Budget Conscious Strategies for Information Security

Building Resources on a Budget

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

It is no secret that many higher education institutions are short on time and resources as they seek to protect the security of their IT systems and data. The most recent EDUCAUSE Information Security Almanac reported that among responding institutions, only 3% of central IT spending is on information security and identity and access management activities; the almanac also noted that colleges and universities have an average of just two central IT information security personnel per 10,000 institutional FTEs. And those are the median numbers—many colleges and universities operate their institutional information security programs with far fewer resources. Operating information security programs with scarce resources requires a fair amount of creativity and flexibility. This paper seeks to share some pragmatic and actionable ideas for building security resources on a budget. The ideas are grouped based on **shared** staff, services, and tools; strategies for **staffing**; and **tools and resources**.

Shared Staff, Services, and Tools

By sharing the costs and risks of certain IT services and tools, as well as particular IT staff positions, institutions can obtain benefits that might otherwise be out of reach.

Shared CISOs

Only 34% of institutions have a dedicated person whose primary responsibility is information security. This means that many institutions do not have someone who is a full-time information security leader, like a chief information security officer (CISO).

Higher education encourages collaborative ventures, but competitive forces often play a part in institutional relationships as well. Careful selection of partners for any collaborative service, especially around information security services, can be

the key to success. When these efforts work, they can provide access to specialized resources otherwise unavailable to small institutions and enhance the overall security stance of the participating institutions. When they don't, they can represent a significant setback. Public institutions that are part of a system can often look to a central office or flagship institutions to lead the way, or they can find a group of peers in their system and build on existing relationships. Private institutions should consider looking to existing consortia or find like-minded institutions with which they can work.

Sharing a CISO/information security office can be done. For example, three geographically separate institutions (Chaminade University of Honolulu, University of Dayton, and St. Mary's University in San Antonio, TX) leveraged the Association of Marianist Universities and worked with the CIOs of each institution to form a shared ISO office. This partnership works well for three reasons. First, the three institutions share a common purpose and philosophy through their Marianist heritage. Second, one institution—University of Dayton—is both larger and has an information security program already in place that could be scaled to meet the needs of all three schools. Third, the institutions do not have any meaningful cross-applications, so there is little concern about competing for students.

To consider using this approach, think about the system you might belong to, other similar institutions in your geographic area, and any consortia in which your institution has membership. Using your existing networks can help smooth some of the growing pains that occur as institutions look to share a security leadership function.

Shared Services and Collaboration

About one-third of institutions share services. While the use of shared services is not specific to security, research found that larger institutions and institutions that are part of systems are more likely to share services, and institutions that share services tend to share more than one.

One form of shared services is peer risk assessments. Periodic, external reviews of higher education information security programs help ensure that resources are correctly focused, a critical task given the rapidly evolving nature of cybersecurity and the limited resources available to most institutions. Of institutions that perform risk assessments, 68% do so for planning/prioritizing institutional security work.

Risk-assessment reviews from service providers, while illuminating, tend to be quite costly. One solution to the costly risk-assessment review is to approach subject matter experts within the higher education community to conduct such a review. Often these reviews will be less expensive than their commercial counterparts. Moreover, peer reviewers from the higher education community may be particularly astute at understanding the constraints that higher education information security programs work within, suggesting controls and solutions that are actionable by a higher education institution. Good planning and direction of scope on the front end are required to make a peer review risk assessment successful. The goals and scope of work for the review must be clearly defined, the peer reviewers and the requesting institution must all understand and agree to the terms of the engagement, and the deliverables must be agreed upon before the engagement starts.

In addition to sharing services, value can be derived from routine collaboration among like institutions. In this context, the Arizona Community Colleges conduct monthly conference calls and engage in ad-hoc discussions on topics of mutual interest, including audit preparation, policy conformance, and budget planning. The CIOs of the member institutions coordinate an annual IT-centric conference held at a rotating member institution. Expenses average $100 per attendee excluding travel, representing a low-cost way to encourage collaboration and knowledge-sharing among peer institutions. Additionally, Slack channels have been established around multiple topic areas, including information security, systems administration, and application development, to allow for improved communication across member institutions.

Members need not be of similar size or scope or maturity level to derive value from information sharing. In Northern Arizona, multiple public colleges and universities meet on a monthly or quarterly basis to review topics of shared interest, generally focused on information security and compliance. Despite significant size, scope, and resource differences, each institution is held to similar regulatory compliance expectations, and as a result, members have found value in sharing the status and results of annual IT audits, policy and procedure development, incident response handling, and tools and services used in support of information security efforts.

Shared-Tool Acquisition

Security tools such as vulnerability scanners, firewalls, antivirus systems, and intrusion prevention/detection systems are often beyond the budget of a small

institution. By forming a consortium or partnership, similar-sized institutions within a state or regional area can reduce costs, making the purchase of such tools and staff affordable. EDUCAUSE research shows that about 80 percent of institutions are part of at least one purchasing consortium. Institutions that are part of such a consortium report that the top benefits include the streamlining of purchasing requirements, lower prices, and prearranged terms and conditions.

Additionally, by forming or joining a consortium/partnership, institutions can share tools and staff, creating an even greater cost savings. By combining tools and resources, the institutions develop a strong, resilient security platform that, when combined with the inclusion of expertly trained subject-matter experts and staff, provides a broader range of services to a larger, more diverse population. The same can be said for contracting with an external vendor to perform vulnerability and penetration testing. The consortium provides a base with which to obtain lower pricing and more effective service and results.

Strategies for Staffing

Developing existing staff skills and transitioning those individuals into dedicated security roles can provide needed capacity to support an information security program. Hiring students to play a role in such programs can also help meet existing needs without significant new investments.

Transforming Current IT Staff into Security Professionals

Although officials at most institutions probably believe they lack the resources required to run a comprehensive IT security program, there may be ways to repurpose, retrain, or redirect existing staff and resources to address this critical area. Combining parts of positions that are even remotely security related into dedicated security positions can create a centralized security function that becomes the core of a security program. With the added focus and some additional training, institutions have found that using this approach enabled them to advance their security program quickly.

Institutions can use a number of approaches to augment their security team. Efforts to create such a team out of existing resources could include the following:

- Develop an existing IT director with a lot of institutional knowledge and some background in security into a CISO.

- Reassign a project manager/business analyst working largely on security- and identity-related projects to the security team.
- Reassign systems operations specialists performing triage and permissions work for the systems admin team to the security team; automate and streamline the triage process so that these staff can be more focused on security-related tasks and processes.
- Reassign a systems administrator who works on security-related systems such as Active Directory and the Microsoft Systems Center to the security team.
- Repurpose a vacant security systems administrator position focused on security tools into a higher-level security analyst position responsible for a broader range of security tasks including incident response, investigations, and deployment of new security initiatives.
- Repurpose a vacant systems analyst position that spent some time on identity into a dedicated identity management owner and assign identity to the newly formed security team; automate provisioning and de-provisioning to help offset some of the resources moved from other areas to create the security team.

Yavapai College used a similar approach to form the basis of its information security efforts. Included in this effort were the following steps:

- The college realigned functional area responsibilities. Formerly, the IT department was responsible for administration of the institutional website. After the realignment, the Office of Public Information (OPI) was formally tasked with this responsibility. One FTE was transferred from IT to OPI. Web Services (web application development and support) had previously been separate from Application Development (ERP and database support). After the changes, these two areas were merged into one.
- The Web Services Manager who had previously supported information security efforts in lieu of dedicated staff was then formally moved into the CISO role.
- After approximately 12 months, a new information security analyst position was approved to supplement the CISO role.
- A continuous review of responsibilities has resulted in moving systems and services such as SIEM, PII scanning and remediation, patching, and related efforts to the Information Security Team from other functional areas to better align capabilities and responsibilities.

Remember, lateral job movement within your organization is not a bad thing. It keeps long-time employees engaged and helps create a better understanding of different aspects of IT and information security. In a smaller college or university,

where the IT professionals wear many hats, rotating people into some form of security operations will pay off without breaking the bank.

Helping you and your staff develop and grow as professionals includes more than simply attending conferences or weeklong training classes. It also includes networking with peers at free and convenient events in your area. Many colleges have formally (sometimes informally) organized by geographic region and meet occasionally to talk about IT matters. Career fairs, tech expos, and other events that draw IT professionals are also a great (and inexpensive) way for you and your staff to network and learn.

Hiring Students

Students are a tremendous resource for the budget-conscious security program, and bringing them onboard can take a variety of forms, including internships, student employment, and experiential learning opportunities. Finding a student who is passionate about cybersecurity and has basic knowledge of operating systems and scripting is a big plus, but don't forget to look beyond the computer science and technology departments—cybersecurity has multidisciplinary dimensions, and any interested and enthusiastic student, no matter his or her major, can make contributions to your program.

If you have a cybersecurity program at your institution (or at a neighboring one), introduce yourself to the faculty. It could become a class project to perform a risk assessment of a department or to help implement an open-source tool. The faculty will also be able to recommend star students who would be perfect additions to your staff. You may even be able to lead a directed, independent project with a talented student—they get credit, and you get a task performed.

With limited resources, start small with just one student. Pick an area for the student to work on—perhaps phishing response or intrusion detection. Teach that student to use the tools you have and document the process as part of the training. The student can then train future students in the tasks you've chosen.

Tools and Resources

Open-source and community-generated services and applications increasingly offer viable options to commercial products whose cost may put them out of reach for some institutions.

Using Open-Source Tools

Almost every commercial security tool has an open-source alternative. While not every tool is as fully featured as its commercial counterpart, many offer the budget-conscious security program tools that would otherwise be unaffordable.

While taking advantage of low-cost alternatives may seem like a no-brainer, the important lesson is to play to your strengths. Open-source tools aren't free—you won't be paying licensing fees in perpetuity, but you still have associated expenses. For instance, do you have the staff to devote to learning the open-source solution? Are they properly trained? Perhaps outsourcing some or all of your security operations would play better to your strengths by freeing up staff time. With that caveat, numerous open-source tools are available for the budget conscious. Many of these tools may free up financial resources to invest in other areas as well.

Following is a list of popular open-source security tools:

- Snort: An intrusion detection system with strong community support; requires tuning to avoid information overload but works very well in smaller (1Gbs) networks.
- Suricata: An intrusion detection system similar in functionality to Snort but that works equally well in small and large networks.
- Bro: A complex but powerful network security monitoring tool and analysis framework; strong community support, widely used in higher education, scales extremely well, and is used in high capacity (100Gbs) networks. (See Overview of Bro for more information.)
- Security Onion: A suite of tools for the security analyst; combines several open-source tools (Snort, Suricata, Bro, OSSEC, Sguil, Squert, and others) into one convenient interface.
- Elastic Stack (formerly the ELK Stack): The open-source alternative to the popular tool Splunk; capable of ingesting data from any source (typically log data) for correlation and analysis; widely supported and highly scalable.
- OSSIM: The open-source engine behind AlienVault, the commercial and widely used SIEM; few SIEMS are open-source SIEMS, but there is quite a bit of development in this area. Recently, the SANS organization developed an open-source SIEM and is teaching a course based on its use.
- OpenVAS: An advanced open-source vulnerability assessment tool.
- Wireshark: A highly popular and widely used network protocol analyzer; long considered a staple tool in the information security community.

- Metasploit: Penetration testing/vulnerability assessment.
- Kali Linux: A distribution of Debian Linux that includes a penetration testing toolset.
- Forensics tools: The Sleuth Kit (Linux) and Autopsy (Windows). Mandiant RedLine (memory and file analysis of a host).
- Open-source incident response tools and monitoring (incident tracking, asset inventory, availability monitoring [Nagios], NetFlow Analyzers)
- PacketFence: Network access control
- TScanner: PII scanner

As with any new IT tool, be sure to learn how to properly implement and use open-source security tools before you deploy them in your production environments. Not all tools are ready for use out-of-the-box.

Using Community-Generated Resources

There is no shortage of higher education–created information security and privacy content. Take the time to familiarize yourself with free materials that are already available for you to use as-is or adopt for your program. The best source of such community-generated information security content is located in the Information Security Guide: Effective Practices and Solutions for Higher Education. This resource is aligned with common information security standards (like ISO/IEC 27002:2013 and NIST 800-53) and includes key objectives and implementation guidance to assist institutions with developing an effective information security program. What makes the Information Security Guide unique is that the resources and content included in its chapters are provided *by* higher education information security professionals *for* higher education information security professionals. Guide content is constantly being added and refreshed by volunteers with expertise in both information security and higher education. Guide resources that can be used *out of the box* include:

- HEISC Information Security Program Assessment Tool
- Information Security Policy Examples
- HECVAT
- Security Awareness Campaign materials

Conclusion

As the proverb reminds us, necessity is the mother of invention. By thinking carefully and strategically about the strengths of your organization, you can better match low-cost solutions to your needs. As institutions look to improve their security posture in lean or resource-constrained times, it makes sense to take advantage of the great networks that higher education institutions tend to create and be part of. By speaking with others in the community, you can recognize opportunities where sharing resources, repurposing your staff, and open-source solutions might make sense.

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.