EAB

Addressing Persistent and Emerging **Campus Risks**

Foundational Capabilities for Enterprise Risk Management, Information Risk, and Student Activism

Business Affairs Forum

EAB

Addressing Persistent and Emerging Campus Risks

Foundational Capabilities for Enterprise Risk Management, Information Risk, and Student Activism

Business Affairs Forum

Business Affairs Forum

Project Director

Laura Whitaker

Managing Director

John Workman, PhD

Design Consultant

Lilith James

Table of Contents

Supporting Members in Best Practice Implementation

Resources Available Within Your Membership

This publication is only the beginning of our work to assist members in optimizing annual giving. Recognizing that ideas seldom speak for themselves, our ambition is to work actively with members of the Business Affairs Forum to decide which practices are most relevant for your organization, to accelerate consensus among key constituencies, and to save implementation time.

We offer a variety of services to assist you with your mission. For additional information about any of the services detailed below, please contact your organization's relationship manager or visit our website at eab.com. To order additional copies of this publication, please search for it by title on eab.com.

Implementation Road Maps and Tools

Throughout the publication, this symbol will alert you to any corresponding tools and templates available in the Toolkit at the back of this book. These tools are also available on our website at eab.com.

Recorded and Private-Label Webconference Sessions

Our website includes recordings of webconferences walking through the practices highlighted in this publication. Forum experts are also available to conduct private webconferences with your team.

Unlimited Expert Troubleshooting

Members may contact the consultants who worked on any report to discuss the research, troubleshoot obstacles to implementation, or run deep on unique issues. Our staff conducts hundreds of telephone consultations every year.

Facilitated Onsite Presentations

Our experts regularly visit campuses to lead half-day to day-long sessions focused on highlighting key insights for senior leaders or helping internal project teams select the most relevant practices and determine next steps.

To access the full range of services available to you, please visit our website at eab.com/baf.

Beyond Business Affairs: Student Affairs and IT Forums

In addition to the resources available through the Business Affairs Forum membership, EAB offers programs focused on the priorities of additional members of the President's Cabinet and campus leadership. Each of these programs offers its executives content-rich roundtable meetings, virtual educational opportunities via webinars for staff development, and unmetered access to program research experts. This report draws on the IT security and campus activism research from the programs below.

Student Affairs Forum

Inspiring Staff Innovation, Fostering Implementation

EAB's Student Affairs Forum produces best practice research and data capabilities in support of student affairs leaders' highest priorities.

Signature Membership Features

- Campus Climate Survey
- Online database of best practice reports and associated implementation toolkits. Areas of focus include:
  - Transforming the First Generation College Student Experience
  - Responding to Students of Concern
  - Supporting International Students on Campus

IT Forum

Unlocking the Power of Data, Guiding Transformation

EAB's IT Forum produces best practice research and data capabilities in support of CIOs' and their team members' highest priorities.

Signature Membership Features

- IT Maturity Diagnostic
- Data Governance Readiness Assessment
- Functional Collaborative on Security

Contact Us

For additional information on these offerings, visit:
https://www.eab.com/saf or https://www.eab.com/itf

Executive Summary

Support for formalized risk management is growing within higher education, driven by board and leadership awareness of today's increasingly complex environment. Institutions' risk profiles are growing wider for a number of reasons—new growth initiatives, research partnerships beyond the institution, connection to the digital world, and burgeoning student activism.

However, many campuses' **attempts at holistic risk management efforts collapse when moving from intent to action**. The common pitfalls that hamper execution include:

- Distractions arise whenever an incident—be it a data breach or a campus protest that spirals into conflict—requires a heroic response. When institutions do not have plans in place for such occasions, these balloon in significance and divert energy and attention away from implementing sustainable risk management practices.
- When risk managers aim too high, they can develop treatment plans that are implausibly huge and not matched with adequate management capability. Too often risk managers declare victory upon assembling a risk register, and the lack of follow-through means that the plans sit on the shelf.
- Finally, treatment plans tend to lack accountability. Unit-level autonomy hampers the center in implementing risk plans.

The Business Affairs Forum first investigated risk management in 2012, conducting nearly 150 interviews with practitioners in higher education and beyond. The resulting study is entitled *A Practical Approach to Institutional Risk Management*. Since then, conditions on the ground have evolved, and EAB is releasing this shorter brief to help readers quickly prioritize where to start. It incorporates insights from more recent projects undertaken by EAB's IT Forum and Student Affairs Forum regarding information security and campus activism, respectively.

Addressing the issues that can derail risk management initiatives, EAB recommends that campuses **approach the effort in three phases**:

1. Develop contingency response plans for rapid-onset risk areas
2. Focus on building foundational capabilities in enterprise risk, IT security awareness, and campus activism engagement
3. Expand risk treatment and mitigation efforts by engaging campus partners

Persistent and Emerging Risks

Review of Higher Education's Risk Terrain

INTRODUCTION

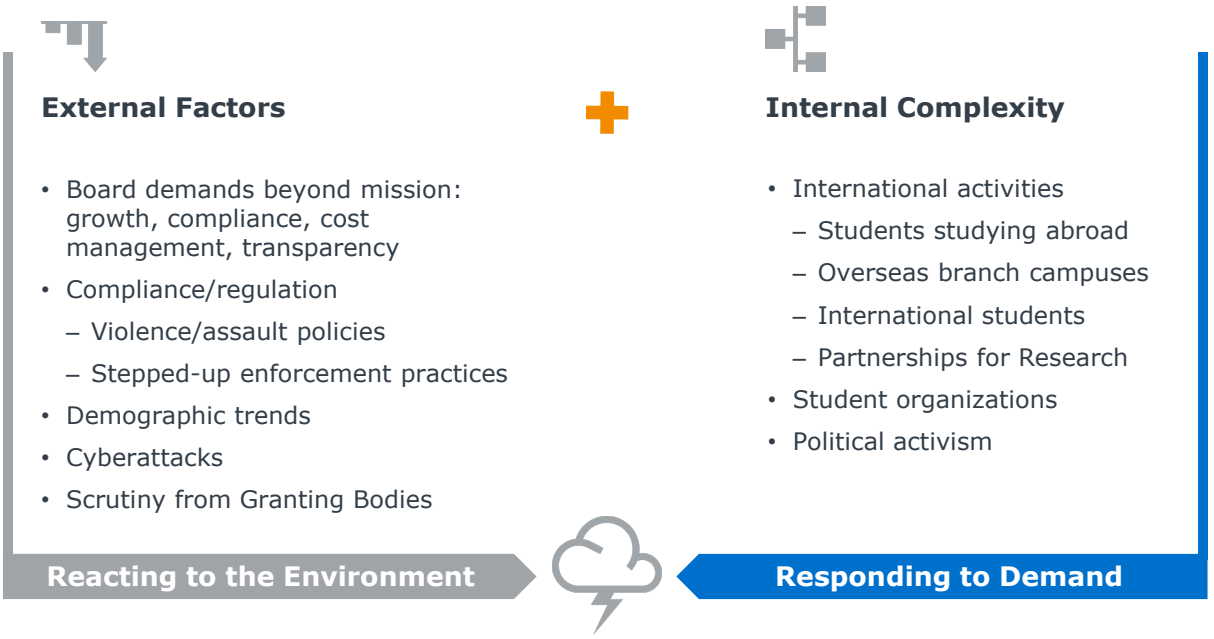
- The Risk Terrain in Higher Education
- Hurdles in the Way of ERM Implementation
- Quick-Start Guide to Risk Management

A Top Expectation for the Chief Business Officer

CBOs on the Hook for Risk, Responding to Pressures from Without and Within

College and university stakeholders—trustees, funders, students, parents, community members, legislators, alumni—are holding their institutions to high standards. Seen as stewards of resources and pillars of the community, these increasingly complex enterprises experience more and more risks.

Flashpoints that have come under continued public scrutiny include financial management, academic ethics, free speech, student conduct, sexual violence, data breaches, demonstrations, and athletic scholarship compliance. As institutions occupy a space that spans roles as lender, teacher, landlord, banker, social chair, counselor, and even *in loco parentis*, administrators must stay on top of the growing list of risk exposures.



Chief business officers share the responsibility for addressing these risks with other leaders on campus. Certainly, the institution's legal staff, IT, student affairs, and other department administrators have key roles to play. However, the burden of leading the charge to address risks as an intentional, managed program falls mainly to the CBO.

This short study assembles resources from across EAB to provide a launch pad for CBOs seeking to make the case for risk management, equip their campus partners with rapid-response plans, and map a path forward to an ongoing program that protects and sustains the institution.

Source: EAB interviews and analysis.

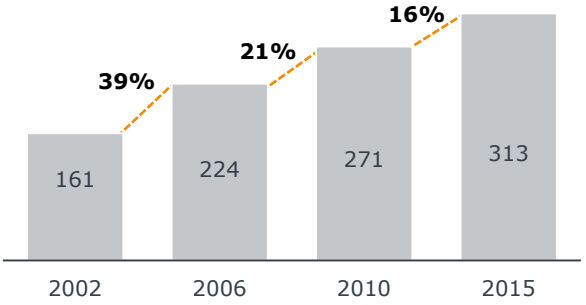
Making the Case: Global and Local Contours of Risk

International Activities, Community Scrutiny Leave Minimal Margin for Error

Among the data points that a CBO may point to when building a business case for a risk management program is the growing complexity of the student body. Data below details both study abroad activities and increasing enrollment of international students. In addition to quantitative increases, campuses experience qualitatively riskier elements of cross-border learning.

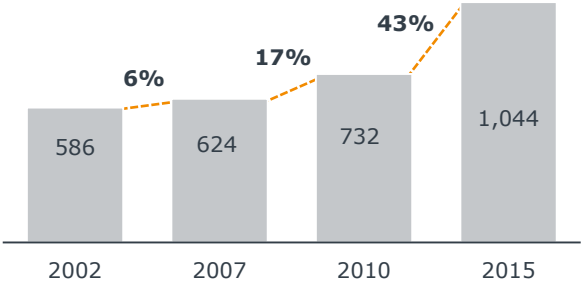
Study Abroad

US Students Abroad (in thousands)



International Students

International Students in U.S. (in thousands)



Risk Exposures

- Students going farther afield—Australia, South Africa, and India hit top 15 destinations since 2001
- Risks moving beyond basic medical, alcohol, or behavioral incidents—Zika virus travel restrictions; Visa restrictions
- Students coming from farther afield—South Korea, Saudi Arabia, Vietnam hit top 15 origin countries since 2001
- Revenue Dependency: 47% of International Students in U.S. from China and India (31% from China alone)

Another factor that can persuade skeptics of the need to proactively address vulnerabilities is the reliance of campuses on public goodwill—for funding, enrollment, and community support—which creates an additional dimension of risk. As the agendas of campus stakeholders and the media may diverge, publicity of internal practices can be politicized in unanticipated ways.

Source: Institute of International Education Fast Facts 2001-2016; EAB interviews and analysis.

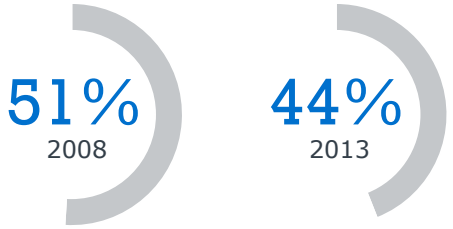
The Solution? ERM Boosts Regular Risk Discussions

Increased Incorporation of ERM into Campus Practice

Enterprise Risk Management, or ERM, is an intentional, holistic approach to managing an organization's awareness and remediation of risks, more widely used in the private sector.

Higher education is getting on board here, if slowly. One way to measure this is by quantifying the means of addressing risks—specifically, is it done proactively, or in some ad hoc way. Data from AGB shows a small, but noteworthy decrease in reliance on reactive, ad hoc meetings.

Reduced Reliance on Ad Hoc Meetings



"By establishing ERM as a regularly repeated business process, leadership avoids the trap of trying to achieve a single 'perfect' process or result, which can take years and sink the most promising ERM effort."

Association of Governing Boards

Issues Generating Ad Hoc Discussions

- Financial underperformance
- Enrollment declines
- High profile event
- Research compliance
- Cyber security
- Legal or regulatory compliance
- Student health and safety
- State budget cuts
- New academic programs

However, there is still no shortage of ad hoc discussions, and many are focused on recurring, persistent, and predictable themes that make them viable candidates for ERM.

Source: https://www.agb.org/sites/default/files/legacy/RiskSurvey2014.pdf; EAB interviews and analysis.

Challenging to Get Arms Around Endless Registers

Sprawling Priorities Defy Easy Sorting and Focus

One of the largest barriers to applying private-sector ERM tactics in higher education sector is simply how burdensome the risk identification process is. A "risk register" is the mechanism that organizations use to inventory all relevant risks. At universities these risk registers can run to the hundreds of lines, with a 400-point risk register being fairly common. This stands in contrast to mature risk organizations in the private sector where initial risk registers generally come in under 50 and ultimately focus on a fraction of those.

For many institutions, the administrative intensity of compiling the list can make ERM a non-starter. Beyond the initial compilation, leaders are paralyzed by the prospect of trying to triage and treat 200 to 500 risks. Compounding this problem, risks are often conflated. Specifically, many risk registers contain risks of varying altitudes – such as systemic risks and operational risks –without regard for this differentiation.

Lacking a method to sort out these tiers, institutions struggle to identify which risks they would recommend for formal treatment.

University's Attempts to Be "Comprehensive" Lead to Unrealistic Results

University Risk Register (Illustrative)

1. Sustainability of high-cost/high-discount pricing model
2. Inability to properly manage academic records
3. Research misconduct
4. Declining public perception of value of liberal arts degree
5. Laboratory safety lapses
6. Misappropriation of research grant costs
7. Unauthorized modification of data
8. Sustainability of student indebtedness levels
9. Inability to meet retention targets
10. Improper use of motor vehicles by students
11. Vandalism to university property
12. Failure to meet institutional enrollment targets
13. HIPAA compliance
14. Inability to meet liquidity targets due to market fluctuations

…

300. Improper receipt/recording of gifts
301. Failure to comply with faculty hiring processes
302. Inappropriate use of university logo or insignia
303. Lack of compliance with smoking regulations

Pitfalls of Average University Risk Register

Inflated Risk Register

Average risk register identifies 200-500 risks—more risks than can be addressed by the institution

Conflated Risks

Attempts to be comprehensive lead to identifying risks of different "altitudes:"

- Sustainability of high-cost/high-discount pricing model
- Inadequate controls over cash receipts
- Inability to meet enrollment targets

Source: EAB interviews and analysis.

The Opportunity Cost of Being Reactive

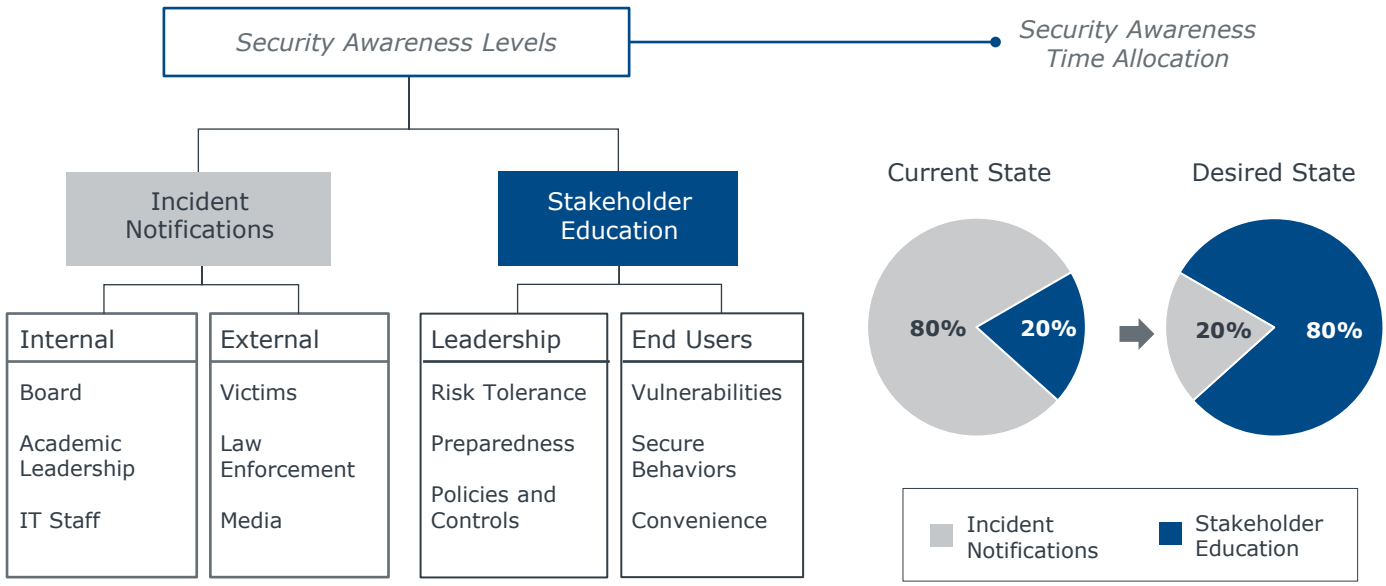
Leaders Struggle to Hold Partners' Attention When Campus in 'Respond' Mode

Moreover, institutions must ensure that their holistic risk management push is paired with a full suite of "crisis" plans. Without these in place, responding to unanticipated incidents (e.g., compromised passwords, a social media-fueled impromptu protest) distracts campus leaders from focusing on sustainable risk mitigation and preparedness efforts.

Because of heightened sensitivity, a charged political climate, the 24/7 news and social media scrutiny, campuses are experiencing amplified reactions to all sorts of stimuli. When no plan exists, leaders scramble to respond, coordinating disparate stakeholders and exhausting those who must quarterback such efforts.

This is particularly acute with incidents involving campus risk, IT breaches, and student activism.

Illustrating the Issue: Complementary (Competing?) Levels of Security 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: https://www.agb.org/sites/default/files/legacy/RiskSurvey2014.pdf; EAB interviews and analysis.

Quick-Start Guide to Risk Management

A practical approach to risk management requires solidifying credibility, building core capabilities that will ensure a viable and sustainable approach to risk, and then expanding across campus. The three phases are depicted below.

Phases for Rapid Acceleration of Risk Management Efforts

Basic Hygiene	Foundational Capability-Building	Partner Engagement and Accountability
Key player Principal executives (CBO, VPSA, CIO)	**Additional players** Audit Committee Chair, Chief Information Security Officer (CISO), Head of Campus Safety	**Additional players** Faculty leadership, campus and community stakeholders
Institutional Risk Management		
• Gain executive buy-in for risk management effort	• Establish right-sized governance • Build a manageable Risk Register *See Appendix*	• Assess and prioritize risks • Increase campus risk awareness • Instill accountability and incentivize action
Information Security		
• Build a breach response toolkit *See Appendix*	• Build channel for Board education • Create unit-level risk profiles • Leverage technology to ID vulnerabilities	• Stand up risk scorecards for units • Roll out incentives for secure behavior
Student Activism		
• Build event response playbook *See Tactic 1 of Navigating the New Wave of Student Activism, available on eab.com*	• Open channels for engagement or interventions with potential activists • Build platform for just-in-time guidance	• Lean in to activism with community engagement • Involve a cross-campus team for long-term change

These tactics are included in this report

These tactics are available through other EAB resources

More Resources on Risk Management from EAB

- A Practical Approach to Institutional Risk Management, 2012
- Elevating Information Security Awareness, 2015
- Navigating the New Wave of Student Activism, 2017

Source: EAB interviews and analysis.

Foundation-Building Guide: Enterprise Risk

Based on *A Practical Approach to Institutional Risk Management: Getting Risk Right in an Era of Constrained Administrative Resources*

SECTION 1

- Tactic 1: Targeted Risk Governance
- Tactic 2: Disciplined Risk Altitudes
- Tactic 3: Peer-Sourced Risk Register
- Tactic 4: Risk Velocity Assessment

Corporate Brethren Positioned for Results

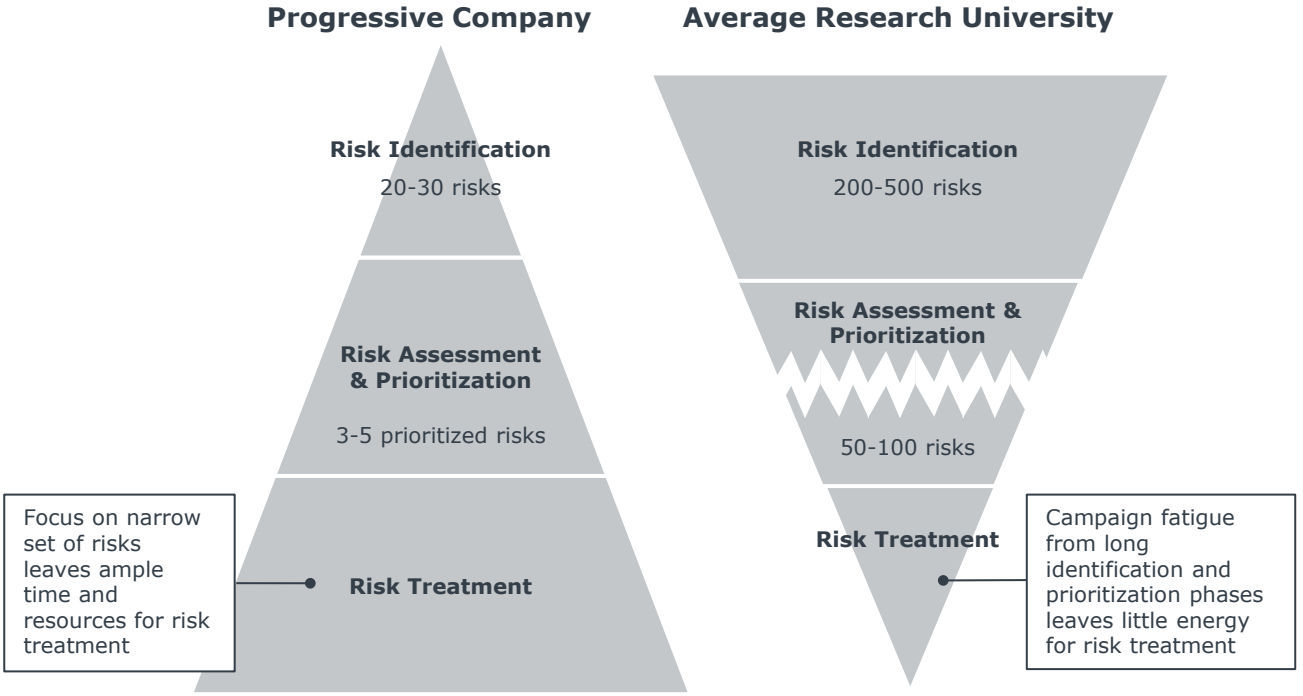
Private Sector Can Move Quickly from Risk Identification to Treatment

Mature private sector risk organizations—in contrast to higher education institutions —generally manage risks off a register numbering in the dozens, not the hundreds. The ability to set clear parameters around risk identification, leveraged off well-defined and concise strategic plans, allows private sector companies to devote the majority of their time on risk treatment.

Higher education's culture of inclusivity and openness—an inarguable strength for many aspects of the mission—can sometimes hinder a disciplined risk focus. An illustrative pyramid of energy expenditure—representing time and effort spent during various phase of a project—stands on its head for higher education organizations. Risk management projects in higher education often start with a massive investment of time in identifying a list of risks, then cull out 75-80% of the "less important" risks. The remaining time and patience must be spread across a list of 50-100 risks that are deemed worthy of treatment. The campus usually suffers from campaign fatigue at this point, leaving little energy or time for risk treatment.

Private Sector More Focused on Risk Treatment Than Identification

Effort Spent on Various Phases of Institutional Risk Management



Source: EAB interviews and analysis.

Enterprise Risk Management Foundational Essentials

Mandate in Brief

Finance and administrative executives seeking to professionalize their campuses' approach to risk management attain critical stakeholder support by clarifying governance roles, preventing scope sprawl, and accelerating progress.

Rationale

While board members, faculty, staff, and other campus community members bring varying perspectives on risks facing the institution, only the CBO is in a position to sort out and prioritize areas for treatment. These stakeholders' voices, in aggregate, would require an untenable effort to account for and efforts to place inclusivity over efficiency will doom

By assigning oversight that includes a comprehensive set of viewpoints, defining the scope of oversight and what is included (and excluded) from the formal risk management process, risk managers can increase the odds of broad campus support for focused treatment of key risks.

Essential Tactics

Tactic 1: Targeted Risk Governance

Risk leaders stand up a bicameral governance structure and a clearly delineated Board oversight charter. These structures sharpen the focus of the three bodies: the manager-level group resolving operational risks, a cabinet-level committee addressing institutional risks, and the Board building out response scenarios for sector-level risks.

Tactic 2: Disciplined Risk Altitudes

Risk committees establish principled sorting methods to avoid conflating the measurement, assessment, prioritization and treatment of operational, institutional, and sector-level risks.

Tactic 3: Peer-Sourced Risk Register

Organizations use existing risk registers to inventory and classify areas of concerns. Leveraging peers' efforts accelerates progress in this early phase and builds credibility for the project.

Tactic 4: Risk Velocity Assessment

Risk leaders move beyond simplistic "likelihood" and "impact" assessment weightings to factor in risks' speed of impact. Taking into account the time horizon of potential risks further clarifies planning and treatment prioritization.

Please see the Risk Register Strawman that accompanies this publication.

Source: EAB interviews and analysis.

Clarifying Ownership from the Committee on Up

Admin Leadership and Board Structure Bicameral Committees

Two common challenges facing organizations standing up risk management is underinvesting in a clearly outlined governance approach that encompasses efforts from staff, administration, and the Board.

At the management level, a frequent misperception is a single governance body will be the right approach. The challenge of inventorying, assessing, prioritizing, treating, and monitoring risks is demonstrably too much for a single risk management committee. A body with representatives addressing everything from strategic risks to operational and compliance risks can find itself stretched too thin. The committee's sweeping mandate, coupled with wide disparities in the backgrounds of members, leads to an unnecessarily slow vetting process and wasted time for both executives and frontline staff.

Similarly, involvement from an active Board may cross the line from well-meaning to distracting. CBOs are challenged to identify the right level of Board involvement, trying to manage the tension of keeping Board members abreast of institutional risks while also trying to prevent "over-involvement" by the Board.

Progressive institutions adopt a tiered committee structure for risk identification and mitigation, and adopt a charter that spells out roles for Board and administration to work effectively in parallel.

Best Practitioner Approach	Key Animating Principle
Element 1: Tiered Risk Committees	
An Institutional Risk Committee, comprising the President's cabinet plus a few key administrators, manages strategic and reputational risks. A Unit-Level Risk Committee, comprising representatives from key operational areas, manages compliance, operational, and financial risks and appoints risk owners within each of their respective units.	Tiers put to best use the respective expertise of senior administrators and unit-level managers, thus improving the focus and efficacy of risk discussions and conserving valuable time for all participants.
Element 2: Role-Defining Board Charter	
Progressive institutions clearly delineate in Board Committee charters that the process of managing risks is central to the Board while actual management of risks remains in the hands of the university administrators.	Clearly written charter delineates Board responsibilities and university administration responsibilities.

Source: EAB interviews and analysis.

Structure for Clarity, Channels for Communications

A critical element that makes this structure effective is ensuring a flow of information between the committees. By briefing each other, the institutional committee receives context for what the unit-level is doing, and the unit-level committee gets credit for being accountable. This pattern also builds a method for the unit-level committee to elevate risks as warranted.

Trading Off Monolithic Risk Committee Structure for Division of Labor

Institutional Risk Committee

Focus: Strategic & Reputational Risks

President's Cabinet

- President
- Exec. VP for Finance & Admin
- Exec. VP for Academic Affairs
- SVP and General Counsel
- SVP and Dean for Campus Life
- VP and Secretary
- VP of Communications
- SVP for Development and Alumni Relations
- Exec. VP for Health Affairs
- Pres. & CEO of Medical Center

- Risk functions overseen:
  - Strategic risks
  - Entity-wide risks
  - Cross-unit risk
- Meets five to seven times per year

Unit-Level Risk Committee

Focus: Compliance, Operational, and Financial Risks

VPs & Directors

- Chief Risk Officer
- Chief Audit Officer
- VP of Investments
- VP of Finance
- VP for Research Admin.
- SVP for Academic Planning & Faculty Development
- Director of Critical Event Preparedness
- Special Asst. to SVP, Campus Life
- VP of Human Resources
- VP of Campus Services
- Deputy General Counsel
- VP of Research
- VP of IT

- Responsibilities:
  - Compliance (entity-wide and cross-unit)
  - Operational risk
  - Financial risks
- Meets 10-15 times per year

Institutional Committee's Update

- A representative reports on emerging risks and latest institutional priorities
- Updates provide institutional context for unit-level risk management

Cross-Committee Updates Provide Accountability and Context

Unit-Level Committee's Update

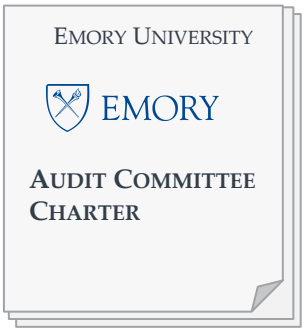
- A representative reports on overall progress of key unit-level risk initiatives
- In a few cases, select risks can be elevated to the Institutional Risk Committee based on impact to the institution

Source: EAB interviews and analysis.

Good Fences Make Good Neighbors

Audit Committee Charter Clarifies Management, Board Responsibilities

The second key element from Emory plays a complementary role to the two-committee structure. Their charter is a mutual agreement between the board (i.e., the Audit Committee) and the Management Committee(s), about where their ownership extends to. It defines responsibilities for management—manage risk, determine when to involve the board, and keep the Audit Committee informed of the top risks. Likewise, the charter clarifies what the Audit Committee's responsibility is—satisfy itself that management has an effective process for identifying and managing risks.



Delineating Management and Board Responsibilities

Management Responsibilities

1. **Management Manages Risk**
   "Management is responsible for monitoring and managing risks."

2. **Management Determines When to Involve Board**
   "Management will exercise its professional judgment in determining when to bring risks to Board attention, which may be as risks evolve…"

3. **Management Informs Audit Committee of Top Risks**
   "Management will provide the Audit Committee with a regular update on the ERM process including a ranked risk listing."

Audit Committee Responsibilities

4. **Audit Committee Oversees Risk Management Process**
   "Audit Committee should review the [risk] listing and satisfy itself that management has an effective approach to identifying and managing risks."

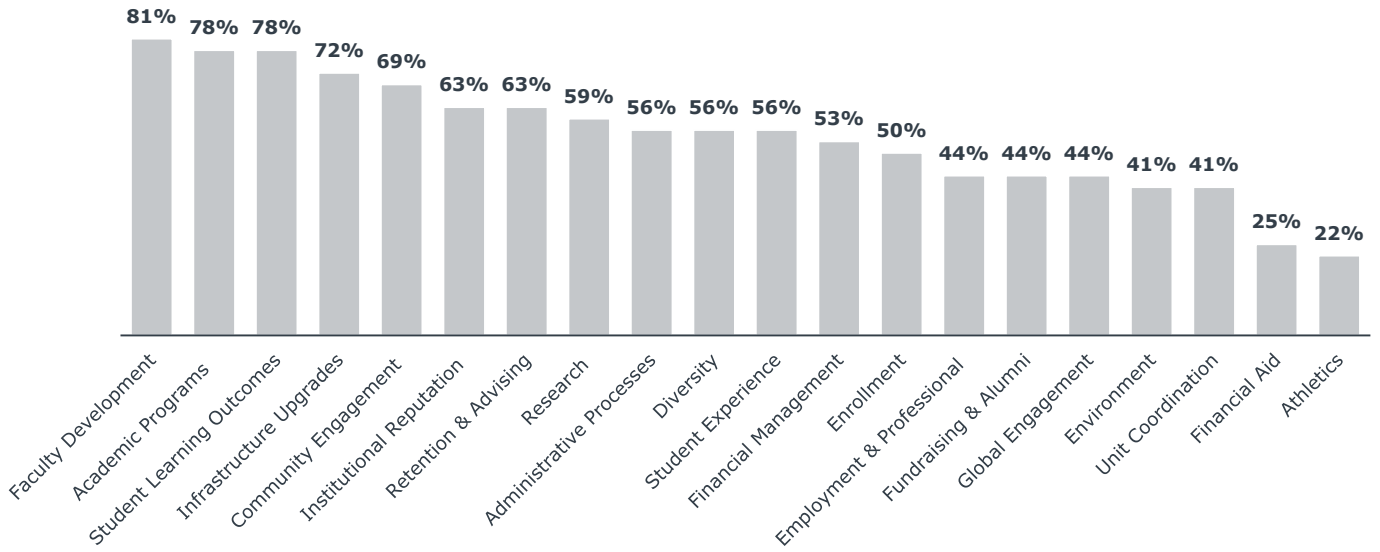
Source: EAB interviews and analysis.

Too Broad, Too Deep

Unbounded Strategic Initiatives, Data-Gathering, Increase Risk Identification

A commonly-identified pitfall of risk efforts is the expansiveness of the effort. The sheer volume of available targets that generate identifiable risks, as represented by initiatives included in strategic plans, sets up the project for an unmanageable volume of work.

Initiatives Included in Sample of University Strategic Plans



Supplementing the top-down identification of risks are the grassroots information-gathering conversations. These frequently occur with the aim of inclusivity and buy-in, and may rely on open-ended queries that attract anything and everything on the interviewee's mind.

Hundreds of Interviews…

- Institution spends 18-24 months interviewing executives, directors, and frontline managers, asking, "what keeps you up at night?"

…Surfacing Hundreds of Risks

- Lack of risk thresholds result in identification of risks of low magnitude (i.e., everything but the kitchen sink is identified as a risk) creating risk register inflation
- Institution surfaces 200-500 risks at institution and unit level

Source: EAB interviews and analysis.

Sorting It Out: 'De-averaging' ERM

Categorizing Risks Allows Proper Triaging for Treatment

The conflation of risks tangles up efforts. Treatment has a greatly increased chance of success if the exercise sorts risks into three "altitudes": systemic and existential, institutional, and unit-level.

A common sentiment is that "ERM is like trying to eat an elephant, and I don't know where to begin." Institutions should work to turn this daunting, monolithic initiative into a more manageable process by de-averaging the initiative into separate processes for systemic and existential, institutional, and unit-level risks. The first benefit of de-averaging the initiative is that it helps avoid "risk paralysis" that takes place on most college campuses by creating a more palatable process. By segregating the risks into different processes, de-averaging provides an opportunity for key university executives (e.g., the president, provost, and chief business officer) to be clear about the risks that they are most interested in discussing and presenting to the board. De-averaging the initiative also sets boundaries for the risk identification process, allowing institutions to spend more time on risk treatment.

Summary of Risk Altitudes and Recommended Management Approaches

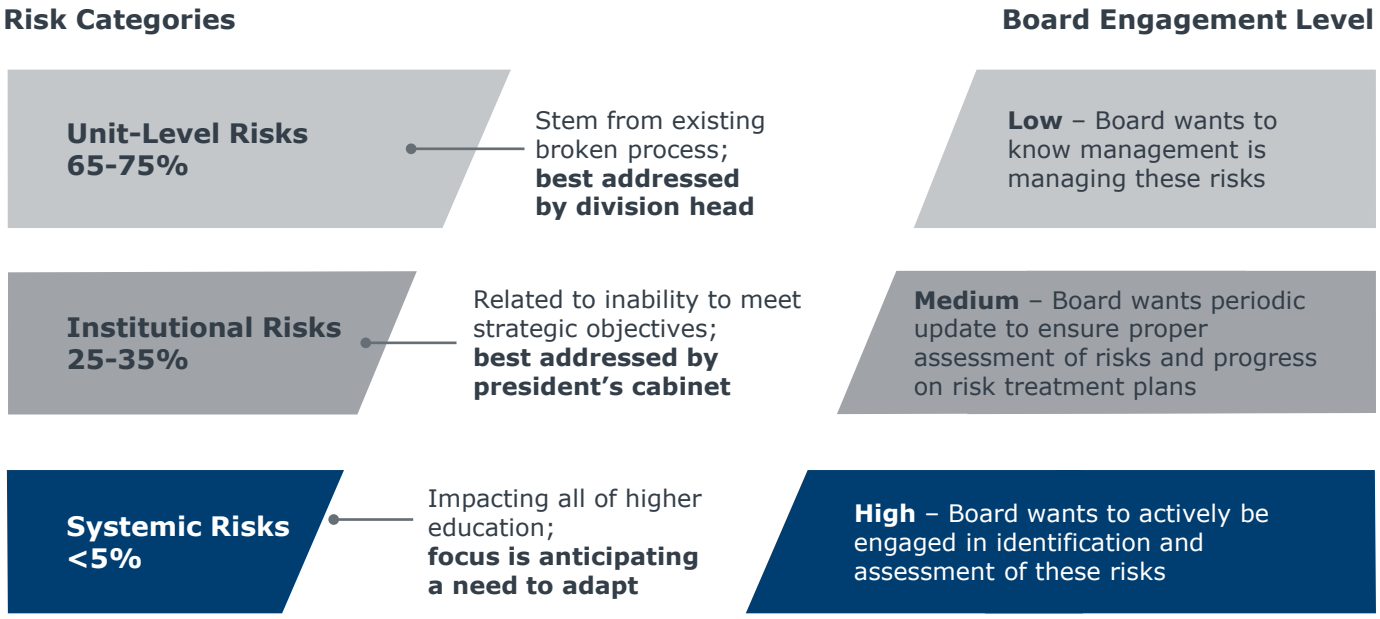
	Systemic and Existential Risks	Institutional Risks	Unit-Level Risks
Risk Type	External, uncontrollable	Strategy execution	Primarily operational, compliance, and financial risk
Measurability	Low: Difficult to measure or estimate likelihood	Medium: Can estimate probability and impact	High: Can measure probability and impact
Risk Assessment Approaches	Risk envisionment scenarios; mental models	Risk maps with nominal scales	Control self assessment; diagnostic controls; operational loss databases
Risk Treatment Objective	Reduce impact should risk occur	Reduce likelihood and impact in a cost-efficient manner	Drive incidence of occurrence to zero
Risk Treatment Approaches	Scenario analysis; contingency planning	Risk reviews at strategy meetings; key risk indicator scorecards	Internal controls; establish policies/procedures; internal audit
Campus Owner	No direct control possible	Best addressed by President's cabinet	Best addressed by divisional head
Sample risks	• Decline of traditional 18-21 student cohort • Sustainability of high-cost/high-discount pricing model • Threat of emerging delivery models • Faculty talent shortage/ misalignment of emerging PhDs • Sustainability of "excessive" student indebtedness • Reduction in family financial capacity and its impact on demand of higher education	• Inability to … • Meet enrollment targets • Meet retention targets • Offer competitive financial-aid packages • Meet liquidity targets against market fluctuations • Fully fund post-retirement obligations • Keep up with growth in data center capacity	• Improper receipt/recording of gifts • Inability to properly manage advising or academic records • Inability to account for property, plant, and equipment due to poor inventory controls • Improper use of motor vehicles by students • Vandalism to university property • Improper use of university logo or insignia

Source: EAB interviews and analysis.

Bringing Oversight to the Altitudes

Different Risks Require Different Board-Level Attention

Another advantage of de-averaging institutional risk management is that it spotlights how different risks require different levels of board engagement. Risk from the (concise) risk register can be mapped to relevant governance bodies or committees, satisfying board concerns of under-engagement in risk management.



Source: EAB interviews and analysis.

Haste to Impact

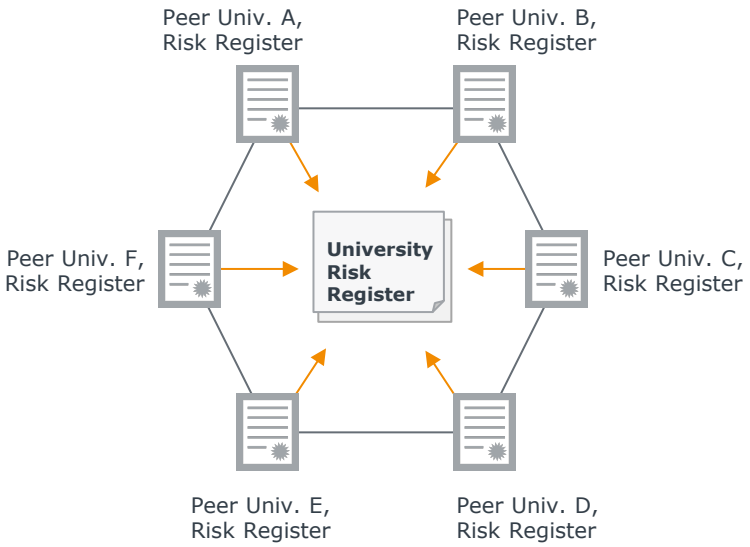
Pre-populated Risk Registers Speed Process, Validate Approach

Progressive institutions fast-cycle their risk identification process by creating a peer-sourced risk register, selecting top risks – in the neighborhood of 30 line items – from a handful of peer institutions.

A peer-sourced risk register can be used as a straw man for conversations with campus representatives, with the objective of quickly moving to conversations about cutting risks that are not applicable and adding risks idiosyncratic to the institution.

This advanced starting point allows institutions to rapidly complete the identification process and move onto the business of risk treatment.

Peer-Sourced Risk Identification



Vetting with Stakeholders

Peer-sourced risk register is used as a straw man for risk committee with an emphasis on identifying:

- Are there risks that aren't applicable to our campus?
- Are there risks that are idiosyncratic to our institution and not reflected on the initial straw man?

To help speed the risk identification process, EAB has developed a peer-sourced register drawing on dozens of risk registers sourced from colleges and universities. The full risk register can be found on page 54 of this publication.

The Risk Register Straw Man and full compendium of risks available are available on page 54 of this publication and on eab.com/baf.

Source: EAB interviews and analysis.

When Everything Seems a Priority

Universities' Traditional Assessment Methods Fail to Highlight Risk Velocity

Having compiled and validated risks relevant to the institution and its setting, risk managers embark on assessing risks in order to prioritize those that merit the most attention. A standard approach to this activity includes considering two factors for each risk: likelihood and impact.

Progressive private sector institutions add a third dimension that factors in risk velocity. Meaning, in the prioritization process, risk administrators estimate those risks that have the highest speed of onset.

Colleges and universities overinvest in mitigating risk items which may naturally decrease over time, or miss risks that will likely trend up in the future.

Average University's Risk Assessment Calculation

This page shows a hypothetical university's consideration of two risks—inadequate staff succession planning, and the inability to meet enrollment targets. Assuming the campus assigns high likelihood scores and medium impact scores to both risks, both receive the same overall risk score.

By limiting assessment to likelihood and impact, however, they ignore the timing of the risks. One may have a faster onset than the other. The outcome of the traditional assessment method is that the institution splits its scarce administrative resources equally between the two risks.

Source: EAB interviews and analysis.

Spotlighting Urgency

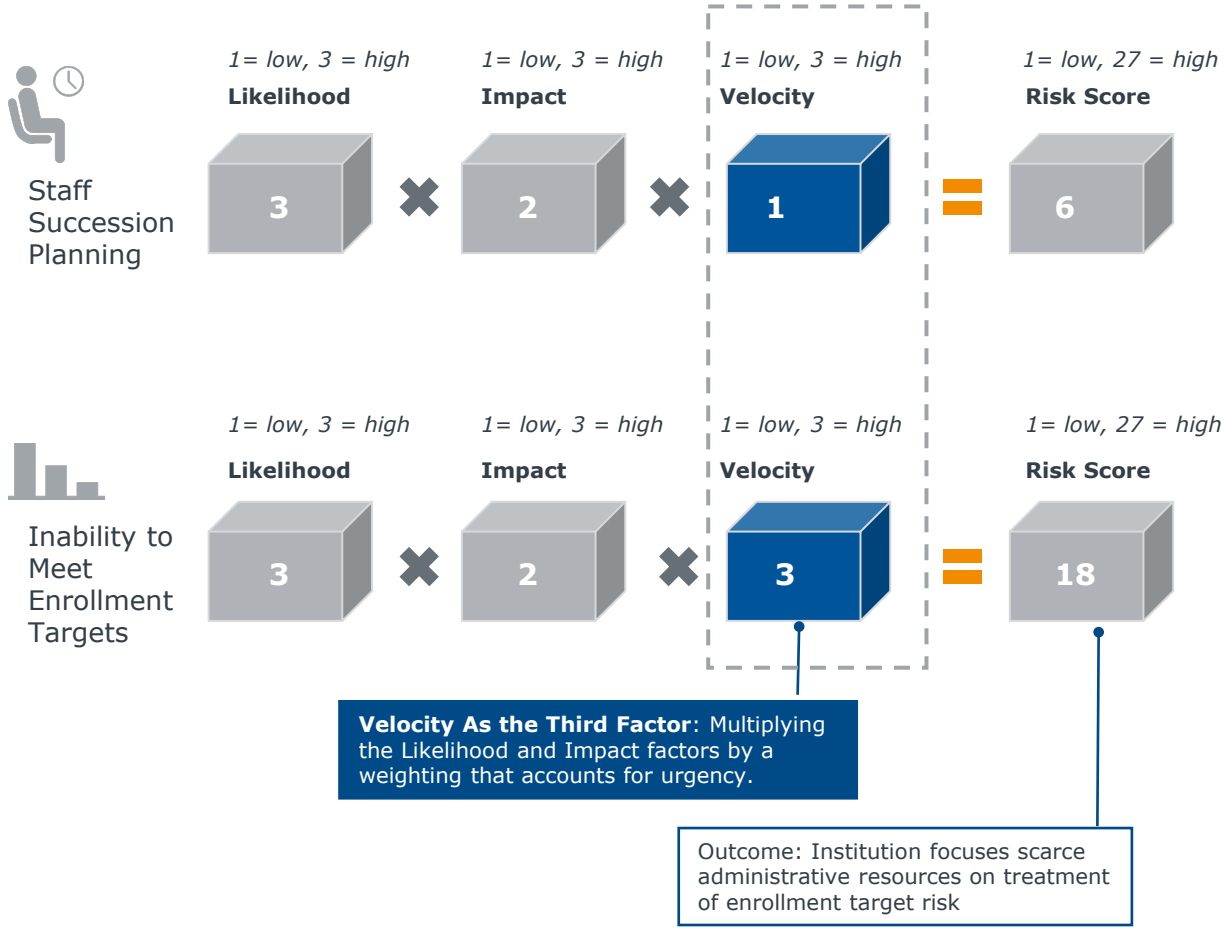
Risk Velocity Helps Identify Risks That Need Immediate Attention

To spotlight the risks that are most urgent and, therefore, to rationalize the deployment of scarce administrative resources toward risk treatment, institutions can consider including "risk velocity" as a risk assessment multiplier.

Risk velocity measures the speech of onset of a risk, typically over a finite period (2-5 years). In short, it answers the question: "How quickly do we expect this risk to manifest itself on our campus?"

By incorporating risk velocity into the assessment process, the most urgent risks receive the most attention—in the illustrated case, the inability to meet enrollment targets.

Progressive University's Risk Assessment Calculation



Source: EAB interviews and analysis.

Building on the Foundation

In addition to this resource, EAB has a full-length study on ERM entitled *A Practical Approach to Institutional Risk Management: Getting Institutional Risk Management Right in an Era of Constrained Resources.* An overview of the structure and tactics of the full publication is below. The foundational essentials detailed on the previous pages drawn from this resource are marked with an arrow on the right.

Section	Tactics
Structuring Ownership and Managing Board Oversight	1. Targeted Risk Governance
	2. Role-Defining Board Charter
Fast-Cycling Risk Identification	3. Peer-Sourced Risk Register
	4. Independent Risk ID Forum
	5. IT and Fixed Asset Interdependency Audit
Assessing and Prioritizing Risk	6. Multidimensional Impact Assessment
	7. Targeted Likelihood and Impact Assessment
	8. Risk Velocity Assessment
Increasing Campus Risk Awareness	9. Academic-Friendly Risk Assessments
	10. Syndicated Risk Assessment & Treatment Workshops
	11. Locally Embedded Risk Resources
	12. Risk Expert Directory
	13. Compliance Matrix Program
Instilling Accountability & Incenting Action	14. Key Risk Hearings
	15. Risk-Based Resource Allocation
	16. Control-Based Cyber Insurance

Source: EAB interviews and analysis.

Foundation-Building Guide: Information Risk

Based on *Elevating Security Awareness: Increasing the Relevance and Scalability of End-User Education*

SECTION 2

- Tactic 1: Board Education Memos
- Tactic 2: Unit-Level Risk Profiles
- Tactic 3: Data-Informed Vulnerability Consultations
- Tactic 4: Security Scorecards

Already Difficult to Secure, Undermined from Within

Self-Inflicted Incidents More Frequent Within Higher Education

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

Openness = Academic Freedom + Shared Governance

Constantly Changing Users

Collaborative Research Around the Globe

New Students, New Devices

Profoundly Decentralized

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 mindset tilts toward academic freedom."

CIO, Regional Masters University

Uniquely Risky

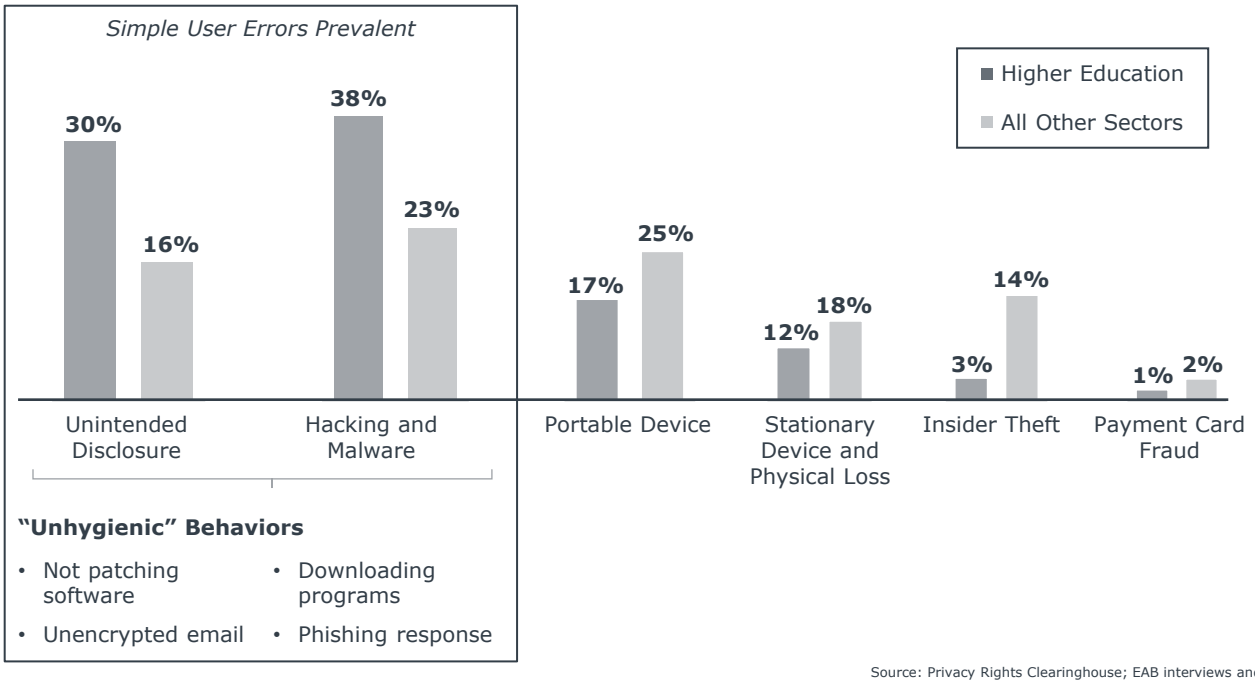
"Higher education is one of the most heavily regulated industries in the U.S.- and it has more risk-producing constituencies than almost any other industry."'

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

(2005-2015)



Source: Privacy Rights Clearinghouse; EAB interviews and analysis.

Biggest Opportunity Is Elevating Awareness

Nudging Users from Neutral to Aware Represents High-ROI Opportunity

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. The focus of the tactics that follow is moving naive and unaware students, staff, and faculty to reliably secure behaviors.

A Taxonomy of End-User Security Behaviors

Malicious Intent ⟵ *Unintentionally Unsecure* ⟶ *Secure and Benevolent*

Intentional Destruction
Break-in of protected file

Unsecure Tinkering
PI sets up wireless gateway

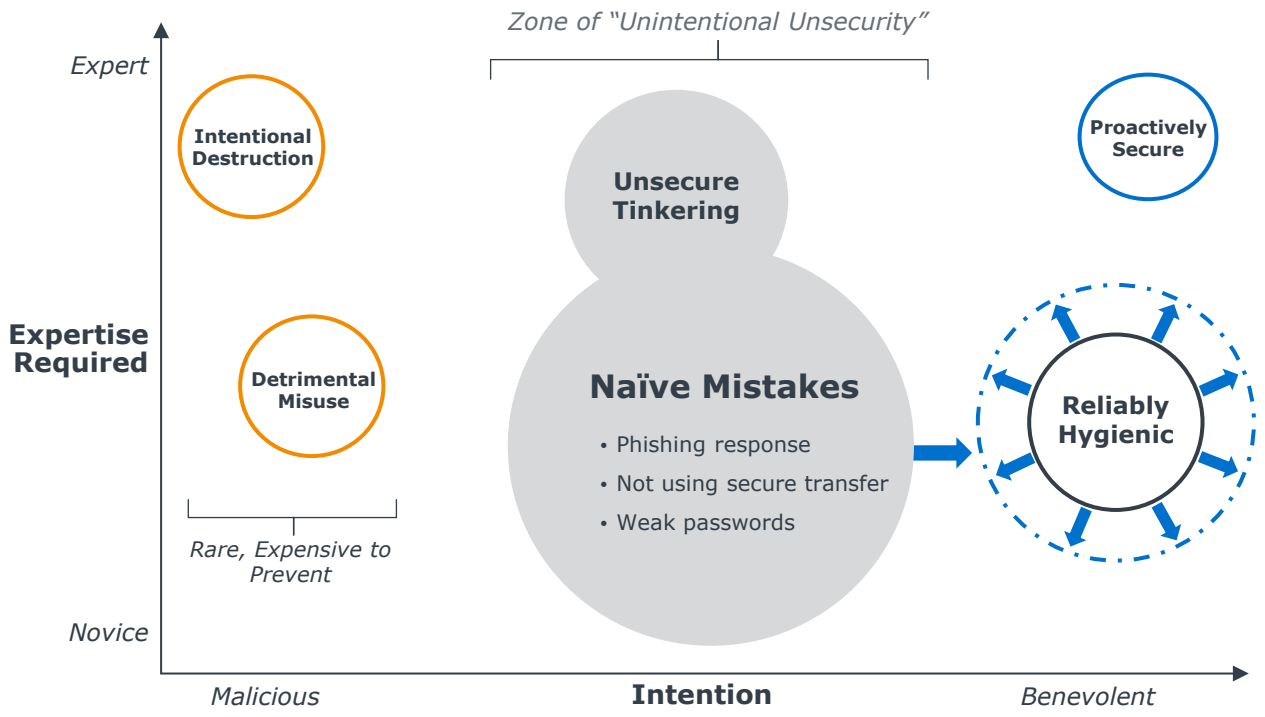
Reliably Hygienic
Changes passwords regularly

Detrimental Misuse
Using email system for spam

Naive Mistakes
Phishing attack

Proactively Secure
Reports backdoor desktop program

The Goal of Elevating Security Awareness



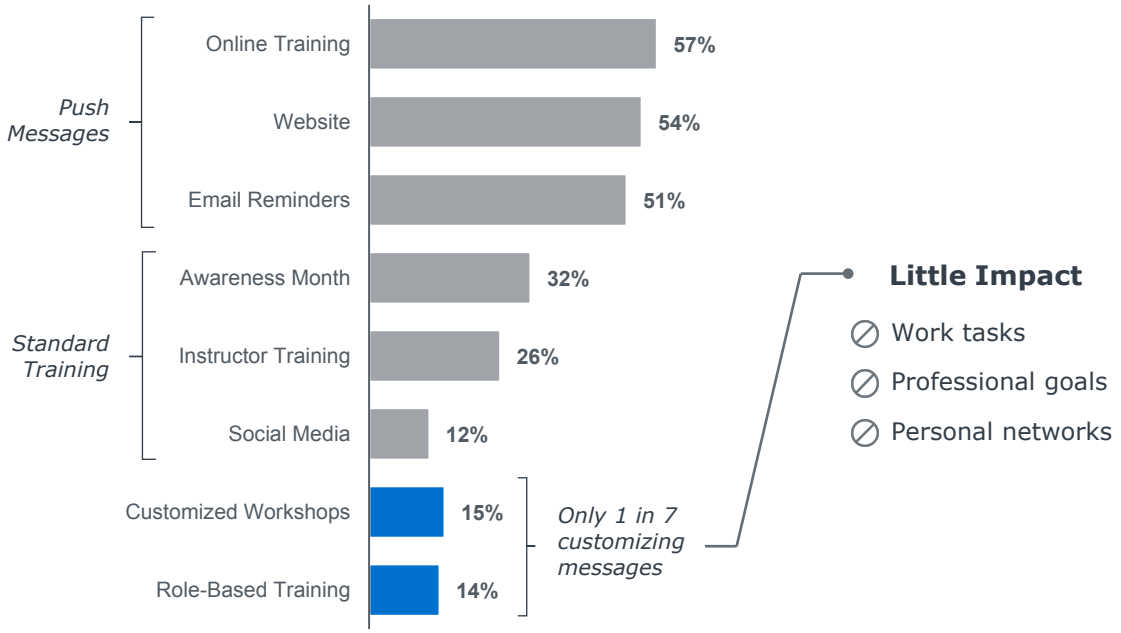
Source: EAB interviews and analysis.

Relying on 'Reach' Because 'Relevance' Is Hard

Typical Security Campaigns Push One-Size-Fits-All Messages

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



Source: Lori McElroy and Eric Weakland, "Measuring the Effectiveness of Security Awareness Programs," EDUCAUSE Center for Analysis and Research, 2013; EAB interviews and analysis.

Information Risk Foundational Essentials

Mandate in Brief

Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) emphasize security awareness among campus members through proactive, relevant, targeted, and sustained communication.

Rationale

The preponderance of data and system security incidents in higher education stem from self-inflicted behaviors, which should be treatable through educational efforts. However, the primary channels are overly-general poster campaigns or blast emails that fail to connect with users' intrinsic motivations and thus do not instill insights or change behavior.

By changing the nature of security-related interactions to providing useful information that targets audiences' interest areas, CISOs can tap into personal motivations, thereby engaging the broader campus in the mission to keep information safe.

Essential Tactics

Tactic 1: Board Education Memos

CISO proactively sends contextualized breach-related information to leaders as events occur. This ongoing education level-sets security awareness among executives and trustees.

Tactic 2: Unit-Level Risk Profiles

Framing security policies as they relate to active projects and priorities brings academic and other departments onto the CISO's side in securing data and systems.

Tactic 3: Data-Informed Vulnerability Consultations

Monitoring data enables CISO to match awareness efforts to prevalence and location of risks.

Tactic 4: Security Scorecards

Self-assessments produce a campus-wide "heat map" of vulnerabilities, and allow department and business unit owners to benchmark their security posture against peer units and over time.

Please see the Breach Response Preparation Toolkit, available on page 63 of this publication.

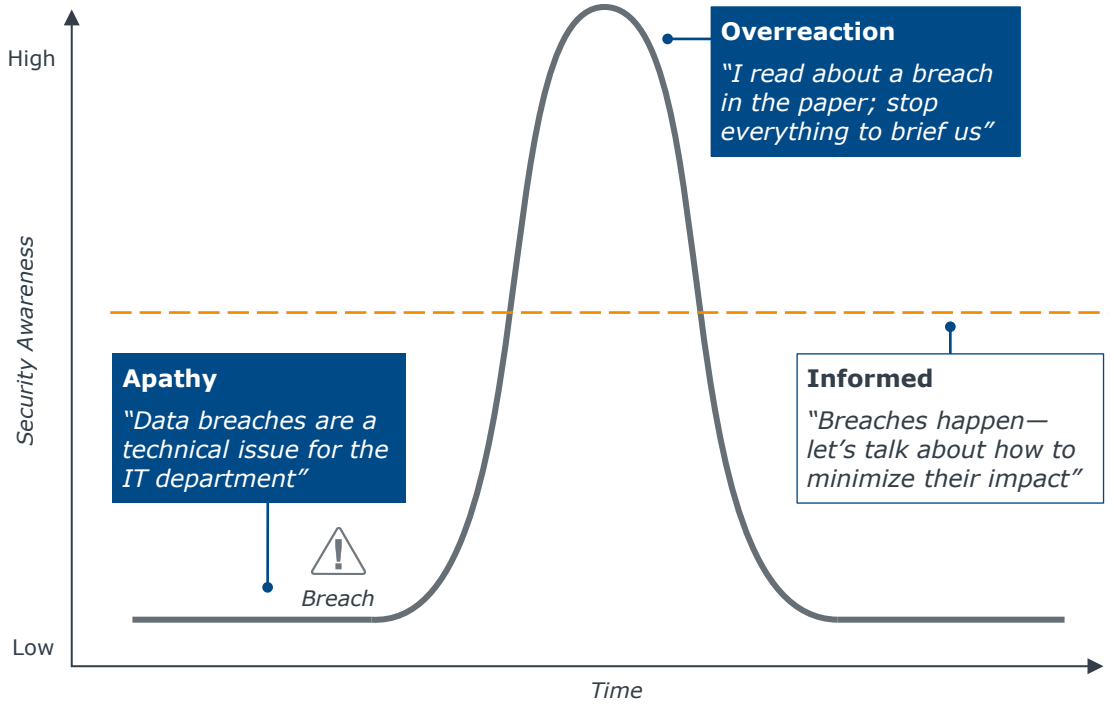
Source: EAB interviews and analysis.

Preventing Whiplash by Anticipating Interest

Responsive Memos Address Otherwise Uneven Board Awareness of Security

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



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.

Ripped from the Headlines: Board Education Memos

CISO Turns Mainstream News into Education Opportunity

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.

"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

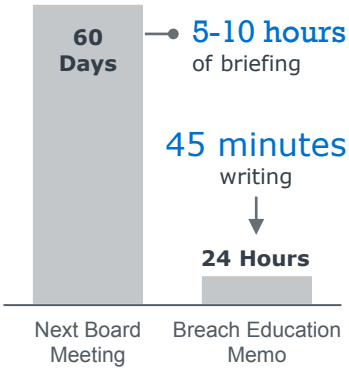
This Could Happen to Us

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.

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



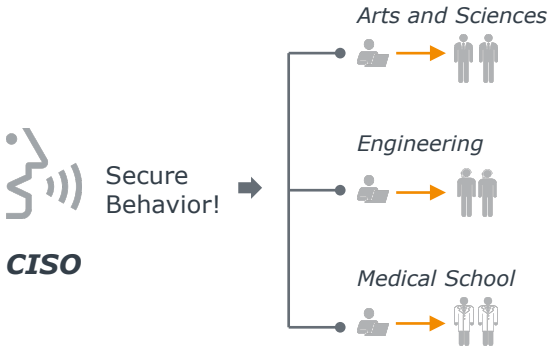
Source: EAB interviews and analysis.

Changing the Security Dialogue from 'Push' to 'Pull'

CISO and Team Spend Time with Unit-Based IT to Itemize Academic Activity

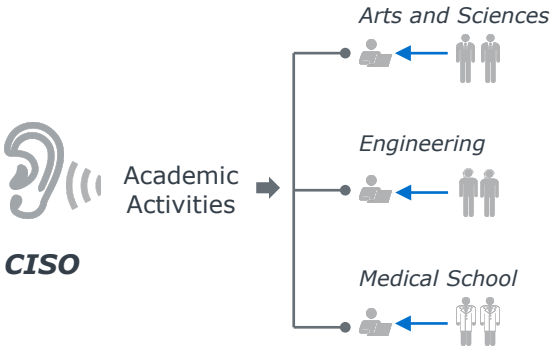
When ordering units to comply with security policies in the abstract, IT typically invokes generic risks and institutional consequences. Before engaging with departments, ask for details about local projects involving data and devices that present risks. CISO meetings with academic departments will be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

CISO Exhorts Unit IT to Get Academic to Comply



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

CISO Asks for Insight into High-Profile Academic Activity



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

Source: EAB interviews and analysis.

Threats to My Life's Work

Security Profiles Make Abstract Risks Relevant to Academic Goals

In particular, end users will better understand the potential risks of data breaches if IT leaders describe potential consequences in the context of academic projects and mission. A conversation tailored to concrete department activity will gain greater attention and long-term compliance than a presentation focused on generic institutional consequences.

Security Profile
Medical School

Project	Risk	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	✔ *HIPAA Compliance* ✔ *Device Tracking* ✖ *Device Encryption*
Cutting-edge textbook on interventional radiology methods	Pirated Scholarship	Hackers steal textbook, post on internet for free	✔ *Regular Changes Passwords* ✖ *Strong Passwords* ✔ *Secure Data Transfer*
Pharmaceutical experiments conducted with international partners	Risky Collaborators	Devices connected to networks in China, Europe routinely compromised	✖ *Remote Mobile Data Wipe* ✔ *Mobile Containerization* ✔ *Email Encryption*

Source: EAB interviews and analysis.

Fine-Tuning Outreach Based on Observed Behavior

Texas State CISO Uses Data from Monitoring Tools to Calibrate Interventions

Non-technical staff may have trouble understanding why cyber risks affect them. Therefore, it is most effective to 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.

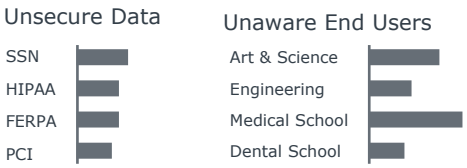
A DLP tool monitors data transfers such as email for information that could be sensitive (e.g., a nine-digit code that could be a Social Security number) and can block outgoing communications. To make the most of a DLP investment, the CISO at Texas State University kept the tool in learn mode for six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

Baselining Nature and Location of Risks Before Activating Controls

TEXAS STATE UNIVERSITY SAN MARCOS

Establishing Baselines for Unsecure Data Transfer

Email Traffic Analysis



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.

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		*Analysis*	*Remediation*

Source: EAB interviews and analysis.

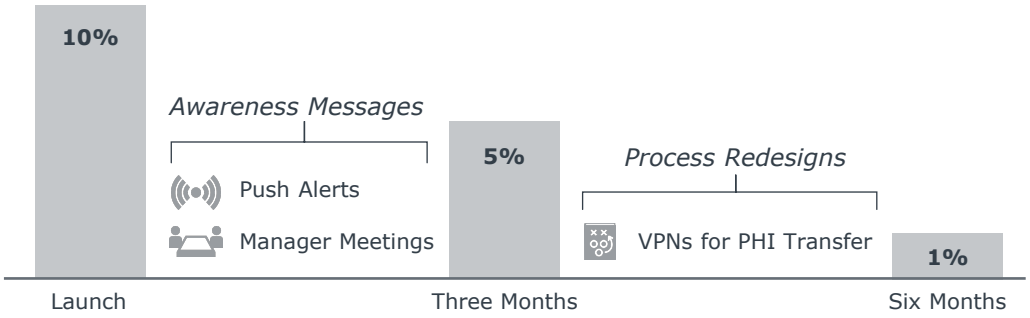
Toward Measurable ROI on Security Initiatives

DLP Monitoring Also Useful in Estimating Impact of Training and Controls

DLP analysis allowed Texas State's CISO to focus valuable in-person conversation time on departments with 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

Ohio State Uses Security 'Heat Map' to Build Unit-Level Risk Awareness

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.

How Are We Doing?

160
"auditable" units

30
risk categories

100
self-ratings

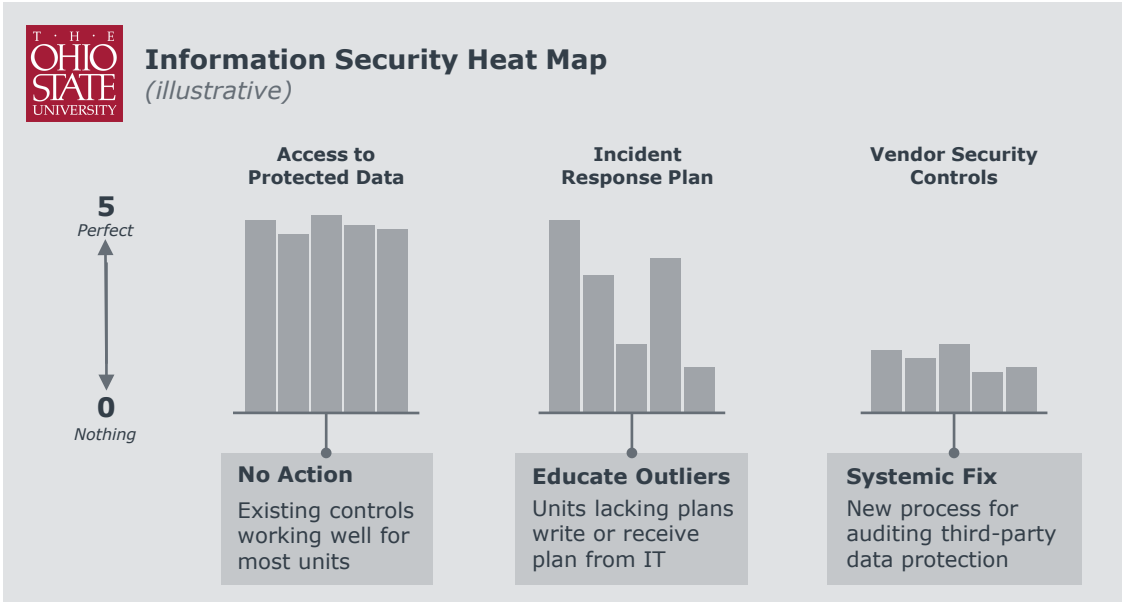
Academic, business, and IT directors must sign off

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

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.

A Bottom-Up Summary of Risks and Recommendations for Board[1]



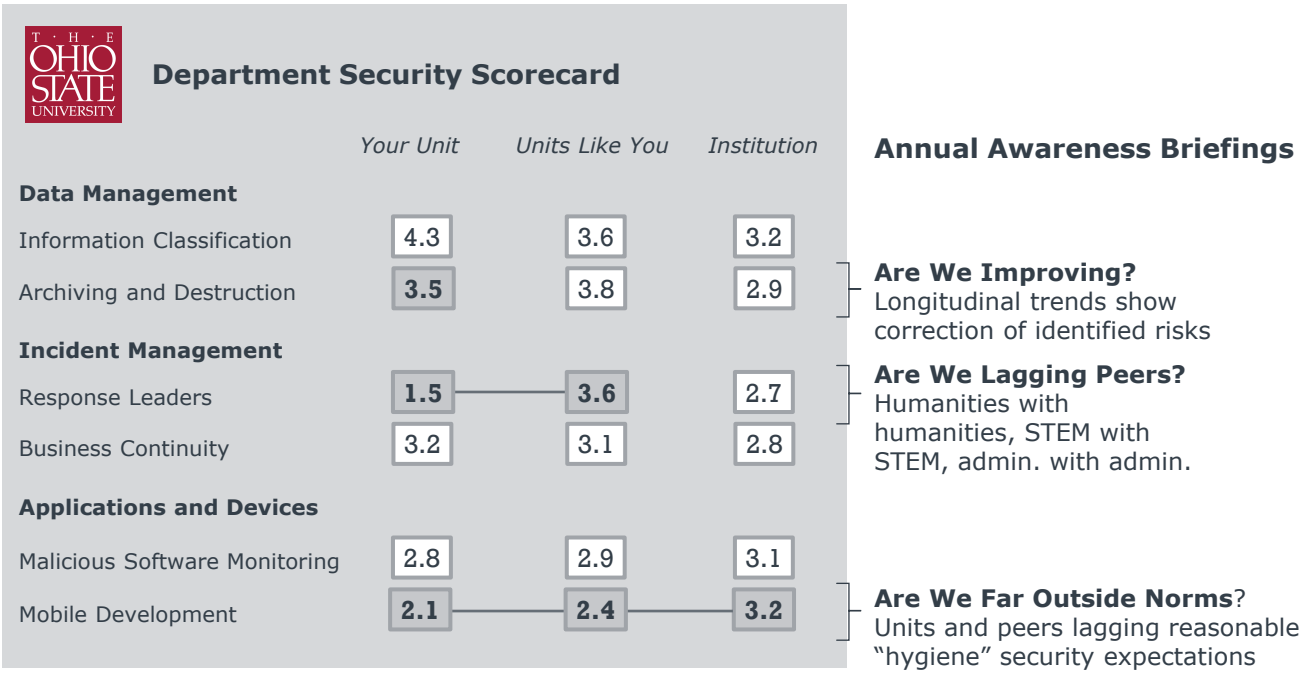
1) Note: Risk categories are illustrative only.

Source: EAB interviews and analysis.

No One Wants to Be Last

Scorecards Show How Units Fare Relative to Local Peers and Overall Norms

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.



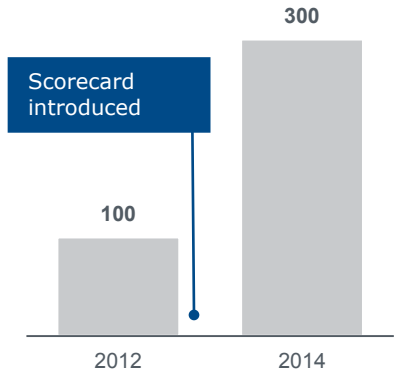
Attention from the board and new visibility into risks for business and academic leaders has already generated positive results for Ohio State. In its second year, the survey gained 100% participation from units, and instead of pushing units to accept cybersecurity policies, there is overwhelming department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

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.

Building on the Foundation

In addition to this resource, EAB has a full-length study on information security entitled *Elevating Information Security Awareness: Increasing the Relevance and Scalability of End-User Education.* An overview of the structure and tactics of the full publication is below. The foundational essentials detailed on the previous pages drawn from this resource are marked with an arrow on the right.

Section	Tactics
Hardwiring Breach Response	1. Incident Managers
	2. Distributed Application Whitelisting
	3. Time-to-Response Tracking
Making Risks Relevant	4. Board Education Memos
	5. Unit-Level Risk Profiles
	6. Personal Risk Audits
Demonstrating Vulnerabilities	7. Vulnerability Consultations
	8. Security Scorecards
	9. Demonstration Hacks
	10. Self-Phishing
Incenting Secure Behavior	11. Breach Chargebacks
	12. Cyber Risk Mitigation Incentives

Source: EAB interviews and analysis.

Foundation-Building Guide: Student Activism

Based on *Navigating the New Wave of Student Activism: Strategies to Engage and Respond to Student Activists*

SECTION 3

- Tactic 1: First-Responder Strategy
- Tactic 2: Targeted Interventions
- Tactic 3: Just-In-Time Guidance

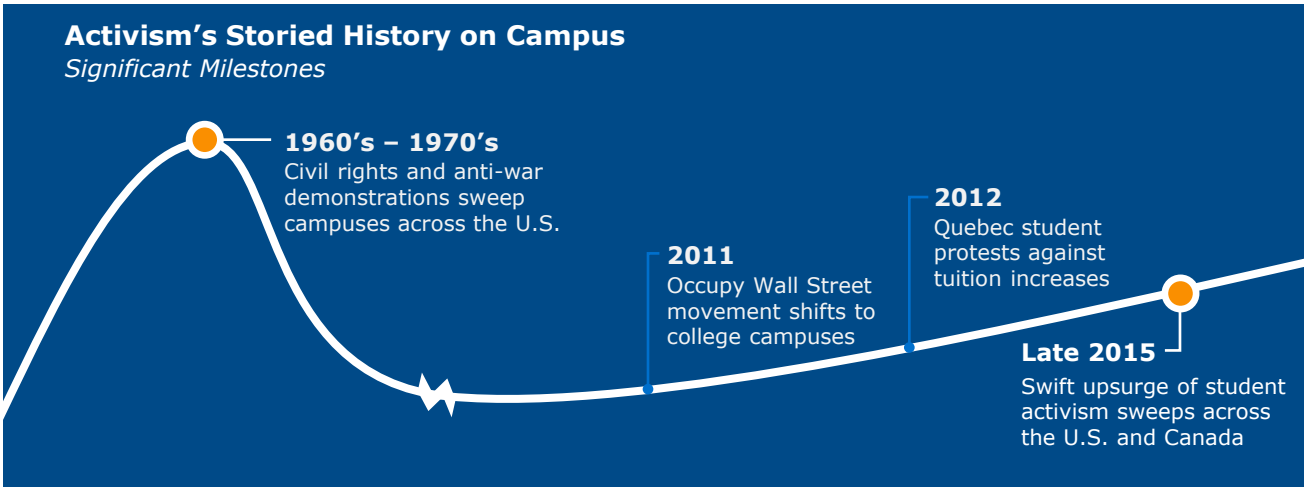
It's the New Reality

From the Iconic 1960s to Today, with a Recent Surge in Volume and Visibility

Student activism has long been part of the narrative of higher education. In the 1960's and 1970's, student activism notably peaked as anti-war and civil rights demonstrations swept across colleges and universities in the U.S.

While activism continued on campuses after that time, it was not until the 2010's that it became once again highly visible. In 2011, the Occupy Wall Street movement spread to college campuses across the U.S. and in 2012 Quebec saw massive protests against tuition increases.

Starting in late 2015, campuses experienced a swift upsurge of student activism in both the U.S. and Canada. This "new wave" of student activism has been widely publicized by those beyond higher education.



Most colleges and universities were caught by surprise. Existing policies and protocols proved insufficient to address today's activism.

Institutions Are Underprepared

Examples of Under Preparation

- ✖ Outdated policies and protocols
- ✖ Lack of proactive engagement and education for students
- ✖ No strategy to respond, leading to slow and reactionary responses
- ✖ No coordinated or trained first responders
- ✖ Senior campus leaders are surprised or frustrated by students' demands

Surprise Among Senior Leaders

Overheard During EAB Research

> *"Generations repeat themselves. I remember thinking, 'Oh wow! Those '60's students won't be back until after I retire.' Oh, how wrong I was!"*

> *"I feel like we are chasing after what's happening right now and scrambling to catch up. It's kind of dizzying after a while…"*

> *"My student affairs colleagues are not prepared. We have not incorporated enough crisis management and strategic thinking skills in our preparation programs for what's happening now."*

Source: EAB interviews and analysis.

Upsides to Action Abound

Interests Aligned Between Mission, Advancement, Enrollment, Job Security

Alongside the reality that today's activism is more complex than ever before, colleges and universities face high stakes to get the response right. There are significant consequences to mismanaging today's activism for both institutions and individual administrators.

Potential consequences include declining donations and support and decreased interest from prospective students. Many senior leaders have seen their jobs put at-risk for mismanaging campus activism and frontline administrators are increasingly asking questions about how their actions might affect their employment.

Fundraising Blowback

$6M

Total drop in new pledges and donations to the University of Missouri in December 2015

Enrollment Impacts

10%

Drop in applications if *The New York Times* covers an institutional scandal in a long-form magazine article

Possible Legal Action

807

Number of student inquiries about free speech violations and restrictions received by FIRE[1] in 2015, up from 719 in 2014

Yet, "today's activists are tomorrow's trustees." This quote illustrates the positive potential of proactively engaging student activists, who are clearly dedicated to improving their institution. Outline below are four reasons why progressive institutions and leaders are capitalizing on the opportunity to engage student activists in a positive manner.

It's our history.

"The great movements of our nation were driven by students. We need to help students understand that this is what our country is founded on and what's important about a public institution guaranteeing free speech."

Vice President for Student Affairs
Public Master's University

It's our mission.

"Our mission is to develop engaged citizens and effective advocates. When they leave, we want our students to advocate for social change and be passionate spokespersons for the issues they believe in."

Dean of Students
Private Baccalaureate College

It's in our students' interests.

"Creating the next wave of activism is part of our job as an institution. There are learning moments and educational opportunities that we can leverage in the midst of all of this passion and activism to make our students stronger graduates."

Dean of Students
Public Research University

It's in society's interests.

"Activism is the hope and promise of post-secondary. If we manage it well, we are going to send out people who are going to make the world better."

Vice President for Student Affairs
Canadian Public University

Source: Foundation for Individual Rights in Education; EAB interviews and analysis.

Student Activism Foundational Essentials

Mandate in Brief

Campus leaders embrace activism as a vital ingredient of students' engagement with the institution by building communication bridges and anticipating incidents. Seeking to professionalize their campuses' approach to activism, Student Affairs offices prepare response plans, engage with potential activists, and ultimately leverage the energy and enthusiasm of activists to work together and drive change on campus.

Rationale

Institutional leaders want students to be active citizens when they leave campus as alumni, yet they face a conflict in reconciling the traditional identity of higher education with modern activism. Institutions must find a delicate balance in the face of increasing questions from the public about ensuring free speech and increasing pressure from students to curb hateful or hurtful speech in an effort to create a welcoming campus climate.

Essential Tactics

Tactic 1: First Responder Strategy

Engaging with activists via dedicated channels and roles ensures consistent experiences during incidents. Campuses may combine "civilian" approaches with law enforcement

Tactic 2: Targeted Interventions

Risk leaders identify and proactively engage with potential and "simmering" activists.

Tactic 3: Just-in-Time Guidance

A 24/7-accessible portal houses relevant information about policies, facilities, and campus philosophy on activism, providing authoritative references for activists and responders alike.

Source: EAB interviews and analysis.

Don't Underestimate the Power of the First Response

Situationally Dependent Status Quo Doesn't Address Immediate Needs

An institution's first response to campus activism is critical, but often underestimated. It sets the tone for the remainder of the institution's interactions with student activists, ensures student safety, minimizes disruption, and will likely be widely magnified and dissected.

However at most institutions the status quo is situationally dependent on who's available to drop everything and respond. The response can be slow as institutions scramble to find someone prepared and available, and the tone and quality of the response varies depending on the expertise of available staff.

Student affairs is well suited to lead the institution's first response to student activists because the success of the response is dependent on understanding people. However, responses must be formalized to ensure a rapid, thoughtful, and consistent approach to activism on campus.

The First Response Is Critical…

- Sets the tone for the remainder of the institution's response
- Ensures student safety and minimizes institutional disruption
- Will be magnified and dissected by students, the public, and the media

…But Status Quo Often Falls Short

- Response can be slow as institutions scramble to determine who is available and prepared to respond
- Tone and quality of the response fluctuates depending on the expertise of available staff
- Unclear goals can lead to first responders not having a purpose or direction when arriving on the scene

The First Response Is All About Understanding People

"To improve the first response, you have to understand that it's a problem about people. When we show up to a protest, students are anxious about how we will react and what we will say. For some, it might even be the first time they are interacting with us. In today's climate, everyone is nervous about what might happen next.

It's our job to let students know that we respect their experiences and concerns, we are listening to their opinions, and we are there to keep them safe."

Dean of Students
Public Research University

Source: EAB interviews and analysis.

First Responders: Civilian and Uniformed

Campus, Local Law Enforcement Play a Critical Role in Response Preparation

Campus and local law enforcement should play a critical role in response preparation. Institutions can involve law enforcement early in conversations about how and when to respond to student activists. Student affairs divisions can engage law enforcement in response preparation in areas such as determining a campus threshold for activism, solidifying a response protocol, and creating a chain of command. Student affairs and law enforcement should also collaborate to provide contextual training and deepen relationships.

Three Approaches for Student Affairs Divisions

1

"We need staff to monitor and record what's happening during a demonstration on campus."

First Amendment Monitors

University of Arizona

2

"We need a team of students who are trusted by their peers and administrators alike."

Social Justice Peer Educators

Southern Illinois University

3

"We need a dedicated team of trained administrators who can quickly respond."

Protest Safety Team

University of Florida

Defining Police's Role: Incorporate Officers into Student-Centered Response

No matter your institution's approach, **campus and local law enforcement** play a critical role in response prep.

Involving Law Enforcement in Early Conversations

"Campus administrators are seeing a benefit to involving them in conversations from the beginning. It's no longer about calling the cops when you need them, but a more proactive and preventive approach."

Kim Richmond, Director
National Center for Campus Public Safety

Student Affairs Can Engage Police in Response Prep

Determine Threshold

Assess the level of activism the campus can safely handle

Solidify Response Protocol

Create an incremental response, determine appropriate use of force

Create a Chain of Command

Determine who has decision-making authority during an event

Provide Contextual Training

Prepare staff with first amendment training and de-escalation skills

Deepen Relationships

Encourage staff engagement with all levels of police, not only with the chief

Source: EAB interviews and analysis.

Ensuring First Responders Are Prepared

The University of Florida employs a comprehensive training model to prepare first responders. Training consists of a core curriculum and event-specific preparation and debrief.

First, volunteers are required to attend a half-day session at the beginning of the fall semester. This session covers topics like university policies, general response protocols, and de-escalation tactics.

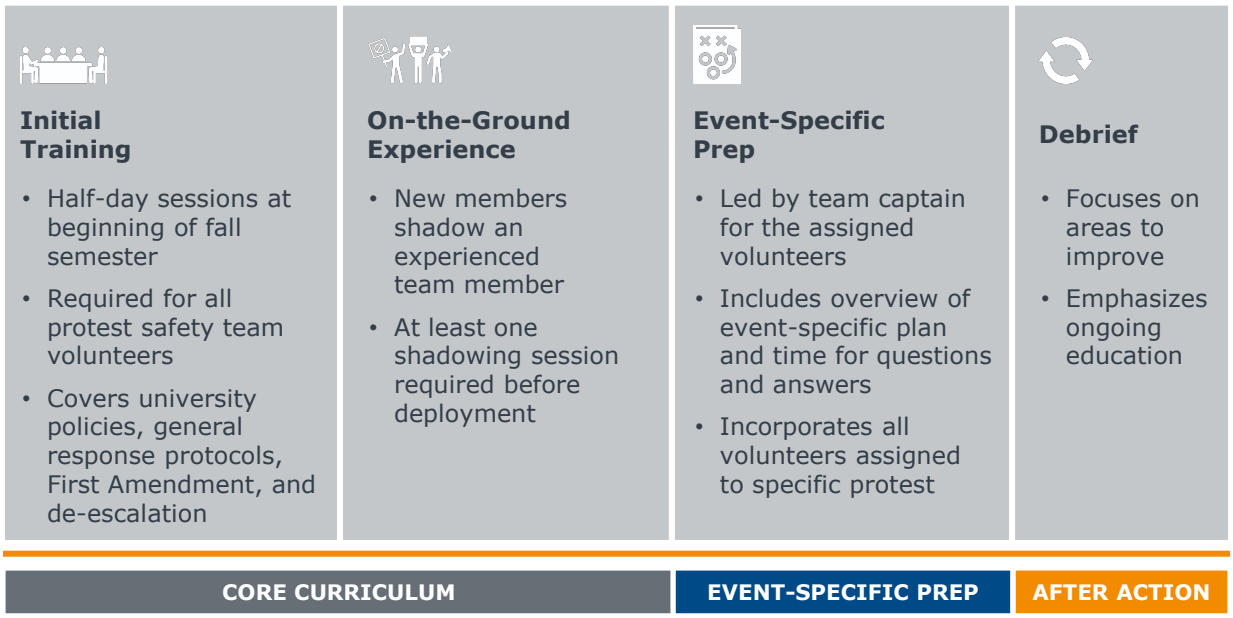
The second component of the core curriculum is on-the-ground experience. Volunteers must shadow an experienced team member at least one time before they are deployed as a fully operational team member.

Before each event, the team captain gathers the first responders who will be deployed and reviews an event-specific plan. This time also provides team members the opportunity to ask questions about the protest.

Immediately following an event, there is a debrief that focuses on immediate areas for improvement and emphasizes ongoing education for Florida's first responders.

Together, this robust training ensures that responders are best prepared to respond to events on campus.

University of Florida's Comprehensive Training Model



Source: EAB interviews and analysis.

Targeted Interventions Meet Students Where They Are

University of Michigan Identifies Activists to Offer Proactive Guidance

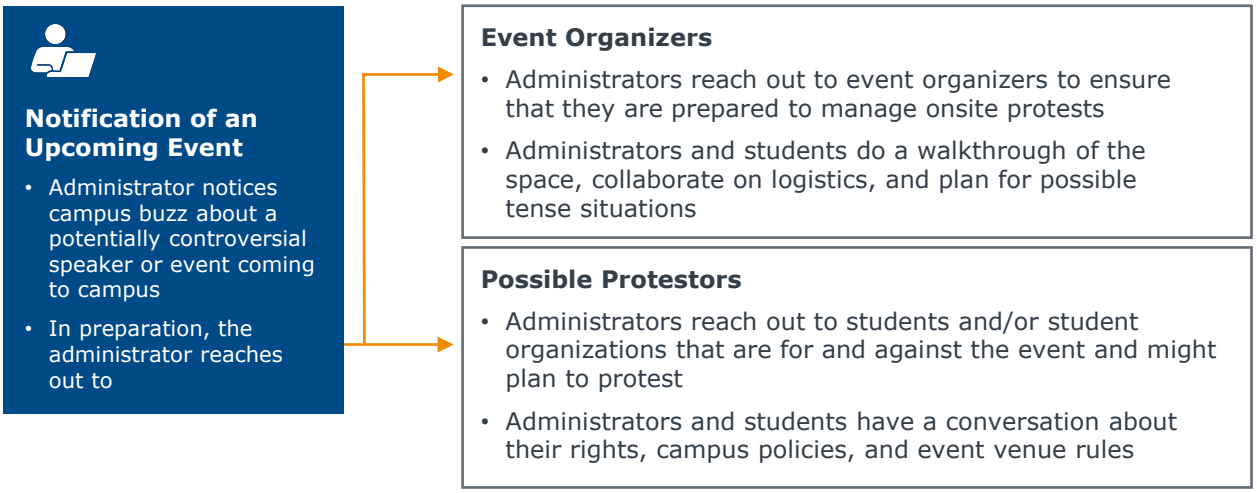
Beyond general activist education for students who are "casually browsing," institutions should address "simmering" activists (those engaged in causes or developing a plan) with targeted interventions. The University of Michigan identifies potential activists and reaches out to offer guidance about upcoming activist activity on campus.

When an administrator at Michigan is notified or made aware of an upcoming event, such as a controversial speaker, they proactively reach out to the event organizers and possible protestors. With event organizers, administrators help students prepare for onsite protests by doing things like a walkthrough of the space and talking through possibly tense situations. With possible protestors, administrators will reach out to have a conversation about their rights, campus policies, and event venue rules.

This approach is mutually beneficial to students and the institution because it provides administrators with more insight about upcoming events, strengthens relationships between students and administrators, increases students' preparation and awareness of resources, and reduces the potential for a tense or regretful exchange.

How Michigan Prepares for and Interacts with Potential Activists

Illustrative Example



Benefits to Students and the Institution

- Provides administrators with more insight about upcoming events
- Increases involved students' preparation and awareness of campus policies and resources
- Reduces the potential for a tense or regretful exchange
- Strengthens relationships between students and administrators

Source: EAB interviews and analysis.

Simple, Accessible, Just-in-Time Guidance for Activists

Michigan State University's (MSU) Brochure Offers Immediate Information

While it is ideal to reach students earlier, once activists move from "simmering" about an issue or plan to "activating" about a cause, it is important to provide just-in-time guidance and support.

Michigan State University's student life division developed a brochure in consultation with student leaders that offers immediate information to activists. The brochure includes MSU's philosophy on activism, relevant policies and ordinances, quick facts and recommendations, action steps for successful activism, and key contact details, including campus life and police.

The brochure is available online and continuously distributed to activists as they come forward on campus.

Brochure Logistics

- Developed by Student Life division in consultation with student leaders
- Shared online and distributed to activists as they come forward

Key Content

- MSU's philosophy on activism
- Relevant policies and ordinances
- Quick facts and recommendations
- Action steps for successful activism
- Key contact details, including campus life and police

"Student Activism at Michigan State"

What Should I Know About Activism On Campus?

Protests, rallies, etc., may not disrupt normal University operations.

For example, activities may not:

- Create excessive noise within or in close proximity to campus buildings.
- Obstruct the free movement of persons about the campus.
- Block access to and from University buildings.
- Enter or remain in another individual's place of residence or work without permission.

While in dialogue, we should:

- Listen to the ideas and beliefs of others.
- Reflect critically on our own ideas and beliefs.
- Accept responsibility for our actions and words.
- Contribute positively to the richness of the intellectual dialogue.

Source: "Student Activism at Michigan State," Michigan State University, 2016, http://studentlife.msu.edu/wp-content/uploads/2012/04/Student-Activism-2016.pdf; EAB interviews and analysis.

Building on the Foundation

In addition to this resource, EAB has a full-length study on student activism entitled *Navigating the New Wave of Student Activism: Strategies to Engage and Respond to Student Activists.* An overview of the structure and tactics of the full publication is below. The foundational essentials detailed on the previous pages drawn from this resource are marked with an arrow on the right.

Section	Tactics
Educating Potential Student Activists	1. Social Media Monitoring Framework
	2. Information Sharing Network
	3. General Education
	4. Targeted Interventions
	5. Just-In-Time Guidance
	6. Follow-Up Support
Facilitating Community Dialogue on Tough Issues	7. Proactive Roundtable Discussions
	8. Notecard Exercise
	9. Neighborhood Policing Initiative
	10. Activism FAQ
	11. Staff and Faculty Training and Support
	12. Briefing for Senior Leaders
	13. Alumni Comment Tracker
	14. Alumni Dialogue Series
Leveraging Activism for Long-Term Change	15. Demand Triage Strategy
	16. Community Letters
	17. Online Tracker
	18. Dedicated Commission
	19. Demand Scorecard
Constructing an Agile Response Blueprint	20. Neutral Observers Program
	21. Social Justice Peer Educators
	22. Dedicated First Responder Team

Source: EAB interviews and analysis.

Implementation Resources

APPENDIX

- Risk Register Straw Man
- IT Security Breach Response Diagnostic and Toolkit

Risk Register Straw Man

Overview and Methodology

In response to a common question received by the Business Affairs Forum—"How can we fast-cycle the risk identification process?"—we have compiled a risk register for higher education institutions to use as a starting point in their discussions. The composite risk register was developed by obtaining risk registers from 17 higher education institutions, totaling approximately 3,000 risks.

Clarifying Terms

The risks included below are separated into two categories: (1) institutional risks and (2) unit-level risks. A key finding in the Roundtable's research is that most universities commingle risks of different "altitudes" in their ERM process. For example, the risk of a declining 18- to 21-year-old traditional student cohort is included in the same process as inability to meet enrollment targets, which is included in the same process as inadequate controls of cash receipts. As such, the Roundtable proposes that higher education institutions should separate the risks into different processes. Below is an overview of the three types of risk "altitudes" identified by the Business Affairs Forum and how the management approach for each risk altitude differs.

	Systemic and Existential Risks	Institutional Risks	Unit-Level Risks
Example	• Sustainability of high price/high-discount pricing model	• Inability to meet enrollment targets	• Inadequate controls over cash receipts
Risk Type	• External, uncontrollable; impacts all of higher education	• Controllable and idiosyncratic risk • Generally relates to inability to meet strategic objectives	• Controllable and idiosyncratic risks • Generally relates to an existing and broken process
Measurability	• Low—Difficult to measure of estimate likelihood	• Medium—Can estimate probability and impact	• High—Can measure probability and impact
Risk Assessment Approach	• Risk environment scenarios • Mental models	• Risk maps with nominal scales	• Control self -assessments
Risk Treatment Objective	• Reduce impact should risk occur	• Reduce likelihood in a cost-efficient manner	• Drive incidence of occurrence to zero
Risk Treatment Methods	• Scenario analysis • Contingency planning	• Risk reviews at strategy meetings; key risk indicator scorecard	• Internal controls • Establish policies and procedures • Internal audit
Board Involvement	• High –Board wants to be actively engaged in discussion	• Medium—Board prefers periodic updates by senior management	• Low—Board wants to know senior management has a risk management process in place

Source: EAB interviews and analysis.

Risk Register Straw Man

Suggested Use of the Risk Register Straw Man

Cognizant of the different risk altitudes, the Business Affairs Forum's risk register separates institutional and unit-level risks. The list of institutional risks is meant to be as comprehensive as possible. As there may be thousands of unit-level risks, the list of unit-level risks in this straw man is not meant to be comprehensive, and instead suggests example risks. Additionally, as mentioned frequently through this study, the Roundtable does not recommend undertaking a risk identification exercise that results in a register with hundreds of risks.

Systemic and existential risks are not included in this analysis because they vary so much by time and institution. Also, at the request of members, this risk register along with our overall best-practice study does not include so-called "black swan" events such as terrorist attacks, natural disasters, pandemics, and hostile intruders/active shooters. For such risks, we recommend institutions hold periodic long-tail risk summits for a deep-dive into these risks.

The Business Affairs Forum suggests that members utilize the risk register straw man as follows:

- The list of institutional risks should be vetted with the president's cabinet to identify which risks on the straw man are not applicable to the organization and which idiosyncratic campus risks should be added.
- The remaining risks should be assessed based on likelihood, impact, and risk velocity to come up with an overall risk score. (See the associated best practices on assessing risk in the full study *A Practical Approach to Institutional Risk Management*.)
- After each risk has been scored, pare down the final list to 25 to 50 risks.
- After the list of institutional risks has been finalized, it will be time to begin identifying unit-level risks. Instead of taking a bottom-up approach to identifying every possible unit-level risk (which may result in hundreds of risks), we recommend using the final list of institutional risks and identifying only the unit-level risks that pertain to the institutional risk. Said differently, it's best to cascade institutional risks down to unit-level risks.

Source: EAB interviews and analysis.

Risk Register Straw Man

Academic Quality
Suggested Risk Owner(s): Provost

Institutional Risks	Example Unit-Level Risks
• Inability to offer courses that meet students' demands • Inability to ensure online education programs meet institutional academic standards • Inability to recruit or retain sufficient faculty to meet desired student-to-faculty ratios • Failure to maintain sufficient academic quality standards required for accreditation • Inability to maintain desired levels of teaching quality • Inability to adequately fund or reallocate resources to core of high-priority academic programs	• Improperly managed academic records • Insufficient faculty support for changes in pedagogy and curriculum • Lack of adequate library services and resources to support institutional needs • Ineffective interdepartmental collaborations

Admissions and Enrollment
Suggested Risk Owner(s): VP of Admissions and/or Director of Financial Aid

Institutional Risks	Example Unit-Level Risks
• Inability to offer competitive financial aid packages • Inability to offer competitive tuition rates • Inability to maintain existing levels of student access • Inability to enroll a diverse student body • Inability to meet application targets • Inability to meet enrollment/yield targets • Inability to maintain affordability due to increasing student fees	• Fraud in admission applications and materials • Conflicting social media policies related to student recruitment • Failure to monitor changing financial aid regulatory requirements • Insufficient personnel/resources to maintain desired level of regional/national recruiting activities

Source: EAB interviews and analysis.

Risk Register Straw Man

Administrative Service Delivery
Suggested Risk Owner(s): Chief Business Officer

Institutional Risks	Example Unit-Level Risks
• Inability to meet desired levels of administrative service quality	• Staff not properly trained in new ERP system • Failure to produce timely and accurate reports for campus administrators • Cumbersome hiring procedures • P-card system too time-consuming for faculty

Athletics
Suggested Risk Owner(s): Director of Athletics

Institutional Risks	Example Unit-Level Risks
• Failure to comply with NCAA regulations including athletic recruiting guidelines • Failure to comply with Title IX regulations • Inability to adequately protect student athlete health and safety	• Lapses in safety and insurance coverage for sports campus • Inadequate fitness machine maintenance • Insufficient first aid/emergency supplies for athletic team practices

Contracts
Suggested Risk Owner(s): General Counsel

Institutional Risks	Example Unit-Level Risks
• Inability to anticipate and prevent legal issues associated with third-party collaborations • Inability to anticipate and prevent undue institutional liability or risk exposure from third-party contracts	• Inadequate signature authority policy and procedures

Source: EAB interviews and analysis.

Risk Register Straw Man

Fundraising/Endowment Management

Suggested Risk Owner(s): Chief Business Officer or Chief Development Officer

Institutional Risks	Example Unit-Level Risks
• Insufficient oversight of internal or external investment managers • Inability to absorb significant loss in endowment or investment value • Over-/under-engagement with key donors	• Improper receipt/recording of donor gifts • Inadequate controls to prevent conflict of interest in investment decisions • Significantly overoptimistic projections of endowment growth

Facilities and Fixed Assets

Suggested Risk Owner(s): Vice President of Facilities

Institutional Risks	Example Unit-Level Risks
• Inability to ensure staff and student safety due to deteriorating buildings • Inability to stem energy cost increases (either due to demand or supply factors) • Inability to meet presidential sustainability targets • Inability to provide sufficient space to meet teaching, research, and administrative needs • Inability to expand campus facilities footprint due to municipal constraints	• Inadequate building security procedures (card access, key control) • Inability to prevent safety lapses in campus construction projects • Failure to implement and test resiliency and contingency plans for essential infrastructure (heat, hot water, electrical, water/sewer, HVAC) • Unsafe surface conditions during inclement weather • Poor response time to utility service failure • Vandalism and damage to university property • Inadequate inventory control of property, plant, and equipment • Poor response time to equipment/facility malfunction • Failure to comply with ADA requirements • Workplace safety protocols inadequate or not followed • Failure to maintain physical plant safety and comply with OSHA regulations • Failure to maintain adequate levels of fire safety and preparedness

Source: EAB interviews and analysis.

Risk Register Straw Man

Financial and Economic

Suggested Risk Owner(s): Chief Business Officer

Institutional Risks	Example Unit-Level Risks
• Inability to detect or prevent conflicts of interest in financial transactions, agreements, or gifts to senior administrators • Occupational fraud; deliberate misuse or misapplication of university's resources or assets • Inability to fund new strategic initiatives due to legacy budgeting model • Inability to cope with unexpected revenue shortfall/budget reductions • Failure of online degree programs to meet financial targets • Inability to manage/absorb rising health care costs • Inability to adequately fund all desired programs due to fund diffusion across multiple objectives • Declining institutional financial flexibility due to reduction in financial reserves • Inability to meet liquidity targets against market fluctuations • Failure to control growth in debt burden • Inability to meet debt covenant requirements • Inability to ensure accuracy or completeness of external financial reporting • Inability to fund progress on deferred maintenance queue • Inability to manage or react to fluctuations in currency exchange rates	• Insufficient oversight over third-party vendors • Inadequate controls over decentralized cash receipts • Ineffective management of self-insurance program and costs • Failure of institution's pension plan to comply with ERISA • Failure to comply with state's debt management regulations • Inability to ensure program-level financial sustainability • Failure to comply with IRS rules and tax reporting requirements

Source: EAB interviews and analysis.

Risk Register Straw Man

Human Resources

Suggested Risk Owner(s): Vice President of HR and/or General Counsel

Institutional Risks	Example Unit-Level Risks
• Failure to prevent significant lawsuits and claims relating to professional liability, discrimination, or equal opportunity noncompliance • Inability to recruit and retain top faculty, staff, and senior administrators • Inability to meet targets in staff and faculty diversity • Inability to offer a competitive benefits package • Inability to retain faculty and staff due to • employee dissatisfaction • Failure to secure favorable collective bargaining outcomes	• Failure to prevent inappropriate alcohol or drug use by employees • Incidences of sexual harassment or misconduct by faculty or staff • Inadequate procedures or controls for new faculty and staff background checks • Failure to comply with overtime and minimum wage regulations (FLSA) • Failure to implement rigorous background checks for new faculty and staff • Failure to establish adequate mediation/resolution channels for employee conflicts • Failure to prevent workplace violence or harassment • Arduous promotion and/or tenure policies

Information Technology

Suggested Risk Owner(s): Vice President of HR and/or General Counsel

Institutional Risks	Example Unit-Level Risks
• Inability to prevent unauthorized modification of data • Failure to recover from system loss or extended downtime in a timely manner • Inability to ensure physical infrastructure security • Inability to maintain or replace obsolete systems/technology in timely manner • Inability to grow IT resources and data center capacity to meet campus needs • Inability to provide accurate and timely updates of core information systems to administrative areas • Inability to deliver satisfactory user support • Failure to comply with information security and privacy regulations • Inability to complete mission-critical IT projects in a timely manner	• Unencrypted data on stolen devices • Inadequate identity management systems • Inadequate protections against virus or spyware infestations • Sensitive data on server not managed by central IT • Inadequate data storage and backup policies • Inadequate controls of security of electronic commerce on campus (including credit cards)

Source: EAB interviews and analysis.

Risk Register Straw Man

Public Safety

Suggested Risk Owner(s): Director of Public Safety; Director of Environmental Health and Safety; Director of Risk Management

Institutional Risks	Example Unit-Level Risks
• Failure to implement and test adequate emergency preparedness measures and post-event contingency plans • Inability to ensure safety of faculty and students working and volunteering off-campus • Inability to ensure safety of faculty and students working, studying, and volunteering overseas • Failure to prevent significant lawsuits and claims relating to workers' compensation • Excessive force by campus policy that may result in severe injury and/or death	• Inability to protect against threats to safety and security of employees and students due to serious or petty street crime • Inability to maintain pedestrian, bicycle, and motorist safety on campus • Improper use of campus-owned motor vehicles by faculty, staff, or students • Failure to comply with Clery act requirements • Inability to properly control hazardous material on campus • Ineffective crowd management/public event controls

Research and Grants

Suggested Risk Owner(s): Vice President of Research; Director of Pre-/Post-Award Office

Institutional Risks	Example Unit-Level Risks
• Inability to detect or prevent major breaches in research integrity and ethics • Inability to detect or prevent conflicts of interest stemming from third-party contracts • Failure to comply with applicable human/animal subject regulations • Inability to prevent intellectual property infringement • Export control violations	• Inaccurate/incomplete effort reports • Inability to obtain audit report or audit certification from sub-recipients • Inability to obtain reasonable assurance that sub-recipient achieved performance goals • Inability to prevent research data loss or contamination • Failure to comply with sponsoring agency regulations and funding conditions • Inability to produce accounting and reporting materials that meet external parties' needs • Failure to ensure that grant funds are used in accordance with grant requirements • Inability to detect or prevent noncompliant cost transfers • Inability to control or prevent lapses in lab safety

Source: EAB interviews and analysis.

Risk Register Straw Man

Student Life

Suggested Risk Owner(s): Vice President of Student Affairs

Institutional Risks	Example Unit-Level Risks
• Inability to ensure that student mental health challenges are adequately addressed • Inability to recruit or retain students due to student dissatisfaction with campus experience • Failure to adequately serve and promote student groups	• Inability to prevent illegal alcohol and drug use by students • Failure to adequately prevent/control student hazing activities • Failure to ensure health standards of campus dining services • Failure to comply with FERPA requirements • Failure to adequately prevent or respond to incidences of sexual harassment or misconduct by students

Student Success

Suggested Risk Owner(s): Provost

Institutional Risks	Example Unit-Level Risks
• Inability to meet retention targets • Inability to retain/graduate students due to lack of early warning systems • Inability to retain/graduate students due to inadequate academic/advising support	• Inability of academic conduct/disciplinary procedures to detect and resolve misconduct • Inadequate numbers of advisors to meet student needs • Poor/outdated tracking of student progress to degree • Insufficient class sections to meet student demand for required courses

Source: EAB interviews and analysis.

Self-Diagnostic for Breach Response Preparation

Standard Practice | Strong Practice | Advanced Practice

		Yes	No
	Plan		
☐	• I have a breach plan in place.		
☐	• My breach plan is approved by the General Counsel and compliance staff.		
■	• My breach plan is reviewed and updated on a regular basis.		
■	• My breach plan defines response based on all critical data systems and information types.		
■	• My breach plan recommends staffing and support based on breach and data types.		
■	• My breach plan defines which technology, security, and legal staff are responsible for early incident triage.		
	Process		
☐	• I have a pool of incident leaders ready to coordinate and lead response when necessary.		
■	• Incident leaders understand the minimum staffing and resources necessary to meet forensic investigation needs, and when to escalate staffing to meet a more critical incident.		
■	• Technical staff are capable of collecting key performance indicators (e.g., mean time to identification) for response analysis.		
	Preparation		
☐	• I have drafted template release and notification documents approved by the General Counsel.		
☐	• I have a list of local breach services vendors and community contacts on hand and with all breach response leaders.		
■	• I verify and update all contact lists at least once quarterly.		
■	• After each incident, staff feed new threat indicators into security training, awareness, and response procedures.		

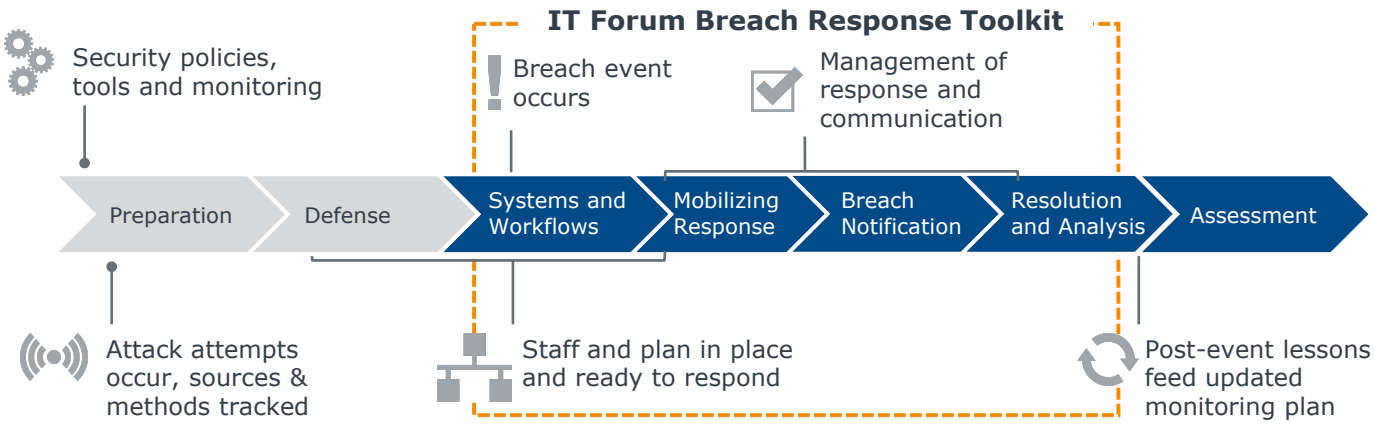
Source: EAB interviews and analysis.

Tools for Effective Preparation and Response

The Purpose of This Toolkit

This toolkit provides guidance on preparation and planning steps that will help members lay the groundwork for effective breach response. As depicted in the graphic below, these resources address only a segment of the data security framework. Use the advice and templates here to:

- Expedite breach response
- Reduce cost of both breach and response
- Minimize risk to the institution if a breach occurs
- Protect the reputation of the institution



Source: EAB interviews and analysis.

Laying the Groundwork for Response

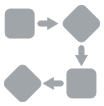
The last thing a technology leader needs to do during a data emergency is quibble over wording or worry about the chain of command. An effective plan provides clear, unequivocal definitions of a data breach, and staff members responsible for identification and response.

These frames for critical definitions and decision ownership are illustrative, combined from the existing plans of several institutions; the most effective policies will reflect campus-specific culture and policies.

Developing a Consistent Workflow to Triage Incidents

Does the Breach Affect a Critical System?

- Hierarchy of Priorities:
  - Human Life and Safety
  - Sensitive and Regulated Information[1]
  - Critical Networks and Systems
  - Business Continuity
  - Internal Customer Service



Who Owns Decisions During the Breach?

- Security Officer
  - Detect and Report Incident
- Chief and Deputy Information Officer
  - Approve Incident Category
  - Manage Internal Communication
- Incident Response Leader
  - Build Incident Response Team

Maintain a pool of potential incident response leaders that will be ready to lead breach operations when necessary; leaders will most likely come from the central IT office, but knowledge and operational ability trump department.

Response leaders need to be empowered to make spending and notification decisions, and will range in seniority appropriate to their incident.

Asking leaders to collect response metrics (e.g., mean time to fix problem) will help technology leaders measure the effectiveness of procedures against different breach types, and improve future response.

Incident Leader Coordinates, Measures Response

Responsibilities of the Incident Response Leader

Manage Internal Communication

- Define incident priority level and notify CIO if necessary
- Update key staff (e.g., CIO, General Counsel) on breach during investigation

Staff Response Team

- Recruit technical staff members with experience in compromised data
- As necessary, involve escalating group of key participants

Ensure Data Collection

- With technical team members, collect forensic evidence and KPI's
- Compile report on data breach and response for future security preparation

Incident Response Is a 'Drop Everything' Priority

Make sure that response leaders have the authority to clear all other team responsibilities during response.

1) At many institutions, this will include licensed research and other high-value targets

Source: EAB interviews and analysis.

Organizing Staff and Resources

When a breach occurs, quick action can staunch losses and expedite the mitigation process. Make sure that response leaders know and are authorized to carry out the actions that will mobilize response, limit damage, and collect necessary data on the breach.

Know the Necessary Immediate Steps

Mobilize Response

- Limit Damage:
  - Limit and secure access to compromised systems
  - If necessary, shut down affected machines and networks until forensic support arrives
- Alert Team:
  - Activate response leaders, who will be responsible for pulling in support personnel
  - Alert external response component groups (e.g., forensic data specialists)

Collect Information

- Document Key Facts:
  - Record date and time of breach incident, breach discovery, and when response efforts began
  - Record who discovered the breach, reporting chain, and who on campus has been notified
- Begin Assessment and Analysis:
  - Estimate impact to institution and possible victims
  - Prioritize response and notification components

A large team can slow response at a critical juncture, but too few participants can generate legal and reputational risk. Criteria that define initial steps and critical systems should build in recommendations for participation in the incident response team (e.g., type of impacted data, media relations, legal vulnerability).

Incident response leaders should prioritize capabilities above formal titles, and maintain a working knowledge of cross-departmental information technology functions.

Escalate the Response Team with the Incident

Incident Response Leader

- Lead Breach Response, Fix, and Verification
- Manage Resources and Communication

Technical Expert

- Collect Evidence, Lead Quarantine and Fix
- Record and Report Key Metrics

Compliance Officer

- Provide Guidance on Regulations and Rules Governing Compromised Data

Department IT

- Expedite Communication with Internal Staff
- Provide Context on Local Data Practices

Minimum Necessary

Medium-Level Threat or Risk

General Counsel

- Evaluate Legal Risk to Institution and Victims
- Assist in External Communication

Media Relations

- Coordinate All Internal and External Communication
- Protect Public Image of Technology Unit, Institution

High Risk to Resources or Reputation

Notifying Authorities and Constituents

The appropriate level of outside notification during a data breach depends on many factors, not the least of which is the university's legal position. The same policies that define critical incidents and systems should provide guidance on which data breach service providers and community contacts should be a part of the post-incident process.

Prepare to Move Past the Rolodex

Data Breach Services

- Forensic Investigators
- Private Investigators
- Outside Legal Counsel
- Mailing Services
- Call Centers
- Public Relations Firms

Community Contacts

- Law Enforcement
- Local Media Outlets
- Vendors Connected with Compromised Data
- Professional Organizations Affected by Breach

Keep All Response Leaders Updated with Key Contacts

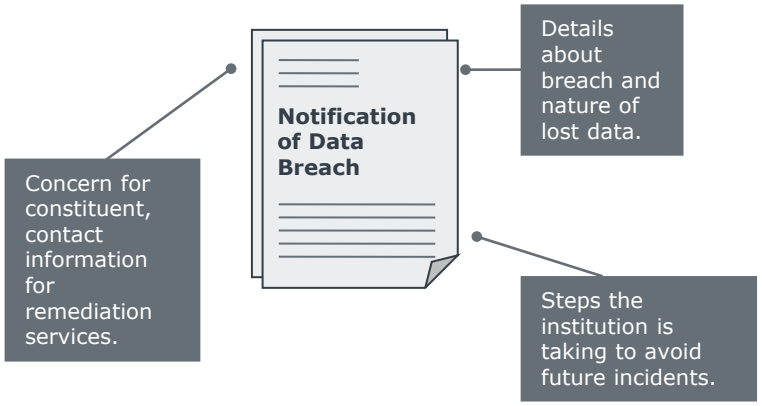
Review lists of breach service providers and community contacts at least quarterly, and make sure all response leaders have accurate information when launching into team recruitment and investigation.

While IT professionals understand the persistent challenges of data breaches, others involved may not react appropriately to incidents. Be prepared for a range of attitudes, from fear and anger to ambivalence.

Seek support from legal counsel and compliance units to pre-draft press release and victim notification language. This can expedite administrative tasks during a breach and ensure rapid response.

Strike the Right Tone

Sample Notification Letter



Remember that a breach can damage relationships with students, staff, and vendors. Ensure that every detail of external communication expresses sincere apologies and conveys determination to do better—down to the quality of paper used in outreach.

Source: EAB interviews and analysis.

Analysis and Process Improvement

A data breach can hurt constituents, incur significant costs, and damage the reputation of the IT function as well as the larger institution.

However, devoting the most skilled and valuable staff to forensic analysis and verification of breach processes can sap IT's ability to move past an incident and improve future risk management. Consider how more effective preparatory steps and response processes can improve time-based metrics.

The Key Performance Indicators of Effective Response

Standard Model

- Did we detect the breach and understand the problem?
- Did we assign an appropriate incident response team?
- Did we fix the problem?
- Did we notify the appropriate authorities and affected parties?
- Is service restored?

Progressive Model*

- Measure Mean Time to:
  - ✓ **Identify**: How long between breach and detection?
  - ✓ **Know**: How long between detection and understanding of root causes?
  - ✓ **Fix**: How long to resolve the situation and restore service?
  - ✓ **Verify**: How long to confirm resolution with affected parties?

If You Had One Security Breach Analysis Tool…

Private industry respondents report[1] that storage of audit trails using a packet capture system or SIEM (security incident and event manager) tool is the most effective way to detect and analyze security breaches.

Conduct a risk assessment of the entire organization and use it as a basis for a remediation plan. Often, assessments and remediation plans are reviewed and monitored by external auditors to ensure management attention and participation. An institution's Board of Trustees may also want to be briefed on these regularly.

Breach plan language, process documents, and discussions should focus on the connections between incident response and effective risk management rather than treat breaches as isolated incidents.

Build New Threat Indicators into Future Planning

Outside Attacks and Threat Indicators

- What was the source of the attack?
- What are the key characteristics of the attacking individual or group?
- What was the vulnerability exploited (e.g., social engineering, poor security architecture)?
- How can future response processes and communications for similar incidents be improved?

Inside Theft and Accidental Exposure

- What was the source of the theft or loss?
- What vulnerabilities were exploited or exposed by the incident?
- Has the responsible employee or department caused problems before?
- Can improved awareness and trainings for local staff prevent future similar incidents?

1) Cyber Security Incident Response: Are we as prepared as we think?" Ponemon Institute LLC, January 2014; http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/; EAB interviews and analysis.

35278
Cover image: iStock.

The best practices are the ones that work for **you.**SM

EAB

2445 M Street NW, Washington DC 20037
P 202.266.6400 | **F** 202.266.5700 | eab.com