



Top Ten **Emerging** Security Leader Issues

Where Do CISOs Feel Urgency to Change the Status Quo?

- | | | | |
|---|---|----|--|
| 1 | “Proceduralizing” Research Compliance | 6 | Socializing Campus Risk Tolerance Levels |
| 2 | Data Classification in a Distributed Environment | 7 | Time-to-Response Target-Setting |
| 3 | Scaling Security Segmentation | 8 | MFA for Students – Who’s Trying It? |
| 4 | Board Reporting Metrics | 9 | Device Enrollment for Admissions |
| 5 | Linking Security Metrics to Mission | 10 | Escalating Restrictions for Repeat Phishing Victims |

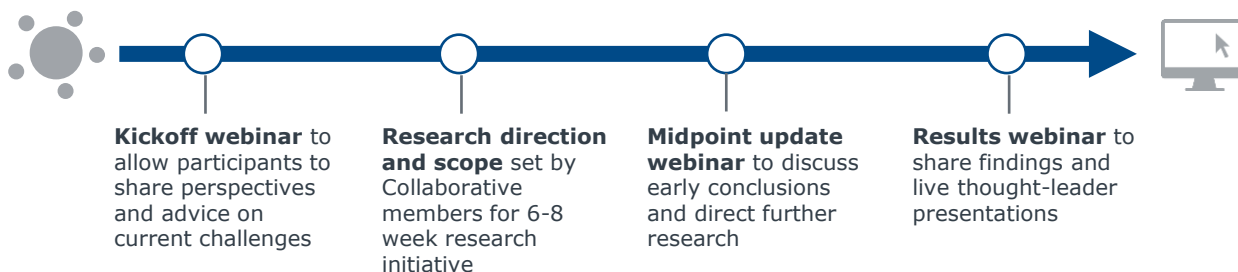
Introducing Functional Collaboratives

Giving Voice to IT Director Issues

Responding to CIO encouragement to help rising IT leaders expand their peer network and share advice on “live” issues, the Forum is delighted to launch our new membership service: IT Functional Collaboratives. They’re designed as cohorts of 10-15 director-level higher ed IT professionals that the Forum convenes virtually for a roundtable discussion to share “pain points”, calibrate campus policies, and compare assumptions about emerging technology rate-of-approach and change management strategies. In contrast to peer groups in state systems and industry associations, which are often successful at defining high-urgency questions but lack capacity to research answers, Functional Collaboratives will pick the handful of issues of broadest interest for an 8-week research effort culminating in short reports profiling innovative practitioners or aggregating reusable planning and communications IP.

Over the next membership year, the Forum will start Functional Collaboratives for the major boxes on the IT organizational chart. This report profiles first findings from our inaugural Collaborative, serving CISOs and security directors.

Timeline of a Functional Collaborative



Functional Collaboratives Launching across 2017-18



What's Keeping Security Directors Up at Night

All the Perennial Security Issues Still There

Each of the ~50 security directors participating in the collaborative took five minutes describing pain points (and victories) on their campuses. Without fail, they began by reiterating the shared, likely perennial challenges of the security role: vulnerability proliferating faster than resources; the need to continuously improve response times in threat detection and remediation; elevating security education and “human engineering” without campus perceptions of intrusive bureaucracy. These issues remain in full force, with security leaders always eager for new approaches.

New, or Newly Urgent Issues Now Arising

Beyond these the perennial issues, Collaborative participants were eager to see if others were spending more time and mindshare on challenges of emerging importance, which standard operating procedures aren't fully prepared to handle. From of the hundreds of perceptive comments across our webinars, a common list of shared challenges took shape. Again, these are not necessarily the most important CISO issues, but ones where members were seeking to compare notes and learn from each other.

Top Ten Emerging Higher Education Security Leader Concerns

- | | | | |
|----------|---|-----------|--|
| 1 | “Proceduralizing” Research Compliance | 6 | Socializing Campus Risk Tolerance Levels |
| 2 | Data Classification in a Distributed Environment | 7 | Time-to-Response Target-Setting |
| 3 | Scaling Security Segmentation | 8 | MFA for Students – Who’s Trying It? |
| 4 | Board Reporting Metrics | 9 | Device Enrollment for Admissions |
| 5 | Linking Security Metrics to Mission | 10 | Escalating Restrictions for Repeat Phishing Victims |

#1 “Proceduralizing” Research Compliance

As the demand for resources dedicated to information security for researchers increase, security directors look for ways to identify contracts at risk, and protections to scale.

— “ —
Researchers used to think they could handle information security themselves, but with the new NIST-800 171 requirements we anticipate more and more requests for assistance from our office. And we need to make our processes more efficient to handle this increase in volume.”

CISO
Public Research University

New Compliance Regimen Too Visible for an Afterthought

High-research and aspiring research universities foresee spikes in the quantity and complexity of research security compliance projects, driven by several concurrent forces:

- › New NIST 800-171 and FIMSA guidance
- › Relatively flat NIH and NSF funding causing more PIs to diversify funding sources to new agencies like Defense and Energy, and to seek philanthropy and industry contracts, both of which carry more stringent security requirements
- › Across the board, more explicit security language in grants and contracts making it impossible for PIs to ignore security as was common in the past

Looking for Occasions and Catalysts for More Standard Procedures

Single Audit: Many institutions are testing whether the new NIST guidelines can serve as a catalyst for consolidating research security compliance, in pursuit of more professionalized security expertise to PIs and “single audit” capability for the institution.

Rationalizing Frameworks: However, a sizable minority of CISOs considered single frameworks and consolidated audits utopian, and instead are consulting with the research enterprise to determine how many different frameworks need to be supported.

Status Quo Mutually Unsatisfactory: Both camps agree that status quo research security compliance is overly opaque and labor-intensive. PIs are uncertain what controls are required, and security heads uncertain how long and labor-intensive projects are and whether decentralized units are consistently compliant.

#1 “Proceduralizing” Research Compliance (cont.)

Security directors seek to increase their interaction with researchers during the pre-and post- award processes through communications that demonstrate the risk to research data, templates that collect information about data to secure, and common solutions to those data security concerns surfaced.

Blueprinting the Ideal Research Security Toolkit



Security Requirements Menu

Low-tech cheat sheet or menu-driven decision support screen specifying what protections are needed for various data types for various grant or contract categories



Integration of Pre- and Post-Awards Systems with Security

Automated workflows that prompt IT when new grant proposal initiated so that security requirements understood and grant language about controls automatically forwarded; compliance monitoring when grant received



Standardized and Well-Socialized PI Policies

Provost, VPR and dean support of campus-wide device usage and storage policies



Effort and Turnaround Time Calculators

Accurate estimation (potentially tied to Project Management software system) of security staff hours and time-to-compliance for research security projects, which currently are opaque and ad hoc to IT and PIs alike

#2 Data Classification in a Distributed Environment

Security directors desire approaches for routinizing and selectively automating central data tracking in the distributed campus environment.



It takes a ton of work just to figure out what security is supposed to be securing."

Information Security Analyst
Private Master's University

Is Anyone Having Success Hardwiring Data and Asset Tracking?

CISOs commiserated that campus hunger for data analytics has meaningfully increased the complexity and effort of information asset tracking. While most schools are confident that their classification rubrics are adequate, few have comprehensive understanding of what kinds of data are on the network vs in the cloud, and what kinds of users have access.

Benchmarking National Practice



Asset Tracking Automation: What tools are effective in network inventory tracking? Are people using scanning tools not just to identify end points, but to ascertain the data contained on objects? If so, are there FERPA, HIPAA or other compliance considerations?



ERP Data Mapping: Security directors fear two endemic ERP-related concerns: inability to map ERP data flows and access privileges to end users, and unwitting extraction of sensitive data from the ERP for storage in less-secured shadow systems or devices



Using ERP Upgrades as Occasion to Introduce Data Mapping and Role-Based Trainings: CISOs in the midst of ERP upgrades and cloud migrations wished they had pre-wired a concurrent workstream for data mapping and role-based security trainings, with stronger trainings required for individuals and devices working with sensitive data categories

#3 Scaling Security Segmentation

Security directors anticipate the political challenges of changing access with fewer profile types and less customization.







When you have multiple campuses, each with their own domain, identity management challenges multiply. We need to straighten out admin access and go to a universal identity management system."

CISO
Private Master's University

How Far, How Fast?

Security directors wanted to compare "how far, how fast" their campuses were realizing the broadly-shared but incompletely implemented goal of mass-segmenting security by information type and end-user profiles.

Where CISOs Want to Compare Notes

-  Who's segmenting what?
-  How many different segments can we ultimately support?
-  What is current and aspirational role-based ID management?
-  How should we classify devices based on data stored?

#4 Board Reporting Metrics

CISOs desire more exposure to boards to make the case for budget and human resources, but question the time commitment (and career risk) involved.



I really struggle to provide metrics that are meaningful to anyone but me. And I worry that if I put a number or graph in front of the board, all they'll see is the red slice."

CISO
Private Research University

What to Report, and Who Should Report It?

The good news is that boards are more aware of (and willing to spend on) security and risk management. The bad news is that security directors still don't think they are striking the optimal balance between technical security metrics (that cause board members' eyes to glaze over) and more qualitative assessments (which may not fully spotlight security costs, risks and performance).

How are Others Handling These Board Communication?



Meeting Presentations: Who presents updates at board meetings – the CISO, CIO or CBO?



Inter-Meeting Updates: How do we communicate with boards between meetings?



Shielding Leadership from Inbound Questions: How can we provide just-in-time reports on incidents without setting off a chain of potentially unnecessary inbound questions disruptive to presidents, provosts, CBOs and CIOs?

#5 Linking Security Metrics to Institutional Mission

CISOs seek approaches that plausibly connect technical and operational metrics to mission goals that resonate across campus.



I really struggle to articulate the value of security to the rest of campus. How do we embed security in the IT governance process, and change the script so that our involvement is seen as an asset and not a hassle?"

CISO
Public Master's University

Reframing Security as a Value Added Service

Security directors broadly shared the aspiration to reframe security reporting away from purely technical metrics that connote technology abstractions and expense, and instead showing how security activities advance mission goals in enrollment, student success, and faculty productivity.

Wanted: Best Examples of Cascading, Interlocking Metrics



How Security Advances Research, Student

Success, and Enrollment: Members were interested in comparing and adopting successful approaches for linking the CISO performance dashboard to key metrics in the institutional strategic plan



Making the CISO Dashboard Lay Person-Friendly:

What metrics belong on the president and dean dashboards? Which technical metrics (if any) merit prominence and leadership education?



Faculty Communications: What communications strategies and mediums best embed in faculty workflows, and convincingly portray how security policies are in their self-interest?

#6 Socializing Campus Risk Tolerance Levels

CISOs agree that an attitude across campus that security should only fall under the purview of IT limits the success of programs to decrease risky behavior and fosters a “head in the sand” mentality.



My campus leadership is more aware of risks than ever before, but they still don't understand the tradeoffs for the choices that we're making related to cybersecurity, disaster recovery, and other concerns."

CIO
Private Baccalaureate College

Clarifying Tradeoffs in Risk Management Decisions

Security directors report an overdue-but-necessary reset of campus leaders' security expectations: more are aware that there simply aren't resources to secure everything, given mushrooming vulnerabilities and industrial-strength hackers. Security directors said the next step in this socialization process is to set up a more formal, transparent process for defining risk tolerances for different asset classes.

Breach Response SLA Targets for Different Kinds of Incidents

CISOs wanted to know the prevalence of schools formally publicizing breach response target times for different kinds of incidents, both to understand state of practice of security SLAs and as a back-of-the-envelope, easier-to-get benchmarking range of incident response times.

#7 Time-to-Response Target-Setting

With reliable higher education benchmarks hard to come by, CISOs see value in norming against other institution's goals for breach response.



If 10 seconds isn't realistic, what targets should we be looking at for incident response- or at least what's the average? And then how do we gather that information effectively, so that we know if we're meeting those targets?"

CISO
Public Research University

Ideal Incident Response Benchmarks Hard to Come By

As is often the case with IT benchmarking, security directors said they had access to breach response benchmarks but wanted better ones, focusing more on higher education and broken out by systems architecture.

SLA Targets - A More Accessible Alternative?



The Specificity of the Most Desirable Metrics Limits Collection Capabilities: CISOs and Security directors agree that such metrics are too hard get, but emphasize how valuable they'd be to breach response continuous improvement efforts



Metrics that Compare Targets are Easier to Collect: Directors suggested that simply sharing time-to-response *SLA targets* would itself be a useful comparison



An Often Suggested Benchmark: What is the security group targeting or promising to the campus for different incident types?

#8 MFA for Students – Who’s Trying It?

Many institutions have already implemented multi-factor authentication for campus employees but hesitate to move forward with MFA for students.



We were successful in our rollout of MFA for faculty and staff, but when we look around we don't see anyone who's attempted implementation with students. This is a political problem, not a technical one, and I could use a roadmap."

CISO
Public Research University

After Success with Faculty and Staff, What's Next?

Security directors agree that students are perhaps the fastest-growing category of campus vulnerability, as thousands come on campus anew each term, with new devices, to exchange sensitive financial, FERPA, and HIPAA data, but little understanding of or interest in campus security practice.

Seeking Reference Policies and Pilot Programs

More Collaborative participants than might have been expected said they've successfully introduced MFA for selected faculty and staff actions, and wondered if any campuses had taken the next step of extending MFA to student accounts. None had, yet, with the general consensus that introducing a security inconvenience cut against the grain of "perfecting the student experience" now a priority for many.

#9 Device Enrollment for Admissions

CISOs report an emerging point of contention with admissions partners whose desire for device-agnostic applications can create vulnerabilities.



One of the first opportunities to make an impact on a perspective or a new student is through their experience with the admissions interface and the network on our campus. We want to make this interaction frictionless without compromising on security.

Information Security Officer
Private Research University

Finding the Balance Between Security and Access

For a handful of security directors, the tension between student experience and security extends to the admissions function. At these tuition-driven institutions, admissions was requesting frequent exceptions to campus acceptable use policies to make the application process more flexible.

Sourcing the Crystal Ball for Device Preferences

Rather than consistently having to say “no” to admissions, security directors at these schools instead want better forecasting intelligence about high-school and adult learner device preferences, so that security controls can be established in advance of applicant demand.

#10 Escalating Restrictions for Repeat Phishing Victims

While not an “emerging” concern, the perennial challenges related to phishing have not diminished, despite time and effort to raise awareness through communication campaigns and self-phishing.



Concerns around phishing have actually increased over the past two years. Even people at the highest level of the institution are phished, and MFA doesn't always prevent that – they just fall for it twice!

CISO
Public Research University

When the Usual Sanctions Don't Alter Behavior

Most participants in the Collaborative were regularly self-phishing – using that approach as a user risk and education tactic appears quite uncontroversial. The questions instead were about what to do about “repeat victims” – faculty and staff who don't change behavior after the normal run of security awareness interventions.

What are the Right Number and Nature of Interventions?



Educational Interventions: Every self-phisher had a repertoire of IT-led education interventions



Publicizing Phishing Victims: Some had the extra step of “name and shame” lists of repeat victims shared with deans or unit managers



Restricting Access: A handful of CISOs said phishing was such a high-leverage, behavior-dependent threat that they were considering importing the practice ascendant in the private sector of “three strikes and you're out”: restricting the credentials of repeat victims pending completion of a formal security awareness course and ongoing monitoring. Such a practice is obviously a big ask in the higher education culture, and no one yet had implemented such a policy, but security directors agreed that it is not out of the question in the future

In Appreciation

The IT Forum Thanks the Participants in Our Security Functional Collaborative

Ball State University

Tobey Coffman

Baylor University

Jon Allen

Berea College

Huapei Chen

**California State University
– Fresno**

Orlando Leon

**Carnegie Mellon
University**

Mary Ann Blair

The College of New Jersey

Matt Cesari

Coppin State University

Sribala Narasimhadevara

Drake University

Peter Lundstedt

**Florida International
University**

Helvetiella Longoria

**George Washington
University**

Brian Markham

Indiana University

Tom Davis

**Michigan State
University**

Seth Edgar

**Louisiana State
University**

Sumit Jain

Mount Royal University

Michael Barr

**Northern Kentucky
University**

David Renaker

Norwich University

George J. Silowash

**Southern Methodist
University**

George Finney

Rice University

Marc Scarborough

**San Jose State
University**

Mike Cook

Spalding University

Ezra Krumhansl

Stony Brook University

Matthew Nappi

Syracuse University

Christopher Croad

**University of Alaska
Anchorage**

Max McGrath

University at Buffalo

Jeff Murphy

**University of California
Santa Barbara**

Sam Horowitz

University of Manitoba

Patrick McCarthy

**University of
Massachusetts Amherst**

Matthew Dalton

**University of Nebraska-
Lincoln**

Rick Haugerud

**University of North
Carolina Chapel Hill**

Kevin Lanning

University of Oklahoma

Ron Fellhauer

**University of
Tennessee- Knoxville**

Bob Hillhouse

University of the Pacific

James August

**University of South
Alabama**

Mark Wilson

**University of Texas at
Arlington**

Kathryn Jacobson

**University of Texas at
Tyler**

Greg Brandenburg

**University of Wisconsin
Oshkosh**

Mark Clements

Wayne State University

Kevin Hayes

Webster University

Kevin Heuser

West Virginia University

Alex Jalso

Western Illinois University

Robert Emmert

Xavier University

Ashley Penchion

Additional Resources for Members

Information Security Management

Elevating Security Awareness

Increasing the Relevance and Scalability of End-User Education

- How do we compellingly make vulnerabilities real to boards, presidents' cabinets, faculty and students?
- What are the highest-impact central subsidies and unit penalties to speed adoption of risk-aware behaviors by faculty and staff?

Hardwiring Data Breach Responses

Reducing Operational Costs and Streamlining Stakeholder Communications

- How are best-in-class institutions (even smaller ones) staffing damage assessment, stakeholder notification and evidence collection?
- What are the right metrics to track to continuously improve time-to-response and breach-related financial costs?

Project Director

Scott Winslow

Contributing Consultants

Anna Krenkel

Design Consultant

Kevin Matovich

Senior Vice President

Chris Miller

LEGAL CAVEAT

EAB is a division of The Advisory Board Company ("EAB"). EAB has made efforts to verify the accuracy of the information it provides to members. This report relies on data obtained from many sources, however, and EAB cannot guarantee the accuracy of the information provided or any analysis based thereon. In addition, neither EAB nor any of its affiliates (each, an "EAB Organization") is in the business of giving legal, medical, accounting, or other professional advice, and its reports should not be construed as professional advice. In particular, members should not rely on any legal commentary in this report as a basis for action, or assume that any tactics described herein would be permitted by applicable law or appropriate for a given member's situation. Members are advised to consult with appropriate professionals concerning legal, medical, tax, or accounting issues, before implementing any of these tactics. No EAB Organization or any of its respective officers, directors, employees, or agents shall be liable for any claims, liabilities, or expenses relating to (a) any errors or omissions in this report, whether caused by any EAB organization, or any of their respective employees or agents, or sources or other third parties, (b) any recommendation or graded ranking by any EAB Organization, or (c) failure of member and its employees and agents to abide by the terms set forth herein.

EAB, Education Advisory Board, The Advisory Board Company, Royall, and Royall & Company are registered trademarks of The Advisory Board Company in the United States and other countries. Members are not permitted to use these trademarks, or any other trademark, product name, service name, trade name, and logo of any EAB Organization without prior written consent of EAB. Other trademarks, product names, service names, trade names, and logos used within these pages are the property of their respective holders. Use of other company trademarks, product names, service names, trade names, and logos or images of the same does not necessarily constitute (a) an endorsement by such company of an EAB Organization and its products and services, or (b) an endorsement of the company or its products or services by an EAB Organization. No EAB Organization is affiliated with any such company.

IMPORTANT: Please read the following.

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

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

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