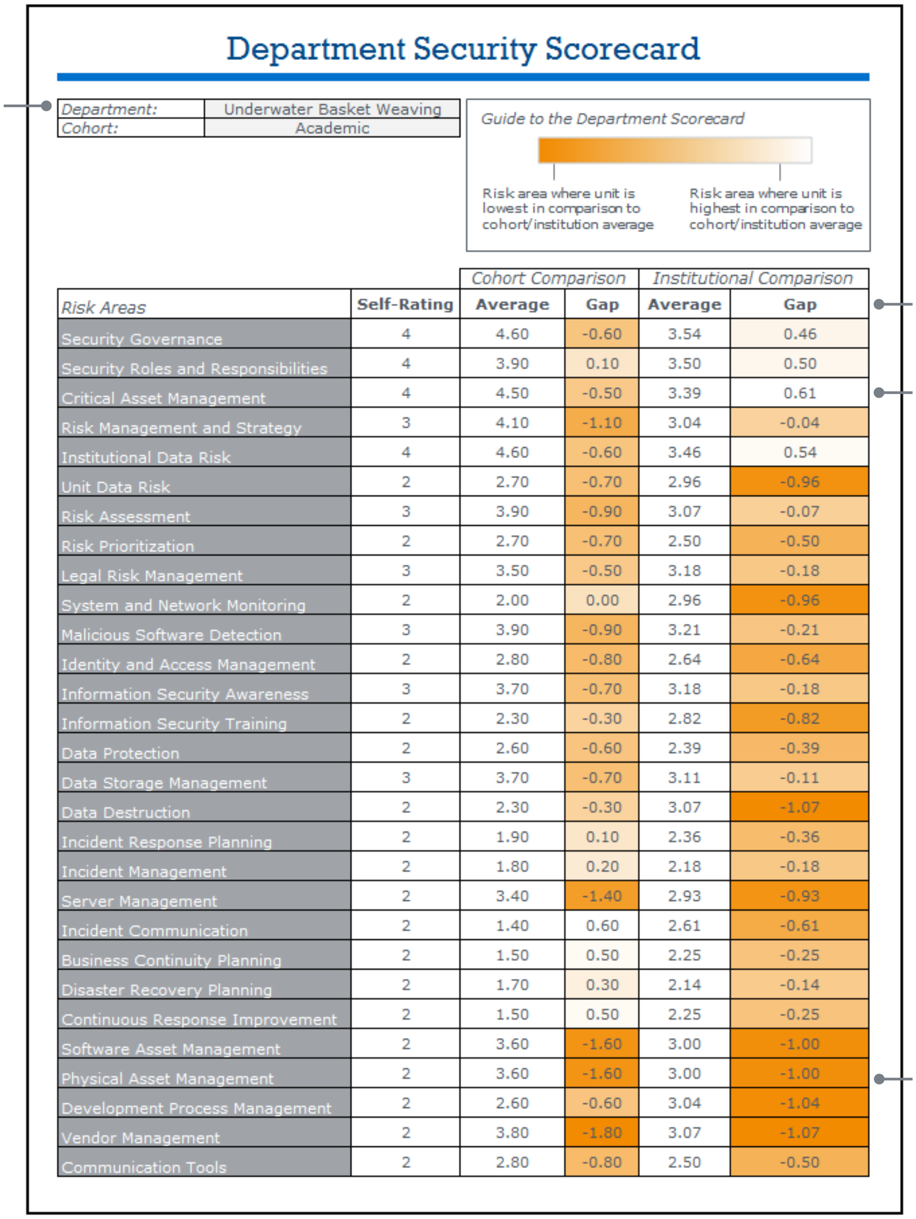
Deliver Effective Department-Level Benchmarks

To help department leaders understand their relative risk and prioritize remediation and security strategy, build and delivery department-level scorecards that show the leadership team how they compare to peer departments as well as the institution.

To learn tactics that help facilitate and focus the scorecard conversation, please see the following page.

A representative populated department scorecard follows, below.

Security team selects unit from drop-down menu for easy printing



Department Security Scorecard

Department:	Underwater Basket Weaving
Cohort:	Academic

Guide to the Department Scorecard

Risk area where unit is lowest in comparison to cohort/institution average

Risk area where unit is highest in comparison to cohort/institution average

		Cohort Comparison		*Institutional Comparison*	
Risk Areas	**Self-Rating**	**Average**	**Gap**	**Average**	**Gap**
Security Governance	4	4.60	-0.60	3.54	0.46
Security Roles and Responsibilities	4	3.90	0.10	3.50	0.50
Critical Asset Management	4	4.50	-0.50	3.39	0.61
Risk Management and Strategy	3	4.10	-1.10	3.04	-0.04
Institutional Data Risk	4	4.60	-0.60	3.46	0.54
Unit Data Risk	2	2.70	-0.70	2.96	-0.96
Risk Assessment	3	3.90	-0.90	3.07	-0.07
Risk Prioritization	2	2.70	-0.70	2.50	-0.50
Legal Risk Management	3	3.50	-0.50	3.18	-0.18
System and Network Monitoring	2	2.00	0.00	2.96	-0.96
Malicious Software Detection	3	3.90	-0.90	3.21	-0.21
Identity and Access Management	2	2.80	-0.80	2.64	-0.64
Information Security Awareness	3	3.70	-0.70	3.18	-0.18
Information Security Training	2	2.30	-0.30	2.82	-0.82
Data Protection	2	2.60	-0.60	2.39	-0.39
Data Storage Management	3	3.70	-0.70	3.11	-0.11
Data Destruction	2	2.30	-0.30	3.07	-1.07
Incident Response Planning	2	1.90	0.10	2.36	-0.36
Incident Management	2	1.80	0.20	2.18	-0.18
Server Management	2	3.40	-1.40	2.93	-0.93
Incident Communication	2	1.40	0.60	2.61	-0.61
Business Continuity Planning	2	1.50	0.50	2.25	-0.25
Disaster Recovery Planning	2	1.70	0.30	2.14	-0.14
Continuous Response Improvement	2	1.50	0.50	2.25	-0.25
Software Asset Management	2	3.60	-1.60	3.00	-1.00
Physical Asset Management	2	3.60	-1.60	3.00	-1.00
Development Process Management	2	2.60	-0.60	3.04	-1.04
Vendor Management	2	3.80	-1.80	3.07	-1.07
Communication Tools	2	2.80	-0.80	2.50	-0.50

Average and gap scores for cohort and institutional comparison

Identify where unit is ahead of institutional average but lags peers

Identify where unit is ahead of peers but lags institution

Department Security Scorecard Template

Provide Guidance to Explain Department Benchmarks

While some department leaders may be very familiar with information security and will quickly understand and use the department scorecards, others may not easily comprehend the meaning of benchmarks and the implications for their units. For those units that have little or no trouble understanding the purpose and value of this tool, the security team should allow local IT staff to explain results for local leaders. The security team should schedule an on-site meeting with local leaders to directly present results in three cases:

- **Leaders Do Not Understand IT Security Issues**
  - Administrators who are new to the position and leaders of very large and complex organizations may have difficulty understanding the full range of risks that affect their department, simply because the scale and technical details of vulnerability are outside of their day-to-day expertise.
  - For these leaders, the security team should serve as an educator, explaining technical details in plain language and guiding administrators through peer unit and institutional benchmarks.
- **Leaders Do Not Understand Why Their Department Is at Risk**
  - Many department leaders, especially those in academic units, may not expect that their team has a role to play in IT security because they themselves do not deal directly with IT issues.
  - Showing these leaders how they fare against peer departments is an excellent opportunity to explain to these groups that even though technology may not seem like their direct responsibility, poor security controls within their unit may be putting their constituents and mission at risk.
- **Unit Has Too Many Security Problems to Address All at Once**
  - In some cases, department business and academic leaders might recognize that their unit is vulnerable to attack or unintentional data compromise, but still be unable to act because there are so many security risks that they do not know where to start.
  - For these groups, the security team plays an invaluable role in prioritizing remediation and helping the unit understand which of the risks are truly urgent (i.e., unit significantly lags peer units and institutional average, and vulnerability is related to very valuable internal data).

!

Warning: Keep Aggregate Scorecard Data Confidential

Remember that data reflecting campus-wide risk profiles is sensitive information, as an adversary could use such a list to determine likely entry points. Only the central security team and IT governance leadership should have access to campus-wide data.

Self-Phishing Pre-wire Templates

Too Many Campus Members See Self-Phishing as an Attack

Used effectively, self-phishing can help security teams educate end users about risks at the point of vulnerability and in connection with normal work processes. Focus education resources on the most at-risk constituents and generate metrics to measure success. Schools that have adopted self-phishing campaigns argue that these benefits outweigh the stigma that many associate with the practice, and that effective preparation of campus through proactive communication can minimize reservations among constituents.

✓

Help Campus Constituents See Self-Phishing as a Service

To build the foundation of an effective self-phishing campaign, begin with pre-wire emails across campus that teach end users, managers, and auxiliary service providers about the reason, importance, and consequences of the new policy. A pre-wire email provides the security team with several key benefits:

- Requires minimal security team time
- Helps end users see that self-phishing is not punitive
- Shows department leaders how new risk data can protect the entire institution
- Prepares other campus support services for end-user questions

In the following pages, find four representative pre-wire emails, alongside key questions that each must answer. Use these questions and templates to build pre-wire emails that will connect with end users and leaders.

Getting Started with the Phishing Pre-wire Emails

□ Define the initial targets and content of self-phishing emails based on past vulnerability and potential future risks

□ Define the scope of self-phishing campaign, the rules governing data sharing, and which outcomes metrics will be used for evaluation

□ Send pre-wire emails to end users, managers, partners and vendors, and the help desk to explain the "What" and "Why" of self-phishing

□ Share suggested response scripting with partners, vendors, and help desk staff to streamline questions

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Communicating Goals to Departmental Managers

In communication with managers, help leaders understand why self-phishing is worth constituents' time.

- **Key Messages to Get Across in Manager Pre-wires Communication**
  - **Reason for the campaign:**
    - Why isn't the status quo education and awareness policy enough to protect campus members?
    - What are the specific problems caused by exposure to phishing attacks that self-phishing will improve?
  - **Description of campaign process:**
    - What is the duration of the campaign?
    - How will the IT team select the email recipients and subjects?
    - How will IT know that vulnerability is improving? What are the goals for improvement moving forward?
  - **Clarification about information managers will receive:**
    - How much detail will the manager be allowed to see regarding vulnerability?
    - How should the manager plan to use this information to support changes in policy or internal planning for the coming year?
  - **How IT plans to use the campaign data:**
    - How will the security team use evidence of vulnerability within departments and associated with specific email types to update future self-phishing modules?
    - How will the security team use self-phishing data to update the online and in-person interactions that all end users go through with the security team?
    - When will IT report on results, and what will they report on?
  - **Clear point of contact for questions:**
    - Who is responsible for the campaign decisions?
    - Who can answer questions from concerned end users?

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Sample Email for Departmental Managers

From: University CISO
To: Dean of the College of Arts and Letters
Cc: University Security Team, University CIO
Subject: 2016 University Self-Phishing Campaign: How It Will Affect Your Department

Dear Dean,

As you may have heard, the IT security team, in partnership with the University Help Desk and IT Governance Group, is conducting a self-phishing campaign in the fall of 2016.

Over the last two years, we have seen a **44% increase in the incidence of monthly new phishing attacks** (i.e., malicious attempts to steal credentials or information through a fake email) on our campus, and despite our efforts to teach constituents about the new risks, the number of successful attacks continues to rise. **Last month, we identified six separate attacks, with over 20 victims affected**; responding to these attacks is draining resources that we desperately need to support new academic and administrative initiatives that can distinguish us from our peers.

Simple metric demonstrates vulnerability

Real campus evidence drives urgency

Over the next six months, the IT team will be using emails sent from our office, but disguised to look like various third parties, to test how vulnerable different parts of campus are to phishing attacks. If a person clicks on the link and "takes the bait," they will immediately be told what has happened, that there are no punitive repercussions, and be directed to a brief online training about what to watch out for in the future. **At many of our peer institutions and other organizations, this has been shown to help individuals by significantly raising their awareness of online threats and how to stay safe**.

Why the dean should care about self-phishing

The campaign will proceed as follows:

- **September 25**: Standard phishing training for all students and semester-start email to all faculty/staff will include notification that the security team will also be self-phishing without warning through the semester.
- **October 15**: First self-phishing email will be sent to all students, promising easy tuition deposit in return for bank account credentials. Those who click will be directed to online phishing detection training; the security team will track all clicks associated with this email.
- After the initial self-phishing email, the security team will use known vulnerabilities to inform ongoing emails and training throughout the semester. **We will send at maximum ten self-phishing emails in the fall semester**.
- In our **Fall Semester Report on November 25**, the security team will include a report on all the self-phishing emails sent during the semester, including the departments affected, numbers falling prey to the campaign, and the number completing training.

Simple schedule of what to expect

However, at no time will managers be given the individual details of email vulnerability or allowed to see which employees and students were affected. This is to ensure that we maintain a cooperative relationship with end-user constituents, who should see self-phishing as a security service consultation rather than an invasive test. Instead, we will provide aggregate information about our performance against goals and update you on how we plan to meet vulnerabilities moving forward.

Clear guidance on what data is available

If you or your staff have any questions, please do not hesitate to reach out to the IT security team by phone at (###) ###-#### or by email at phishingquestions@university.edu. As always, we appreciate the opportunity to help advance the research and teaching missions of our shared home, and look forward to continuing our collaboration in the years to come.

Easy route to additional information

All the best,

Security Director

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Sharing Information with Operational Partners and Vendors

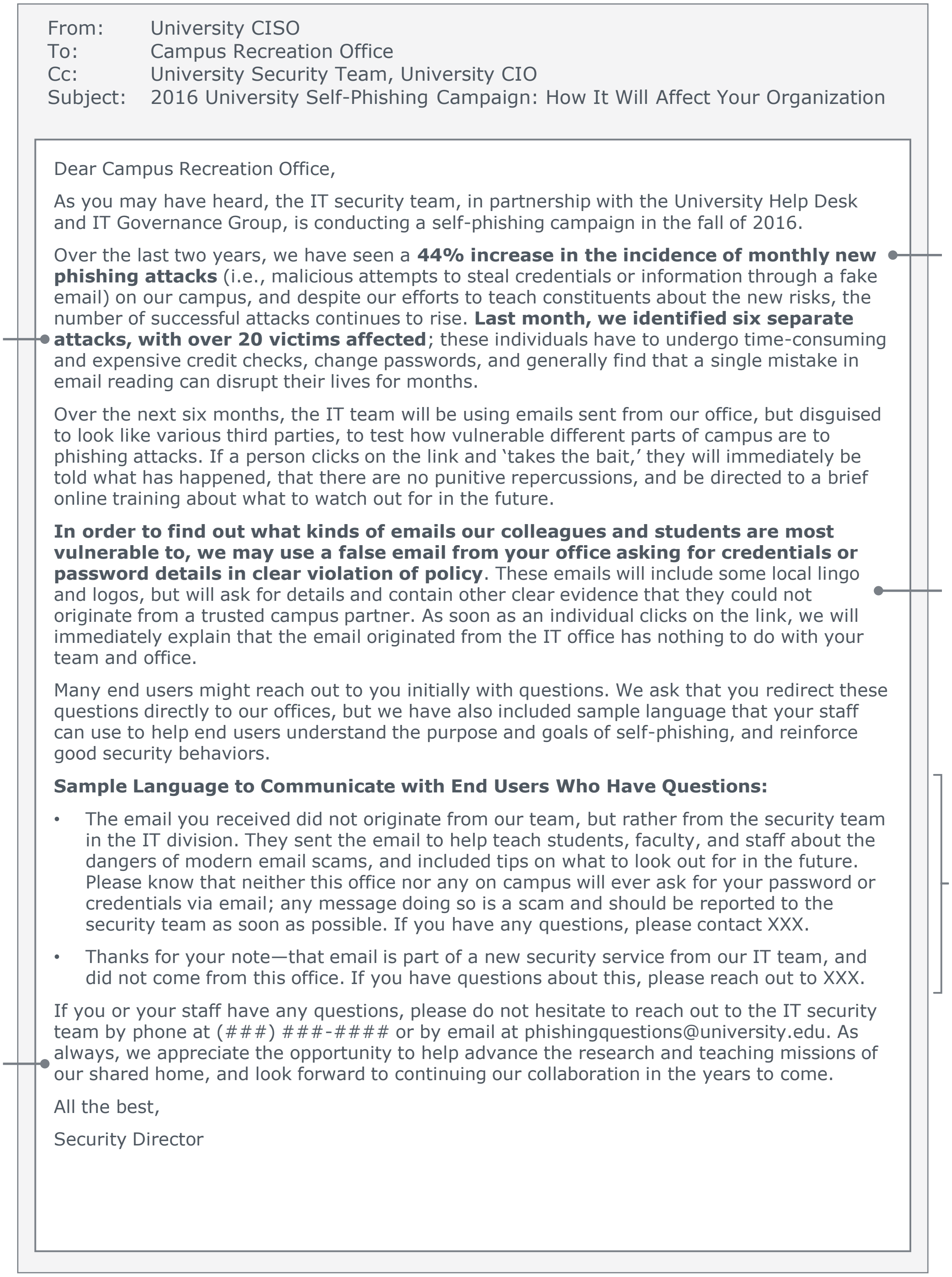
Many of the most damaging phishing schemes involve clever "spear phishes," or carefully designed messages that mimic the look and language of local vendors and offices (e.g., bank on campus where students have direct deposit, campus athletic facilities). To teach end users how to recognize these schemes, the security team needs to show them messages that duplicate this logic, but there are several important items to share with those vendors and offices before the campaign begins.

- **Key Messages to Get Across in Partner and Vendor Pre-wire Communication**
  - **Reason for the campaign:**
    - Why isn't the status quo education and awareness policy enough to protect campus members?
    - What are the specific problems caused by exposure to phishing attacks that self-phishing will improve?
  - **Description of campaign process:**
    - What is the duration of the campaign?
    - How will IT know that vulnerability is improving? What are the goals for improvement moving forward?
  - **How vendor and office could become involved:**
    - In what situations will IT use a false email from the vendor or office to test security?
    - How will IT ensure that the self-phishing email does not affect end users' relationship with vendor or office?
    - How should the vendor or office staff respond to end-user questions about self-phishing campaign if they come up?
  - **How IT plans to use the campaign data:**
    - When will IT report on results, and what will they report on?
  - **Clear point of contact for questions:**
    - Who is responsible for the campaign decisions?
    - Who can answer questions from vendor/office staff and end users?

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Sample Email for Partners and Vendors



From: University CISO
To: Campus Recreation Office
Cc: University Security Team, University CIO
Subject: 2016 University Self-Phishing Campaign: How It Will Affect Your Organization

Dear Campus Recreation Office,

As you may have heard, the IT security team, in partnership with the University Help Desk and IT Governance Group, is conducting a self-phishing campaign in the fall of 2016.

Over the last two years, we have seen a **44% increase in the incidence of monthly new phishing attacks** (i.e., malicious attempts to steal credentials or information through a fake email) on our campus, and despite our efforts to teach constituents about the new risks, the number of successful attacks continues to rise. **Last month, we identified six separate attacks, with over 20 victims affected**; these individuals have to undergo time-consuming and expensive credit checks, change passwords, and generally find that a single mistake in email reading can disrupt their lives for months.

Over the next six months, the IT team will be using emails sent from our office, but disguised to look like various third parties, to test how vulnerable different parts of campus are to phishing attacks. If a person clicks on the link and 'takes the bait,' they will immediately be told what has happened, that there are no punitive repercussions, and be directed to a brief online training about what to watch out for in the future.

In order to find out what kinds of emails our colleagues and students are most vulnerable to, we may use a false email from your office asking for credentials or password details in clear violation of policy. These emails will include some local lingo and logos, but will ask for details and contain other clear evidence that they could not originate from a trusted campus partner. As soon as an individual clicks on the link, we will immediately explain that the email originated from the IT office has nothing to do with your team and office.

Many end users might reach out to you initially with questions. We ask that you redirect these questions directly to our offices, but we have also included sample language that your staff can use to help end users understand the purpose and goals of self-phishing, and reinforce good security behaviors.

Sample Language to Communicate with End Users Who Have Questions:

- The email you received did not originate from our team, but rather from the security team in the IT division. They sent the email to help teach students, faculty, and staff about the dangers of modern email scams, and included tips on what to look out for in the future. Please know that neither this office nor any on campus will ever ask for your password or credentials via email; any message doing so is a scam and should be reported to the security team as soon as possible. If you have any questions, please contact XXX.
- Thanks for your note—that email is part of a new security service from our IT team, and did not come from this office. If you have questions about this, please reach out to XXX.

If you or your staff have any questions, please do not hesitate to reach out to the IT security team by phone at (###) ###-#### or by email at phishingquestions@university.edu. As always, we appreciate the opportunity to help advance the research and teaching missions of our shared home, and look forward to continuing our collaboration in the years to come.

All the best,

Security Director

Simple metric demonstrates vulnerability

Real campus evidence drives urgency

Why the organization should care about self-phishing

Sample language to redirect end users to IT security team

Easy route to additional information

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Supporting the Help Desk Function

IT's partners in the campus help desk are the most likely to be impacted by questions and complaints during a self-phishing campaign, despite efforts to clarify the purpose of the work and embedded suggestions to contact the security team with questions.

- **Key Messages to Get Across in Help Desk Pre-Wire Communication**
  - **Reason for the campaign:**
    - Why isn't the status quo education and awareness policy enough to protect campus members?
    - What are the specific problems caused by exposure to phishing attacks that self-phishing will improve?
  - **Description of campaign process:**
    - What is the duration of the campaign?
    - How will the IT team select the email recipients and subjects?
    - How soon before sending a self-phishing message can the security team brief the help desk about planned recipients and subjects?
    - How many end users will be involved in each email, and how many responses should the help desk expect to field?
    - Where will end users be redirected if they click on the phish?
  - **How help desk staff could become involved:**
    - How should help desk staff respond to end-user questions about self-phishing campaign if they come up?
  - **Clear point of contact for questions:**
    - Who is responsible for the campaign decisions?
    - Who can answer questions from concerned end users?

Self-Phishing Pre-wire Templates

Pre-wire Emails for Campus Partners

Sample Email for Help Desk Workers

From: University CISO
To: Help Desk Team
Cc: University Security Team, University CIO
Subject: 2016 University Self-Phishing Campaign: How It Will Affect The Help Desk

Dear Dean,

As you may have heard, the IT security team, in partnership with the University Help Desk and IT Governance Group, is conducting a self-phishing campaign in the fall of 2016.

Over the last two years, we have seen a **44% increase in the incidence of monthly new phishing attacks** (i.e., malicious attempts to steal credentials or information through a fake email) on our campus, and despite our efforts to teach constituents about the new risks, the number of successful attacks continues to rise. **Last month, we identified six separate attacks, with over 20 victims affected**; responding to these attacks is draining resources that we desperately need to support new academic and administrative initiatives that can distinguish us from our peers.

Simple metric demonstrates vulnerability

Real campus evidence drives urgency

Over the next six months, the IT team will be using emails sent from our office, but disguised to look like various third parties, to test how vulnerable different parts of campus are to phishing attacks. If a person clicks on the link and "takes the bait," they will immediately be told what has happened, that there are no punitive repercussions, and be directed to a brief online training about what to watch out for in the future.

Why Does This Matter to the Help Desk?

Self-phishing emails generate questions and responses which frequently come to IT help desks. Messages will be sent to all students on campus (e.g., we plan to begin this campaign with an email to all students on October 15), but will also target some specific academic and administrative areas where we have evidence of previous vulnerability. As a rule of thumb, **we expect between 10 and 30% of recipients to "take the bait," and a far smaller percentage to reach out to you with questions**. We will notify the help desk with the full details of a planned self-phishing email at least two weeks before it is sent.

Explanation of what to expect from any given phishing message

When end users might reach out to you initially with questions, we ask that you redirect these questions directly to our offices, but we have also included sample language that your staff can use to help end users understand the purpose and goals of self-phishing.

Sample Language to Communicate with End Users Who Have Questions:

- The email you received did not originate from our team, but rather from the security team in the IT division. They sent the email to help teach students, faculty, and staff about the dangers of modern email scams, and included tips on what to look out for in the future. Please know that neither this office nor any on campus will ever ask for your password or credentials via email; any message doing so is a scam and should be reported to the security team as soon as possible. If you have any questions, please contact XXX.
- Thanks for your note—that email is part of a new security service from our IT team, and was sent to help students, faculty, and staff learn about new cyber threats. If you have questions about this, please reach out to XXX.

Sample language to redirect end users to IT security team

If you or your staff have any questions, please do not hesitate to reach out to the IT security team by phone at (###) ###-#### or by email at phishingquestions@university.edu. As always, we appreciate the opportunity to help advance the research and teaching missions of our shared home, and look forward to continuing our collaboration in the years to come.

Easy route to additional information

All the best,

Security Director

Self-Phishing Pre-wire Templates

Pre-wire Emails for Constituents

Explaining Purpose and Consequences to End Users

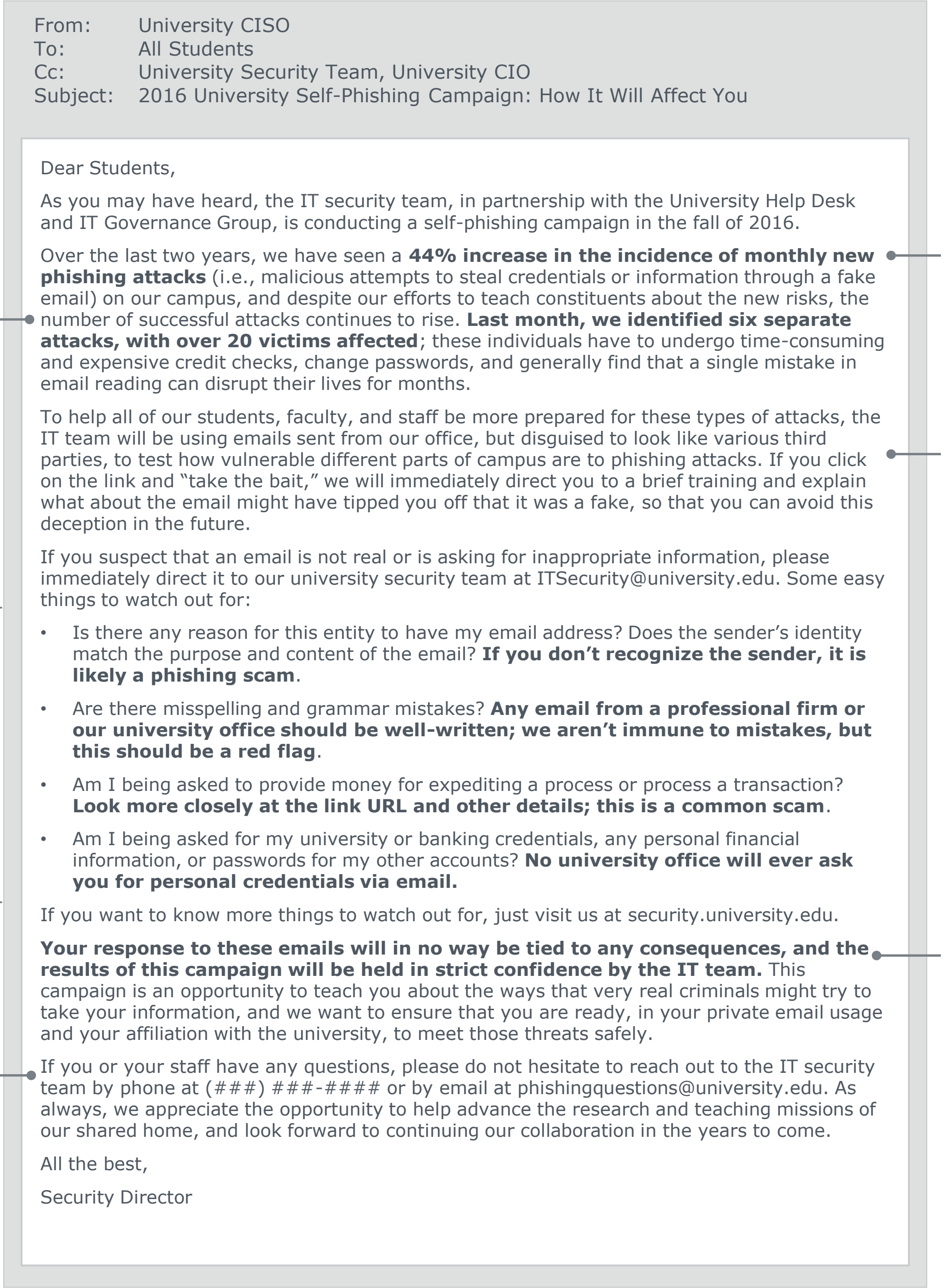
End users can react negatively to self-phishing emails if they perceive the intent as an invasive test that will be used against them. The primary purpose of pre-wire emails to end users is to alleviate those concerns and help constituents understand the new nature of cyber threats.

- **Key Messages to Get Across in Manager Pre-Wire Communication**
  - **Reason for the campaign:**
    - Why isn't the status quo education and awareness policy enough to protect campus members?
    - What are the specific problems caused by exposure to phishing attacks that self-phishing will improve?
  - **Description of campaign process:**
    - What is the duration of the campaign?
    - How will the IT team select the email recipients and subjects?
    - How will IT know that vulnerability is improving? What are the goals for improvement moving forward?
  - **Clarification about information managers will receive:**
    - How much detail will the manager be allowed to see regarding vulnerability?
    - How should the manager plan to use this information to support changes in policy or internal planning for the coming year?
  - **How IT plans to use the campaign data:**
    - How will the security team use evidence of vulnerability within departments and associated with specific email types to update future self-phishing modules?
    - How will the security team use self-phishing data to update the online and in-person interactions that all end users go through with the security team?
    - When will IT report on results, and what will they report on?
  - **Clear point of contact for questions:**
    - Who is responsible for the campaign decisions?
    - Who can answer questions from concerned end users?

Self-Phishing Pre-wire Templates

Pre-wire Emails for Constituents

Sample Email for End Users



From: University CISO
To: All Students
Cc: University Security Team, University CIO
Subject: 2016 University Self-Phishing Campaign: How It Will Affect You

Dear Students,

As you may have heard, the IT security team, in partnership with the University Help Desk and IT Governance Group, is conducting a self-phishing campaign in the fall of 2016.

Over the last two years, we have seen a **44% increase in the incidence of monthly new phishing attacks** (i.e., malicious attempts to steal credentials or information through a fake email) on our campus, and despite our efforts to teach constituents about the new risks, the number of successful attacks continues to rise. **Last month, we identified six separate attacks, with over 20 victims affected**; these individuals have to undergo time-consuming and expensive credit checks, change passwords, and generally find that a single mistake in email reading can disrupt their lives for months.

To help all of our students, faculty, and staff be more prepared for these types of attacks, the IT team will be using emails sent from our office, but disguised to look like various third parties, to test how vulnerable different parts of campus are to phishing attacks. If you click on the link and "take the bait," we will immediately direct you to a brief training and explain what about the email might have tipped you off that it was a fake, so that you can avoid this deception in the future.

If you suspect that an email is not real or is asking for inappropriate information, please immediately direct it to our university security team at ITSecurity@university.edu. Some easy things to watch out for:

- Is there any reason for this entity to have my email address? Does the sender's identity match the purpose and content of the email? **If you don't recognize the sender, it is likely a phishing scam**.
- Are there misspelling and grammar mistakes? **Any email from a professional firm or our university office should be well-written; we aren't immune to mistakes, but this should be a red flag**.
- Am I being asked to provide money for expediting a process or process a transaction? **Look more closely at the link URL and other details; this is a common scam**.
- Am I being asked for my university or banking credentials, any personal financial information, or passwords for my other accounts? **No university office will ever ask you for personal credentials via email.**

If you want to know more things to watch out for, just visit us at security.university.edu.

Your response to these emails will in no way be tied to any consequences, and the results of this campaign will be held in strict confidence by the IT team. This campaign is an opportunity to teach you about the ways that very real criminals might try to take your information, and we want to ensure that you are ready, in your private email usage and your affiliation with the university, to meet those threats safely.

If you or your staff have any questions, please do not hesitate to reach out to the IT security team by phone at (###) ###-#### or by email at phishingquestions@university.edu. As always, we appreciate the opportunity to help advance the research and teaching missions of our shared home, and look forward to continuing our collaboration in the years to come.

All the best,

Security Director

Simple metric demonstrates vulnerability

Real campus evidence drives urgency

How the campaign will affect students

Quick pointers begin the education process

Clear explanation of campaign consequences

Easy route to additional information

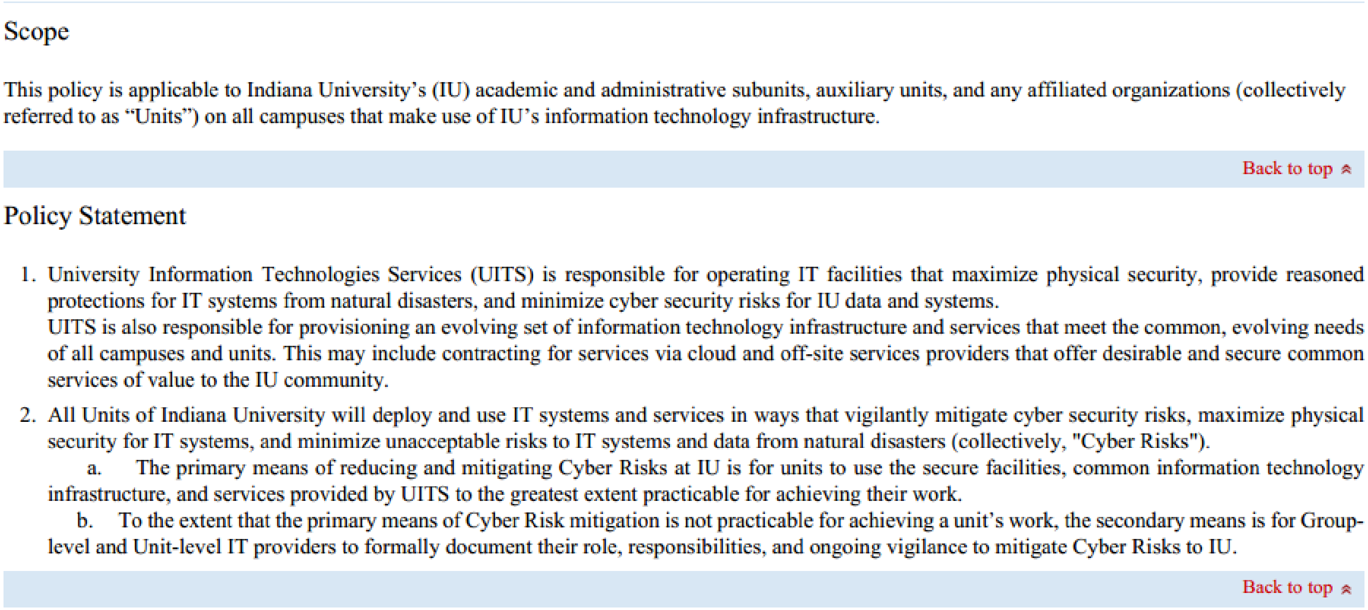
Cyber Risk Mitigation Policy Language

Framing the Shared Benefits of Better Security

The purpose of this tool is to allow IT to build policy around language that has proven to be effective in gaining institution-wide buy-in for security upgrades and migration of servers/technology to a central, secure facility.

The document included on the following pages has been implemented at Indiana University-Bloomington through the process detailed on pages 48-51, a cooperative effort that included IT and departmental stakeholders across campus. Framing the benefits of security to a diverse audience of academic and administrative staff requires significant "advertising" in digital and face-to-face appearances from the CIO and the entire IT team, but institutions that have made progress in this area argue that the benefits of cyber risk mitigation far outweigh the temporary costs.

If writing similar policy on your own campus, ask for input from stakeholders throughout the development phase, especially from units that could have a large number of administrative-use servers and other technologies in the department that could be centralized under new policy.



Scope

This policy is applicable to Indiana University's (IU) academic and administrative subunits, auxiliary units, and any affiliated organizations (collectively referred to as "Units") on all campuses that make use of IU's information technology infrastructure.

Back to top ⮝

Policy Statement

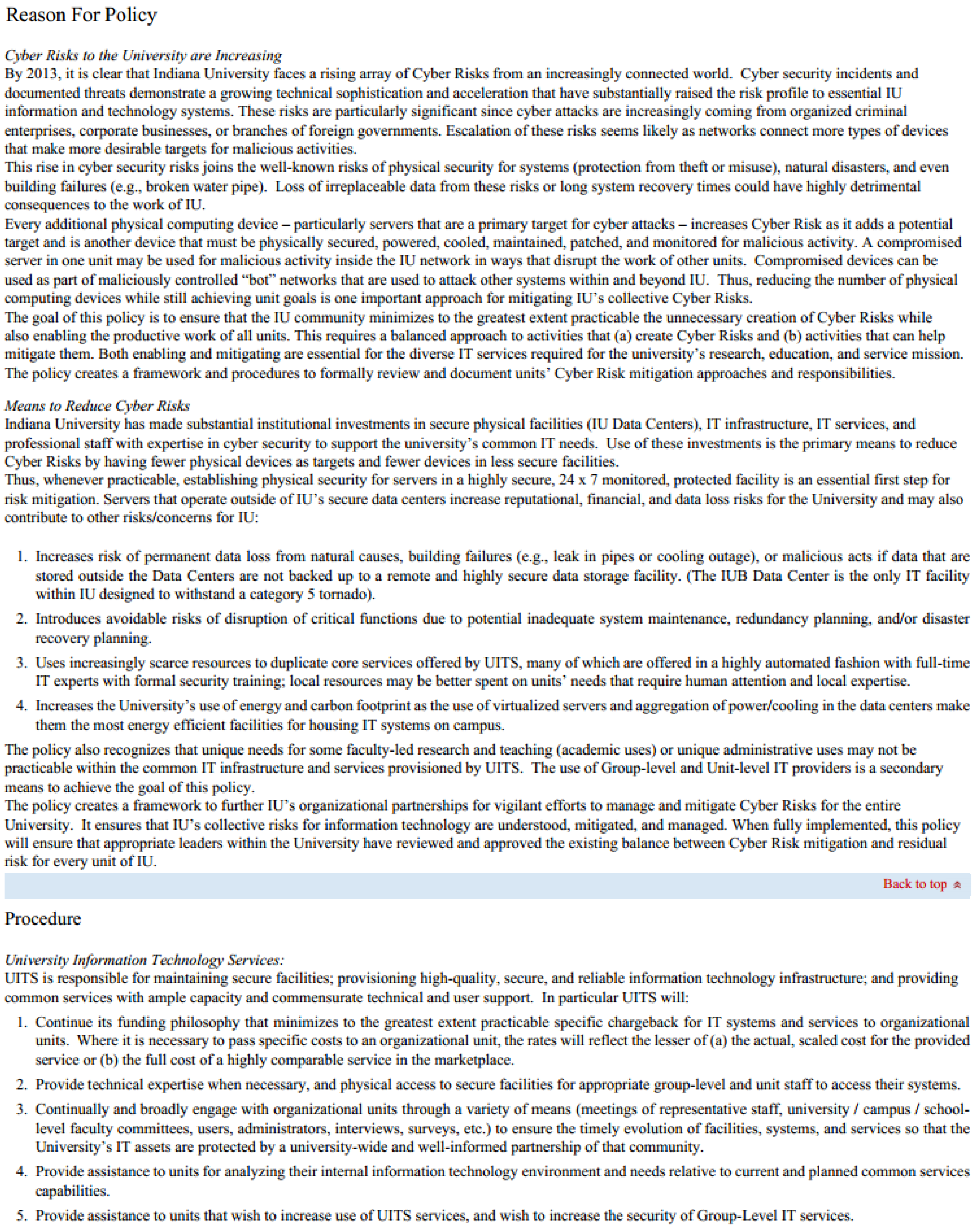
1. University Information Technologies Services (UITS) is responsible for operating IT facilities that maximize physical security, provide reasoned protections for IT systems from natural disasters, and minimize cyber security risks for IU data and systems.
   UITS is also responsible for provisioning an evolving set of information technology infrastructure and services that meet the common, evolving needs of all campuses and units. This may include contracting for services via cloud and off-site services providers that offer desirable and secure common services of value to the IU community.
2. All Units of Indiana University will deploy and use IT systems and services in ways that vigilantly mitigate cyber security risks, maximize physical security for IT systems, and minimize unacceptable risks to IT systems and data from natural disasters (collectively, "Cyber Risks").
   a. The primary means of reducing and mitigating Cyber Risks at IU is for units to use the secure facilities, common information technology infrastructure, and services provided by UITS to the greatest extent practicable for achieving their work.
   b. To the extent that the primary means of Cyber Risk mitigation is not practicable for achieving a unit's work, the secondary means is for Group-level and Unit-level IT providers to formally document their role, responsibilities, and ongoing vigilance to mitigate Cyber Risks to IU.

Back to top ⮝

Note: Taken from Cyber Risk Mitigation Responsibilities, Indiana University, http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml.

Tool 7

Cyber Risk Mitigation Policy Language



Reason For Policy

Cyber Risks to the University are Increasing

By 2013, it is clear that Indiana University faces a rising array of Cyber Risks from an increasingly connected world. Cyber security incidents and documented threats demonstrate a growing technical sophistication and acceleration that have substantially raised the risk profile to essential IU information and technology systems. These risks are particularly significant since cyber attacks are increasingly coming from organized criminal enterprises, corporate businesses, or branches of foreign governments. Escalation of these risks seems likely as networks connect more types of devices that make more desirable targets for malicious activities.

This rise in cyber security risks joins the well-known risks of physical security for systems (protection from theft or misuse), natural disasters, and even building failures (e.g., broken water pipe). Loss of irreplaceable data from these risks or long system recovery times could have highly detrimental consequences to the work of IU.

Every additional physical computing device – particularly servers that are a primary target for cyber attacks – increases Cyber Risk as it adds a potential target and is another device that must be physically secured, powered, cooled, maintained, patched, and monitored for malicious activity. A compromised server in one unit may be used for malicious activity inside the IU network in ways that disrupt the work of other units. Compromised devices can be used as part of maliciously controlled "bot" networks that are used to attack other systems within and beyond IU. Thus, reducing the number of physical computing devices while still achieving unit goals is one important approach for mitigating IU's collective Cyber Risks.

The goal of this policy is to ensure that the IU community minimizes to the greatest extent practicable the unnecessary creation of Cyber Risks while also enabling the productive work of all units. This requires a balanced approach to activities that (a) create Cyber Risks and (b) activities that can help mitigate them. Both enabling and mitigating are essential for the diverse IT services required for the university's research, education, and service mission. The policy creates a framework and procedures to formally review and document units' Cyber Risk mitigation approaches and responsibilities.

Means to Reduce Cyber Risks

Indiana University has made substantial institutional investments in secure physical facilities (IU Data Centers), IT infrastructure, IT services, and professional staff with expertise in cyber security to support the university's common IT needs. Use of these investments is the primary means to reduce Cyber Risks by having fewer physical devices as targets and fewer devices in less secure facilities.

Thus, whenever practicable, establishing physical security for servers in a highly secure, 24 x 7 monitored, protected facility is an essential first step for risk mitigation. Servers that operate outside of IU's secure data centers increase reputational, financial, and data loss risks for the University and may also contribute to other risks/concerns for IU:

1. Increases risk of permanent data loss from natural causes, building failures (e.g., leak in pipes or cooling outage), or malicious acts if data that are stored outside the Data Centers are not backed up to a remote and highly secure data storage facility. (The IUB Data Center is the only IT facility within IU designed to withstand a category 5 tornado).
2. Introduces avoidable risks of disruption of critical functions due to potential inadequate system maintenance, redundancy planning, and/or disaster recovery planning.
3. Uses increasingly scarce resources to duplicate core services offered by UITS, many of which are offered in a highly automated fashion with full-time IT experts with formal security training; local resources may be better spent on units' needs that require human attention and local expertise.
4. Increases the University's use of energy and carbon footprint as the use of virtualized servers and aggregation of power/cooling in the data centers make them the most energy efficient facilities for housing IT systems on campus.

The policy also recognizes that unique needs for some faculty-led research and teaching (academic uses) or unique administrative uses may not be practicable within the common IT infrastructure and services provisioned by UITS. The use of Group-level and Unit-level IT providers is a secondary means to achieve the goal of this policy.

The policy creates a framework to further IU's organizational partnerships for vigilant efforts to manage and mitigate Cyber Risks for the entire University. It ensures that IU's collective risks for information technology are understood, mitigated, and managed. When fully implemented, this policy will ensure that appropriate leaders within the University have reviewed and approved the existing balance between Cyber Risk mitigation and residual risk for every unit of IU.

Back to top ⮝

Procedure

University Information Technology Services:

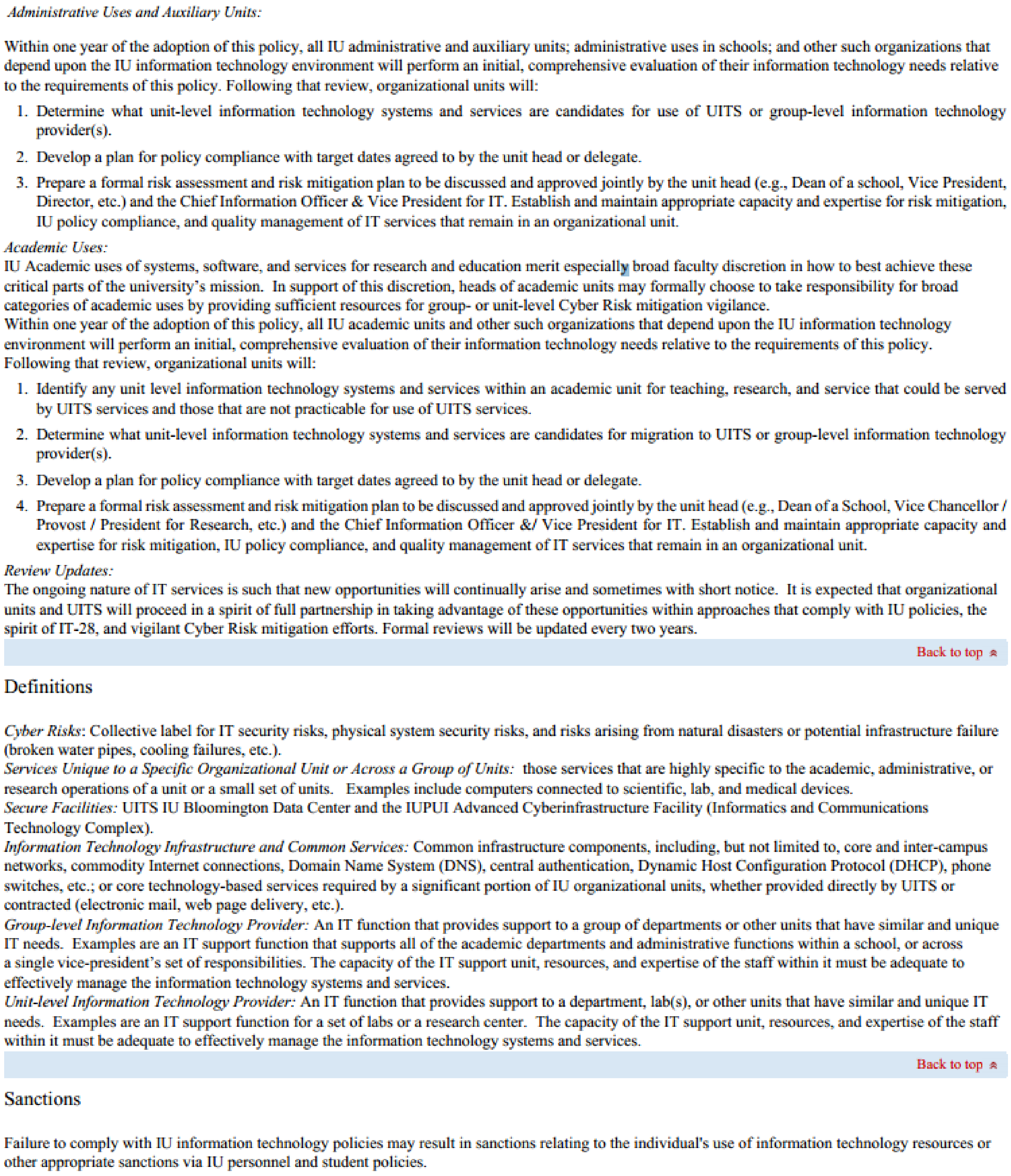
UITS is responsible for maintaining secure facilities; provisioning high-quality, secure, and reliable information technology infrastructure; and providing common services with ample capacity and commensurate technical and user support. In particular UITS will:

1. Continue its funding philosophy that minimizes to the greatest extent practicable specific chargeback for IT systems and services to organizational units. Where it is necessary to pass specific costs to an organizational unit, the rates will reflect the lesser of (a) the actual, scaled cost for the provided service or (b) the full cost of a highly comparable service in the marketplace.
2. Provide technical expertise when necessary, and physical access to secure facilities for appropriate group-level and unit staff to access their systems.
3. Continually and broadly engage with organizational units through a variety of means (meetings of representative staff, university / campus / school-level faculty committees, users, administrators, interviews, surveys, etc.) to ensure the timely evolution of facilities, systems, and services so that the University's IT assets are protected by a university-wide and well-informed partnership of that community.
4. Provide assistance to units for analyzing their internal information technology environment and needs relative to current and planned common services capabilities.
5. Provide assistance to units that wish to increase use of UITS services, and wish to increase the security of Group-Level IT services.

Note: Taken from Cyber Risk Mitigation Responsibilities, Indiana University, http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml.

Tool 7

Cyber Risk Mitigation Policy Language



Administrative Uses and Auxiliary Units:

Within one year of the adoption of this policy, all IU administrative and auxiliary units; administrative uses in schools; and other such organizations that depend upon the IU information technology environment will perform an initial, comprehensive evaluation of their information technology needs relative to the requirements of this policy. Following that review, organizational units will:

1. Determine what unit-level information technology systems and services are candidates for use of UITS or group-level information technology provider(s).
2. Develop a plan for policy compliance with target dates agreed to by the unit head or delegate.
3. Prepare a formal risk assessment and risk mitigation plan to be discussed and approved jointly by the unit head (e.g., Dean of a school, Vice President, Director, etc.) and the Chief Information Officer & Vice President for IT. Establish and maintain appropriate capacity and expertise for risk mitigation, IU policy compliance, and quality management of IT services that remain in an organizational unit.

Academic Uses:
IU Academic uses of systems, software, and services for research and education merit especially broad faculty discretion in how to best achieve these critical parts of the university's mission. In support of this discretion, heads of academic units may formally choose to take responsibility for broad categories of academic uses by providing sufficient resources for group- or unit-level Cyber Risk mitigation vigilance.
Within one year of the adoption of this policy, all IU academic units and other such organizations that depend upon the IU information technology environment will perform an initial, comprehensive evaluation of their information technology needs relative to the requirements of this policy. Following that review, organizational units will:

1. Identify any unit level information technology systems and services within an academic unit for teaching, research, and service that could be served by UITS services and those that are not practicable for use of UITS services.
2. Determine what unit-level information technology systems and services are candidates for migration to UITS or group-level information technology provider(s).
3. Develop a plan for policy compliance with target dates agreed to by the unit head or delegate.
4. Prepare a formal risk assessment and risk mitigation plan to be discussed and approved jointly by the unit head (e.g., Dean of a School, Vice Chancellor / Provost / President for Research, etc.) and the Chief Information Officer &/ Vice President for IT. Establish and maintain appropriate capacity and expertise for risk mitigation, IU policy compliance, and quality management of IT services that remain in an organizational unit.

Review Updates:
The ongoing nature of IT services is such that new opportunities will continually arise and sometimes with short notice. It is expected that organizational units and UITS will proceed in a spirit of full partnership in taking advantage of these opportunities within approaches that comply with IU policies, the spirit of IT-28, and vigilant Cyber Risk mitigation efforts. Formal reviews will be updated every two years.

Back to top ⌃

Definitions

Cyber Risks: Collective label for IT security risks, physical system security risks, and risks arising from natural disasters or potential infrastructure failure (broken water pipes, cooling failures, etc.).
Services Unique to a Specific Organizational Unit or Across a Group of Units: those services that are highly specific to the academic, administrative, or research operations of a unit or a small set of units. Examples include computers connected to scientific, lab, and medical devices.
Secure Facilities: UITS IU Bloomington Data Center and the IUPUI Advanced Cyberinfrastructure Facility (Informatics and Communications Technology Complex).
Information Technology Infrastructure and Common Services: Common infrastructure components, including, but not limited to, core and inter-campus networks, commodity Internet connections, Domain Name System (DNS), central authentication, Dynamic Host Configuration Protocol (DHCP), phone switches, etc.; or core technology-based services required by a significant portion of IU organizational units, whether provided directly by UITS or contracted (electronic mail, web page delivery, etc.).
Group-level Information Technology Provider: An IT function that provides support to a group of departments or other units that have similar and unique IT needs. Examples are an IT support function that supports all of the academic departments and administrative functions within a school, or across a single vice-president's set of responsibilities. The capacity of the IT support unit, resources, and expertise of the staff within it must be adequate to effectively manage the information technology systems and services.
Unit-level Information Technology Provider: An IT function that provides support to a department, lab(s), or other units that have similar and unique IT needs. Examples are an IT support function for a set of labs or a research center. The capacity of the IT support unit, resources, and expertise of the staff within it must be adequate to effectively manage the information technology systems and services.

Back to top ⌃

Sanctions

Failure to comply with IU information technology policies may result in sanctions relating to the individual's use of information technology resources or other appropriate sanctions via IU personnel and student policies.

Note: Taken from Cyber Risk Mitigation Responsibilities, Indiana University, http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml.