Budget Conscious Strategies for Information Security

Building Institutional Capability and Sustainability

HEISC Working Group Paper

APRIL 2018

EDUCAUSE

Table of Contents

This paper is part of a series of papers prepared by members of the Higher Education Information Security Council (HEISC) to provide budget-conscious advice for information technology leaders and managers tasked with developing and delivering institutional information security programs and services. Learn more about HEISC and the EDUCAUSE Cybersecurity Program.

Introduction

Information security programs require investments in resources and tools and need a deliberate plan for sustainability and success. Such investments can often be costly and hard to justify to institutional leaders, especially in a budget-strapped environment. However, not all investments come with a large price tag. This paper offers a series of relatively low-cost tactics that can used to build institutional information security capability. These tactics include establishing a knowledge framework; building relationships across campus; training your team and your community in information security concepts; and establishing a sense of shared responsibility for information security across the institution (and within the IT organization). Ultimately these tactics contribute to building a roadmap that can help your institution maximize scarce resources and achieve its desired information security stance.

Connect with Information Security Professionals

Information security spans technology, geographic regions, laws, and cultures. When building an information security program, it is essential to keep this broad context in mind. There are excellent professional resources available such as member groups and social networking to help you understand and establish a knowledge framework for the latest information security issues. Member groups like REN-ISAC, volunteer groups like the Higher Education Information Security Council (HEISC) of EDUCAUSE, and the EDUCAUSE Security Discussion Group offer access to a community of information security professionals from higher education institutions around the world. In addition, some regional security groups or industry-focused groups like the MS-ISAC can be joined with no membership cost. The professionals who work at, support, and participate in these groups are constantly assessing and releasing security tools and resources, as well as hosting timely events that endeavor to help institutions stay informed in a constantly shifting security landscape.

Social media is a great touchstone for assessing your security knowledge, seeking inspiration for where you want to go, and staying abreast of emerging threats. On Twitter, there are many worthwhile information security handles. Consider following individuals who are interested in security, including CIOs, CISOs, and other security professionals. In addition, consider following the Twitter handles of organizations for whom security is a mission, including groups like the National Cyber Security Alliance (@StaySafeOnline), REN-ISAC (@renisac), and HEISC (@HEISCouncil). Even a passive following can yield timely notifications regarding relevant information.

Train Your Team and Your Community

Encourage your entire team, as well as your community, to leverage professional development opportunities to learn and share experiences and solutions related to the ever-changing world of information security. Webinars provided by EDUCAUSE and free massively open online courses (MOOCs) like the University of Washington's four-part series on cybersecurity are great ways to gain new knowledge or give back to the community.

Across your wider institutional community, even the smallest teams might train by using department-specific talks, relevant security articles distributed via faculty and/or staff email blasts, advertisements in the university portal, guest lectures, and more. One idea is to enable "just in time" learning for your community. For example, self-enrolled courses can be created within your institution's SCORM-compatible LMS to enable e-learning. PhishMe offers 17 free SCORM modules covering regulatory topics like the European Union General Data Protection Regulation (GDPR), the Payment Card Industry (PCI) standards, and other regulations concerning personally identifiable information (PII), cybersecurity, and business email compromise.

As security awareness builds across your community, more active types of training begin to make sense as next steps. If you believe your institutional culture is conducive to self-phishing, get buy-in from the institution's administration and other institutional governance bodies (e.g., faculty senate) to begin quarterly self-phishing campaigns. A free and open-source self-hosted application called GoPhish is one option. There is also a free cloud-hosted self-phishing assessment tool called Duo Insight. Tabletop exercises, where participants role-play a specific security scenario, are active learning tools to assess how a security incident may play out and to understand your community's readiness for such an incident. Sean Mason, Director of the Incident Response Practice for Cisco, blogged about how to conduct such an exercise and even provided a few mock scenarios that can be used to get you started. For all training activities, it is important for key stakeholders and leaders to participate, to model and emphasize the shared responsibility of security. Such an exercise can be a liberating way to provide context and spark creative, "outside the box" ideas.

Build Relationships with Security Stakeholders

When your security leaders achieve a level of fluency about information security in higher education, it is incumbent to spread that knowledge across your institution, starting at the top of the organizational chart. The president, provost, CFO, CIO, deans, and other institutional leaders have undoubtedly heard about customer breaches involving the federal government, Equifax, Target, and Home Depot. Connect these events in a relatable way to higher education and outline specific ways in which information security aligns with the institution's mission and goals, including providing a safe learning environment for students. Develop a process for regularly checking in with institutional leaders to ensure that expectations regarding security awareness and compliance are met at every level of the institution. Distribute timely and relevant communications that relate security items in language that is easily understood and free of tech jargon. One example is the uptick in phishing around tax time each year during the distribution of W2 forms. Time a message to go out during that period detailing what to watch out for and the ramifications of tax info being accessed and acted upon by unauthorized actors.

With the core administration on board, begin to foster a model where security is understood as a shared responsibility. One relevant way to engage your entire campus in security awareness is through participation in National Cyber Security Awareness Month (NCSAM) each October. Participation enhances your institution's information security awareness program. Your institution can sign up as an NCSAM champion each May, taking advantage of the resources available.

In time, you may be able add your own content to expand the training as institutional resources allow. For instance, Texas A&M "gamifies" cybersecurity training by internally developing and releasing a new game each year coinciding with NCSAM. Supported by the StaySafeOnline team of the National Cyber Security Alliance, tools for getting involved in NCSAM are available on the website or can be conducted using the NCSAM Planning Toolkit provided by SANS.

In addition, EDUCAUSE develops security awareness campaign materials each year that can be adopted by institutions to assist with building awareness about security topics.

Build Security Awareness

A community's cybersecurity awareness has been said to have the greatest impact on the security of an organization. This is because most institutions use a decentralized, delegated access control model and make a lot of information available to many different constituencies. Use a repeatable training model that integrates with an already existing directory for single sign-on; leverage the timing requirements of other legally mandated training (such as anti-harassment, Title IX, ethics, etc.); and consider simple dashboards to assist department and unit leaders in managing completion. Tactics for building awareness include:

- Refreshing formal information security training each year. There are always new threat vectors and stories to communicate to your organization.
- Encouraging information technology staff to share timely security-related information such as the discovery of new malware or helpful information about the sharing of user permissions in the cloud. For example, share information and training processes such as the training that cashiers participate in as part of PCI compliance.
- Leveraging existing technologies such as internal email lists, blog tools, Slack channels, or your help desk's knowledge base that allow you to repackage security information from sources such as the National Cyber Security Alliance, Multi-State Information Sharing and Analysis Center, SANS, and information security professionals on Twitter.
- Using existing security communications in your other communications campaigns. Refer to them as often as you can. Most members of your community will never seek out the security website or email list, but referencing them in other documentation and training sessions will increase readership. Any searches for relevant and associated topics should direct searchers to security information.

Whether there is a dedicated team or decentralized and interested parties, the security program is a community effort and need not be housed in one department. Many security teams have digital and cyber teams separate from physical security such as officers and building controls such as lights, locks, and cameras. A strategic goal of all sensible security programs is to improve visibility into your institution's security posture. This is ultimately the key to enabling your institution to manage technology assets and services that rely on those assets in their area of responsibility.

Position Security as a Shared Responsibility

Institutions with a robust and clear policy framework typically effect change more quickly. In practice, this requires a policy model where the department responsible for the university service is also responsible for the security of the service. For example, when a department launches a new website, certain individuals should be responsible for the content of the site while others are responsible for its security and technical architecture.

Encourage all faculty and staff to embrace ownership of their data assets. If policies do not exist, work to create and implement a clear policy framework that begins with acceptable use, data governance, data classification, and ultimately, incident response. Free resources for the development of such policies, as well as examples of existing and exemplary institutional policies, are available via the Higher Education Information Security Guide.

Consider forming a security task force and an executive incident-response team that will set recommendations for corrective action during critical security incidents. These teams will serve at least two purposes: (1) The institution will become increasingly aware of security concerns, and (2) the security team will unify the institution by allowing all stakeholders to participate in the process and the outcome. One activity could be the documentation of your institution's response to known compliance concerns, such as PCI requirements or the Gramm-Leach-Bliley Act (GLBA). LeTourneau University has developed such a document that provides a guide to the institutional community and that also serves as a reference for auditors. Such documentation can yield sufficient evidence of compliance to an auditing body and can even be adapted to the templates used by auditors to assess an organization.

Assess Your Security Stance and Build a Security Roadmap

Technology risk assessments are frequently security focused, but an increasing number of institutions are finding that a broader assessment is helpful in allowing a university to address risk across all components of its technology infrastructure. This may include strategies and procedures for data backups, access control and business continuity, and newly developed web services.

A free tool for EDUCAUSE members that provides a common framework for measurement is the EDUCAUSE Information Security Program Assessment Tool, developed by HEISC. After downloading the assessment spreadsheet from the EDUCAUSE website, be sure to read all of the tabs, which will walk you through the questions, show how to use the tool, and explain how to score your organization and your institution. For questions about and help using this tool, you can contact security-council@educause.edu.

After you assess the current state of your information security program using this tool, various information security gaps will be highlighted. The next step is to think about risks associated with those gaps. What could happen? What is the likelihood of those events? Engage your institutional community, in and outside the IT organization, for thorough and thoughtful answers. Once you identify and understand your risk, you can rank known gaps, which will become actionable priorities in your security strategic plan. Using the security program assessment tool establishes your baseline capabilities, and the strategic plan becomes the security roadmap that will help you achieve an increasingly mature information security program.

Strategic planning also can help you define larger goals and an approach to assist in closing gaps. Examples might include establishing a set of technical policies and standards, implementing security awareness training, or creating a data governance committee. As much as possible, align your information security strategic activities with already established institutional goals, the institution's IT strategic plan, or the institution's strategic plan. The list of strategic priorities may reveal unexpected progress. For example, multifactor authentication is an obvious example for phishing mitigation, but other IT projects and initiatives could include next-generation desktop management software that has automated inventory, imaging, antimalware, and data-loss-prevention modules that are represented in all of the security frameworks. Microsoft and Google include advanced threat prevention (interrogation of suspicious logins including impossible travel and login attempts from new devices) and data loss prevention (identification of personal information in email and cloud storage) as part of their offerings by default, which links cloud strategies to security initiatives. In today's security climate, many of your existing investments have a security-related component or can be linked to a security theme.

Conclusion

No matter your approach to your information security program, do not lose sight of the core responsibility: meeting the needs of educational, research, and administrative functions while understanding the risk tolerance at the institution's executive level. Leverage all the available tools, tap into the community, and inform executive leadership. Enable your institution to phase in changes that improve the overall risk posture. In many cases, unit leaders will begin to take guidance from security discussions and incorporate security elements into their areas with little cajoling. When everyone takes responsibility for security, the institution wins.

Acknowledgments

This paper was prepared as a group effort by a number of higher education professionals passionate about evolving institutional information security practices, particularly in resource-constrained environments. We hope you find these recommendations and resources useful in establishing and improving your institution's information security programs.

- Bill Barnes (Bloomsburg University)
- Alan Bowen (Franklin & Marshall University)
- Michael Davis (LeTourneau University)
- Dale Fay (Michigan Medicine)
- Chris Gregg (University of St. Thomas)
- Sean Hagan (Yavapai College)
- Todd Herring (REN ISAC)
- Kyle Johnson (Chaminade University of Honolulu)

- Tolgay Kizilelma (University of California, Agriculture and Natural Resources)
- Karen McDowell (University of Virginia)
- Dave Nevin (Oregon State University)
- Michael Perdunn (University of Nebraska, Omaha)
- Paul Perrone (University of Rhode Island)
- Sharon Pitt (University of Delaware)
- Dan Sanders (Widener University)
- Theresa Semmens (University of Miami)
- Isaac Straley (University of California, Irvine)
- Tina Thorstenson (Arizona State University)
- Adam Vedra (Calvin College)
- Nathan Zierfuss-Hubbard (California State University)
- Joanna Lyn Grama (EDUCAUSE)
- Valerie Vogel (EDUCAUSE)

About EDUCAUSE

EDUCAUSE is a higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. Technology, IT roles and responsibilities, and higher education are dynamically changing. Formed in 1998, EDUCAUSE supports those who lead, manage, and use information technology to anticipate and adapt to these changes, advancing strategic IT decision making at every level within higher education. EDUCAUSE is a global nonprofit organization whose members include U.S. and international higher education institutions, corporations, not-for-profit organizations, and K–12 institutions. With a community of more than 99,000 individuals at member organizations located around the world, EDUCAUSE encourages diversity in perspective, opinion, and representation. For more information please visit educause.edu.