Budget Conscious Strategies for Information Security

Capability Roadmap

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

When building an information security program, it's important to move with a purpose. Budget-challenged programs must often build from nothing, yet the stakeholders expect (at least in some form) to be able to justify security expenditures with an improved institutional security stance. Determining the elements of an effective security program that are also sustainable is often a difficult task as well. Much research has to be done to determine what sort of program to build and to develop enough evidence to justify the money and time spent to produce such a program. Of course, all aspects of a maturing information security program are important—and many are critical—but the differentiating factor between institutions may be the depth of implementation that the program undertakes. Accordingly, there can't be a one-size-fits-all approach; what works for one institution may not work for others. A budget-conscious information security practitioner must decide on a framework to determine what needs the institution has, what practices achieve the desired information security results, and what relationships exist to help build and run the program.

Choosing a Framework

In a discussion of frameworks, it's important to distinguish the framework used for identifying capabilities from other frameworks and methodologies. Many frameworks are area-specific, such as NIST's Cybersecurity Framework or the Department of Energy's Cybersecurity Capability Maturity Model (C2M2). The NIST framework is a federally developed, risk-based approach to managing cybersecurity risk on a controls level and is based on existing standards, guidelines, and practices for critical infrastructure organizations to better manage and reduce cybersecurity risk. The C2M2 is a public–private partnership effort (designed originally for the energy sector) that quantifies the overall maturity of a program and measures the program's health and sophistication.

EDUCAUSE has done extensive research on higher education information security capabilities and maturities. Those resources are purposefully aligned with other EDUCAUSE resources and guidance materials created by higher education information security professionals. The use of those resources is particularly appropriate for budget-conscious institutions that want to take advantage of high-quality yet complementary resources. For this reason, we use the 2016 EDUCAUSE report *Digital Capabilities in Higher Education, 2016: Information Security* as the basis for the framework we share in this paper. The report examines EDUCAUSE Core Data Service (CDS) information security maturity and deployment indices to provide a view into the current status of information security digital capabilities in higher education. These indices are straightforward and clear, and EDUCAUSE collects data on them each year, so users can not only employ them as a framework for their own programs but also use data collected by EDUCAUSE to compare their programs to the programs of their peers. This helps an institution provide validation of its efforts to institutional leadership as well.

Examining the questions asked in the CDS information security maturity and deployment indices, even well in advance of an assessment of information security program maturity, can provide the budget-conscious practitioner with a lot of ideas and directions for a growing program.

Information Security Practice Areas

We can determine many practice areas for the budget-conscious information security program, as they are typically found across a broad section of organizations, though often at differing deployment levels. The *Digital Capabilities in Higher Education, 2016: Information Security* paper identifies six categories (called *dimensions*) of information security practice:

- Security services and operations
- Asset protection
- Systems review
- Policies
- Business continuity
- Identity management

Each category is defined below and includes a list of the individual capability components which should be considered as part of a functional information security program.

Security services and operations is "the extent to which the institution manages information security across the institution, including management responsibility for information security activities and overall direction for information security activities." Capabilities in this category include the following:

- The CISO (chief information security officer, or the person who fulfills that role)
- Incident handling
- Security policy
- Awareness training
- Institutional collaboration (such as HEISC, REN-ISAC, or other ISACs that exist)
- External entity assessments (penetration tests, vulnerability assessments)
- Forensic collection
- Relationships with law enforcement (including campus security)

The CISO role is complex (and will be discussed further in a companion document), but of particular note is the responsibility to produce an information security plan (ISP). This is the development and tracking document that will provide the blueprint for the implementation of the program and its evolution. It is also a living document and will be amended as the program is built. The CISO will also facilitate the inception and implementation of a security governance committee. Ideally, this group will bring in stakeholders (or representatives) of each department of the institution, including faculty (if possible, and as early as possible).

Asset protection is "the extent to which the institution manages and protects data during the entire data life cycle." Capabilities in this section include the following:

- Creating standards for configuration, backup, testing, and restoration
- System patching and updating
- Access control (data, system, and physical)

This is the area where "breaches" happen (because data are most often the target). Developing these components should be a high priority at any institution.

Systems review refers to "the extent to which practices and processes are in place to protect institutional information systems." This is where much of the management occurs, in areas such as these:

- System logs
- Configuration
- Vulnerabilities
- Malware detection
- Internal reviews (such as audits and upon changes)

It is often easy for needed information to get lost in the flood. Careful review of the elements listed above by the information security practitioner can help prevent allowing the abundance of information available to eclipse the critical data needed to protect the organization.

The **policies** dimension includes "the extent to which the institution approaches formalized information security policies, standards, and procedures." These refer to the security rules and behaviors to which the users and organization adhere. Policies will be necessary in quite a few areas:

- Encryption
- Record lifecycle and management
- Sensitive data
- Mobile computing
- Data classification

As mentioned in the definition, procedures are usually aligned with policies and should be developed and documented as well. Although policies will usually differ between organizations, some are critical at any institution and several are driven by regulatory or industry compliance. It is up to the information security practitioner to work with institutional stakeholders to determine which should be prioritized. It is also not necessary to "reinvent the wheel" with information security policy—many institutions have published their policies, and direction can usually be taken from these.

In addition, HEISC has provided many "boilerplate" policies that can be used as-is or further developed, as the situation requires (see Information Security Policy Examples). Policies are important, and identifying which policies to work on and developing them earlier (rather than later) allows the activities the program undergoes to have a basis in "why," which is vital to the sustainability of the program.

Business continuity is “the extent to which the institution has prepared to ensure continued operation of critical business functions.” Capabilities components in this domain include the following:

- Creation of a business continuity plan
- Testing the business continuity plan

The business continuity dimension is one of the most visible parts of any information security program because it must necessarily interact with other departments in the institution. Notable in the definition is that not only are IT functions considered but so are the activities of the entire organization. A business continuity plan must be developed, and members of the team must be identified. It isn’t necessary that the team members be information security practitioners or even IT staff. Specific roles exist in the arena of continuity, however, and it’s impossible for one person (or even a too-small infosec department) to handle it without help. No clearer evidence of that will be seen than when the plan is tested, preferably annually. Testing is critical to the success of the plan and will show where weaknesses and failure points lie. When done well, testing will also raise awareness and support of your overall mission because it brings in many non-IT personnel to look at the plan and to review the process.

Identity management is “the extent to which there are practices and processes the institution follows to verify and authenticate the identity of users, processes, and devices prior to granting access to information systems.” Capability components include the following:

- Identity management policies
- Network access policies
- Risk assessment
- Multifactor authentication

Identity management services are often not directly provided by information security departments, yet awareness of the identity management lifecycle from start to finish is vital because so many information security controls depend on a user’s identity and the roles assigned to that user. In addition to identity management policy, issues such as assessing risk and evaluating multifactor authentication concepts fall here, as well overseeing the user lifecycle—from hire to offboarding—and managing ongoing accounts (alumni, corporate, etc.).

Next Steps

As you build your institutional capability roadmap using the above categories, you will want to clearly define each category for your institution. Understand your goal in each category, know which business or academic units may be stakeholders in that category, and determine the resources (time, money, and staff) that you can devote to each category. Some categories may be easier to consider as you get started.

You might be limited to focusing on only one area at a time, whether due to money, time, or available staff constraints. In many cases, the most critical area to focus on first is security services and operations. The elements of this category contain the groundwork for everything else your program will accomplish. Many of the subcategories will be critical for you to develop first. Your best bet for first focus is policy. Specifically, these are policies that deal with behaviors themselves (acceptable use, compliance-based policies around FERPA, HEOA, etc.). These will begin to drive the behaviors that lead to a security culture at your institution.

A good idea for your next focus would be the policy section itself. Beyond the policies mentioned above, other policies will begin to establish and flesh out the development of your program (e.g., encryption, vendor relationships, mobile device management). If one domain were a good candidate to defer, it would likely be business continuity—though this domain is important, at the early stages you will likely not have enough established process to work (especially as an advisor) with the many stakeholders across your institution.

As you continue to refine your capability roadmap, community tools can help. For instance, HEISC provides the Information Security Program Assessment Tool for use in determining a program's maturity. This is a tool for institutions to use on their own to assess program process. It contains a number of questions (more than the CDS information security maturity index) that you can use not only to assess institutional information security progress but also to identify additional capability components that you may want to consider in the future. The tool also includes a mapping to the CDS information security maturity index so you can see where they align.

Keep in mind that no one can build an information security capability alone. In fact, it cannot be overstated that building relationships is critical to the budget-challenged information security program. Unless your institution is large and very well-funded, and unless the institution directs funds your way, you will have staffing issues. There simply isn't enough time in the day for a small team—certainly not a solo ISO—to do all you need to do. As you work on your capability roadmap, you should also do the following:

- **Map out the territory:** Document physical assets and architectures, as well as the institution's data assets.
- **Get to know your institution's culture:** For example, how is policy developed and approved? Who provides reports to the board about information security?
- **Establish information security governance and policies:** This is also a program category discussed above.
- **Enlist security stewards:** Networking and operations teams, as well as the help desk, can be additional eyes and ears to help alert you to information security issues and concerns.
- **Make friends:** Form well-established and ongoing communications with the following groups (because you will need them if the institution experiences an information security crisis):
  - Human resources
  - Internal audit
  - General counsel
  - Risk management
  - Campus police/security
  - Public relations
  - Business services (administration and finance)
- **Secure ongoing funding:** Don't treat this as a one-time capital project.
- **Help secure future funding:** Create a strategic plan for your information security program (typically the ISP mentioned above). The strategic plan (which can also be tactical in nature) should include opportunities for improvements, short- and long-term goals, and budget/resource needs.
- **Wash, rinse, and repeat:** Information security is a process as well as a result. You will never be finished, but you can and should establish a known roadmap with key stakeholders and be able to demonstrate your progress over time.

For more information about this type of undertaking, see "Anatomy of a Sustainable Information Security Program."

Maturity Model Considerations

Many frameworks—including the ones that we recommend here—talk about program maturity. Although determining an institution's level of information security program maturity is both important and valuable, the early stage of development is generally too soon to expend much effort on determining maturity. Nevertheless, it is useful to look at some of the areas within these models that will eventually be examined for levels of maturity. Doing so can help glean from them particular aspects upon which to build. Many of the scales that maturity models use are as follows (moving from low to high maturity):

- Not achieved > Slightly achieved > Partially achieved > Fully achieved
- No deployment > Tracking > Planning/piloting/initial deployment > Deployed to parts of institution > Institution-wide deployment
- Initial deployment > Developing capability > Partially deployed > Enterprise use
- Absent > Initial > Developing > Established > Optimized

As stated, these are all valuable indices, but in determining institutional needs and subsequently mapping capabilities to those needs, institutions should bear in mind that the highest state of maturity is not always desired or needed. Depending on institutional culture and goals, a mid-level maturity might be acceptable in some areas but not in others. It is important to understand the items (in the language of the above scales) that are being examined and what an institution is achieving/deploying/establishing and hopefully optimizing.

Conclusion

Deciding where to spend limited time and money is not easy. In many cases, the budget-challenged infosec practitioner is a "team of one" and the burden of security falls squarely on that person's shoulders. That doesn't mean, however, that it's a lonely road; making alliances, recruiting your IT colleagues, and nurturing relationships across campus are all critical to any information security program.

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.