Security Program Development

Table of Contents

Getting Started

Information security or IT staff responsible for developing and maintaining an effective information security program can take advantage of information and resources in the HEISC *Information Security Guide* that can assist with key information security initiatives. Following are some additional recommendations:

1. **Adopt** a standardized (best practices) approach to developing your information security program. A wealth of guidance is provided in the below standards and frameworks:
    a. NIST Cybersecurity Framework
    b. NIST Special Publication 800-53 Revision 4
    c. ISO/IEC 27001:2013
    d. ISO/IEC 27002:2013
    e. COBIT 5
    f. 20 Critical Security Controls
2. **Incorporate** compliance requirements that may apply to your institution:
    a. FERPA (Family Educational Rights and Privacy Act)
    b. GLBA (Gramm-Leach-Bliley Act) Safeguards Rule
    c. HIPAA (Health Insurance Portability and Accountability Act)
    d. PCI-DSS (Payment Card Industry Data Security Standard)
    e. Additional resources include the Higher Education Compliance Alliance's Compliance Matrix and an article describing New Mexico State University's IT Compliance Framework for Higher Education.
3. **Review** the following HEISC resources for additional recommendations:
    a. Toolkit for New CISOs
    b. Mentoring Toolkit
    c. Mobile Internet Device Security Guidelines
    d. Developing Your Campus Information Security Website
    e. Top Information Security Concerns for Campus Executives & Data Stewards
    f. Top Information Security Concerns for HR Leaders & Process Participants
    g. Top Information Security Concerns for Researchers
    h. Many more resource are available under Hot Topics and Toolkits!
4. **Identify** the roles and responsibilities of staff with direct responsibility for information security. Use the standards and frameworks below as references.
    a. National Cybersecurity Workforce Framework
    b. National Initiative for Cybersecurity Careers and Initiatives (NICCS) Workforce Planning
5. **Use** the Information Security Program Assessment Tool to help you determine the maturity level of your institution's information security program. Identify opportunities for improvements and potential collaborations with key stakeholders.
6. **Review** the results of prior risk assessments and IT controls audits to help identify and prioritize areas that need the most attention.
7. **Develop** an information security plan that addresses:
    a. Gaps in coverage (information security controls, policies, and/or program initiatives that need to be developed)
    b. Compliance requirements
    c. How your information security program's initiatives align with IT and Institutional goals and objectives
8. **Engage** with other higher education information security professionals at the annual EDUCAUSE Security Professionals Conference
9. **Join** the EDUCAUSE Security Discussion List
10. **Consider** whether your institution may benefit from becoming a member of Research and Education Networking - Information Sharing and Analysis Center (REN-ISAC)

Top of page

Overview

Security Program Development can be thought of as having an emphasis on establishing information security related roles and responsibilities throughout an institution of higher education. Two major areas are addressed in this section:

1. Developing an effective Information Security Organization
2. Mobile Computing and Teleworking standards (and the "BYOD challenge")

Establishing an effective internal **Information Security Organization** can be further sub-divided into multiple topics of interest:

- One of the key sub-topics is information security roles and responsibilities, which addresses the need to designate and assign accountability for information security across the institution to ensure that institutional staff and faculty apply appropriate protection to assets and information under their direct control. Additionally, this topic addresses the need to establish an information security governance framework and designate a leader who will manage the information security program and develop program initiatives. This designation should be documented in a formal job description for the individual with the designated responsibility and such designation should be utilized in properly demonstrating compliance with applicable regulatory and compliance requirements such as HIPAA, GLBA, and PCI DSS. (HIPAA, for example, requires this designation in §164.308(a)(2).) Note that there are a variety of roles and responsibilities for campus information security leaders (read more in this article on the 7 Types of CISOs or visit the National Cybersecurity Workforce Framework).
- Avoiding conflicts of interest that can arise when segregation of duties is not considered. This is another area to be addressed to ensure that no single individual at an institution can escape detection if engaging in unauthorized activities or abusing access to information and technology systems.
- The information security organization is also responsible for appropriate contact with authorities and contact with special interest groups.
- Addressing information security in project management activities is important to ensure that risks are identified and addressed throughout the project management lifecycle.
- The information security organization is typically also responsible for developing information security policies and creating a comprehensive risk-based information security program. (These topics are covered more thoroughly in other chapters in the guide.)

Mobile Computing and Teleworking relates to the risks of working with mobile devices in unprotected environments.

Top of page

Internal Organization

Objective: Institutions of higher education need to establish a mechanism to manage information security across the entire enterprise and gain the support of institutional leadership to assist in providing overall direction.

Implementing a Security Strategy

Key Question: Do we have a regularly updated information security strategy that supports the mission and strategic objectives of our institution?

An effective information security strategy for a higher education institution must take into account the overall strategic objectives of the institutions and varied campus groups, including academic (research included), administrative (or business), clinical, and residential environments. Even when focusing on critical processes and legal mandates, it is necessary to extend protective measures beyond the underlying IT systems and associated administrative staff. For example, many faculty members have access to student records, and this access must be considered when assessing the security risks associated with these data. A failure to provide faculty with securely configured workstations increases the risk of sensitive data being exposed via their computers. This risk can also be reduced by implementing a middleware solution to properly control which records each faculty member can access and to minimize the amount of sensitive data stored on their computers. Also, to be effective, security practices cannot rely completely on technological solutions. Continuing the example, policies are required to clearly define faculty members' responsibilities relating to student data and the security of their workstations. Also, awareness programs aimed specifically at faculty members and their responsibilities to safeguard student information might be developed, possibly in conjunction with the institution's student information steward (e.g., at many institutions this is the Registrar).

To complicate matters, the operational needs of college and university networks often directly conflict with security practices such as perimeter firewalls, port authentication, centralized configuration management, and strong authentication. Higher education networks must therefore be designed to balance security and privacy requirements while accommodating a wide variety of end users and their needs – e.g., visitors, new students arriving with computers, researchers sharing large quantities of data with members of other academic institutions, remote access to a variety of network services for individuals who are traveling or telecommuting, and mobile users moving between classrooms, libraries, and indoor and outdoor study spots on campus. Although firewalls are becoming widely used to protect critical systems on university networks, their use at the perimeter is less common because it is difficult to reconcile their restrictiveness with the need for an open networking environment that supports research, learning, and high-speed networking. Although centralized management is feasible for certain hosts on a university network, this approach is not suitable for most student computers and many faculty, research, and clinical systems. In the end, security and privacy practices need to be integrated into operational practices in a way that makes the most sense for each campus.

This is not to say that higher education institutions cannot be secured; many colleges and universities are successfully balancing the need for security and an open, collaborative networking environment. Throughout this Information Security Guide readers will find general advice, as well as specific institutional examples, of successful approaches to managing information security within higher education.

Here's a reference to one approach to strategic planning, "The Shifting Landscape Strategic Security Model" (presented at the 2010 Security Professionals Conference, which might prove to be a useful aid).

Top of page

Information Security Governance

Key Question: Have we established governance structures and groups that foster awareness and shared ownership of information security issues and objectives?

Effective institutional governance of the information security function is critical to a successful program. It can be both the "proof of the pudding..." with regard to management commitment and provide necessary guidance when deciding where to allocate scarce resources. This well researched section draws from experts in the field and provides useful background and advice which can be adapted to a wide variety of campus cultures. The topical outline shown below reflects the broad array of subjects covered in this very deep **Information Security Governance** article. Additional resources are available on the EDUCAUSE IT Governance, Risk, and Compliance website or in the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) Toolkit.

- What is Information Security Governance and What it is Not
- Why Information Security Governance is Needed
- How to Govern Information Security
    - Organizational Structure
    - Roles and Responsibilities
    - Strategic Planning
    - Policy
    - Compliance
    - Risk Management
    - Measuring and Reporting Performance
- Governance Models and Success Stories

💡 Building ISO 27001 Certified Information Security Programs (University of Tampa, 2017)

This case study describes a decision and process used by the University of Tampa to go beyond compliance with ISO 27002 (essentially the controls portion of the ISO standard) and become certified under 27001 (ISO/IEC 27001:2013 Information technology -- Security techniques -- Specification for an Information Security Management System) which required complete commitment from top management.

Some additional resources and examples of higher education information security governance:

1. Information Security Council Charter (University at Albany - SUNY)
2. Information Security Advisory Council Charge (Appalachian State University)
3. Initiating Security Initiatives Through System-Wide IT Governance (University of Alaska, 2011 presentation)

Top of page

Managing the Information Security Program

Here are several useful references that provide insight into the process of managing information security within the higher education community. There are no magic bullets provided but each reference does develop some ideas that may prove useful.

Gaining the Confidence of Others

While information security offices generally have the authority to help establish policies and standards, transitioning these policies and standards into actual practice often involves extensive communication, relationship management, and development of influence. The resources below can also help provide some outside perspective.

- The Career of the IT Security Officer in Higher Education is an ECAR Research study of information security across a variety of institutions. Not only does it provide the reader with useful comparisons and statistics regarding the practice of information security in higher education but it also provides useful advice for the information security officer regarding positive interaction with others (i.e., leaders, peers, colleagues, staff, faculty, and students).
- A Guide to Security Metrics is a presentation made at the 2010 Security Professionals Conference. It provides a definition of security metrics, explains their value, discusses the difficulties in generating them, suggests a methodology for building a security metrics program, and reviews factors that affect its ongoing success. Numerous examples of security metrics will also be covered.
- Scale the Solution to the Problem is an *EDUCAUSE Quarterly* article describing an approach to both gaining the confidence of others within the institution and effectively leveraging other appropriate institutional resources in the pursuit of improved information security.
- Effective Management of Information Security and Privacy is an *EDUCAUSE Quarterly* article proposing (as it summarizes in its subtitle) security and privacy are not IT issues -- they demand a comprehensive, strategic, team approach to find effective solutions.
- Information Security and Internal Audit: Working Together is a presentation made at the 2011 Security Professionals Conference.
- Information Security and the Institutional Review Board: A Roadmap for Securing Research Data at Your Institution is a presentation made at the Security Professionals Conference, 2011

Getting Along with Less

Another common issue faced by campus information security offices is limited resources (in terms of funding, personnel, or both).

- Surviving the Onslaught: Running a Security Program by Yourself is a presentation made at the 2010 Security Professionals Conference which examines ways in which a security program can be successfully mounted with very limited resources.

Top of page

Information Security Program Self-Assessment Tool

The Information Security Program Self-Assessment Tool allows colleges and universities to evaluate the maturity of their campus security programs. This tool is intended for use by an institution as a whole, although a unit within an institution may also use it to help determine the maturity of its individual information security program. Unless otherwise noted, it should be completed by chief information officer, chief information security officer or equivalent, or a designee.

Top of page

Information Security Roles and Responsibilities

Key Question: Have we established well-defined roles and responsibilities at all levels of our institution to help support and address our information security strategy and objectives?

Information security is the responsibility of everyone at the institution. It is important to establish roles and responsibilities for campus staff, faculty, and students so that everyone knows what is expected of them when handling information. Leadership is also very important, and many institutions have at least one person who is primarily responsible for organizing the information security program. Typically this is a Chief Information Security Officer (CISO), Information Security Officer (ISO), Director of Information Security, although the title may vary depending on the campus. No matter what title is selected, there should be someone at the institution who can provide a high level of decision-making support to campus leadership when considering information security issues and solutions. Read more in the *EDUCAUSE Review* article, Evolution and Ascent of the CISO.

It is also important to establish data ownership and data handling roles (e.g., data owners, stewards, custodians, and users). Many institutions formally identify and document these roles within their information security policies and data management frameworks.

Top of page

Segregation of Duties

Key Question: Have we reviewed areas where procedures and tasks for critical data and systems can be segmented between multiple individuals and/or roles to lower the risk of insider threats?

Segregation of duties is the concept of having more than one person required to complete a task. This is a best practice, especially in cases where sensitive data is being handled. Segregation of duties is a control put in place by many institutions to mitigate the risk of an insider threat or accidental employee mistakes. Sometimes this isn't practical or possible, but the institution should be aware of the risks of a single person having too much access.

Ideally, critical processes or activities should be split up between multiple people. For example the initiation of a process, its execution, and authorization should be separated when possible.

When this is not possible, monitoring and auditing critical processes is very important.

Top of page

Contact with Authorities

Key Question: Have we identified and established a relationship and contacts with relevant agencies including law enforcement partners who may be called upon during emergencies?

Relationships with law enforcement are important to an institution, and should be established prior to an emergency. Having a protocol for engagement established before there is an emergency will help in handling an incident appropriately.

A protocol for engagement with law enforcement can be a part of the security incident response plan or a broader crisis management procedure for the campus. The plan should be clear about which situations require working with law enforcement, such as when laws are broken. The plan should also clearly state who contacts authorities and under what circumstances (e.g., when law enforcement should be contacted by the information security office or campus safety).

Law Enforcement Resources and Contacts

- **InfraGard** is a partnership between the FBI and the private sector, and provides sharing of information and intelligence to prevent hostile acts against the United States, including cyber threats.
- **FBI Regional Field Offices** are another resource if you need contact information for local law enforcement.

Note: It is also important to establish relationships with key campus partners prior to an emergency - e.g., internal audit, human resources, and legal counsel.

Top of page

Contact with Special Interest Groups

Key Question: Have we engaged with groups within our community of practice to share and receive ideas and information?

There are many groups that support Information Security that an institution can collaborate and participate in. The information security threat landscape is ever changing and security professionals can benefit from collaborating together. Being connected to special interest groups allows for knowledge transfer and best practice development. Warnings about potential threats can also help security operations prepare and respond appropriately. Some organizations include:

- EDUCAUSE Security Discussion List: The Higher Education Information Security Council (HEISC) is a key organization for collaborating with other security professionals in the higher education space, and oversees this open discussion group.
- REN-ISAC: This organization allows private information sharing within a community of trusted representatives at member organizations in the research and education communities.
- ISSA: An international community of cybersecurity professionals.
- ISACA: An association that engages in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. The organization currently reflects a broad range of IT governance professionals.
- US-CERT: A United States Government organization sharing information about cybersecurity threats to a broad audience of government, business, and citizens.
- SANS Internet Storm Center (ISC): Provides a free analysis and warning service to Internet users and organizations.

Top of page

Information Security in Project Management

Key Question: Do we have a formal IT project management discipline and does it include integration with relevant information security roles for risk assessment?

Information Security should be a part of the project management lifecycle in any institution. From project concept to completion, information security should be consulted so that information assets are properly protected. Often information security is an afterthought or not included in the project process. This approach can dramatically increase project costs and expose the institution to unnecessary risk.

Practical Project Management For Security Implementation in Enterprise Systems

Top of page

Mobile Computing and Teleworking

Objective: To cover the appropriate safeguards that an institution can implement to prevent the unauthorized access to institutional information resources while using mobile computing and teleworking facilities.

Teleworking (i.e., telecommuting), e-commerce, use of intranets, online education, and the increase use of portable computing devices (e.g., laptops, tablets, smartphones) are driving the need for access to information resources from any place at any time. Today's mobile workforce or users are no longer just staff faculty, and students trying to check e-mail from home but part and full-time telecommuters, business partners, full-time students. and patients who rely on access to institutional networks to accomplish day-to-day business functions, attend classes, and follow-up on medical treatments. Information security controls specifically targeting mobile computing and remote access to information resources are becoming an increasingly critical component of any institution information security program ensuring the protection of the integrity of the institutional networks while allowing remote access to it.

Challenges of Mobile Computing:

- User Authentication
- Protection of Transmitted Data
- Protection of the Institutional Network

To enable remote access to institutional information resources, institutions of higher education are implementing Virtual Private Networks (VPN) technology to provide a secure connection to the institutional network. VPNs send data securely through a shared network. VPNs can be established between remote users and a network or between two or more networks thus using the Internet as the medium for transmitting information securely over and between networks via a process called tunneling.

The EDUCAUSE Mobile Internet Device Security Guidelines page contains helpful advice to develop mobile Internet device security policy, standards, guidelines and procedures. It is organized into easy to follow steps to define objectives, develop a plan, and answer some of the questions being asked by users and security professionals alike.

Top of page

Resources

Campus Case Studies On This Page
Building ISO 27001 Certified Information Security Programs (University of Tampa, 2017)

EDUCAUSE Resources

- 7 Things You Should Know About Cloud Security, EDUCAUSE 7 Things You Should Know, 2010
- A Guide to Security Metrics, Presentation at the Security Professionals Conference, 2010
- Building Security into the RFP Process, Presentation at the Security Professionals Conference, 2010
- The Career of the IT Security Officer in Higher Education, ECAR Occasional Paper, 2009
- Cloud Computing: Clear Skies or Rain?, Presentation at the Security Professionals Conference, 2010
- Data Protection Contractual Language, Information Security Guide
- Do They Measure up? Assessing the Security Posture of Third-Party Service Providers, Presentation at the Security Professionals Conference, 2011
- Effective Management of Information Security and Privacy, EDUCAUSE Quarterly, Volume 29, #1, 2006
- Higher Education Information Security Governance Guide, Presentation at the Security Professionals Conference, 2010
- Hot Topic Discussion: Mobility, Telecommuting, and the Cloud. Presentation and discussion at the Security Professionals Conference, 2010

- Guidelines for Responding to Compulsory Legal Requests for Information, Information Security Guide
- Information Security and Internal Audit: Working Together, Security Professionals Conference, 2011
- Information Security and the Institutional Review Board: A Roadmap for Securing Research Data, Security Professionals Conference, 2011
- Information Security Governance, Information Security Guide
- Information Security Governance Assessment Tool, Information Security Guide
- Initiating Security Initiatives Through System-Wide IT Governance, Security Professionals Conference, 2011
- Information Security Program Self-Assessment Tool, EDUCAUSE Resource, 2013
- Information Security Governance: Standardizing the Practice of Information Security, ECAR Research Bulletin, 2008
- Process and Politics: IT Governance in Higher Education, ECAR Research Study, 2008
- Scale the Solution to the Problem, EDUCAUSE Quarterly, Volume 27, #1, 2004
- Security Considerations for Cloud Computing, Information Security Guide
- Stewards for Higher Education: Looking at Clouds & the Top-Ten Issues, EDUCAUSE Review, Volume 45, #3, 2010
- Structuring the IT Organization for Cloud Services, ECAR Research Bulletin 12, 2010 (*login required*)
- Surviving the Onslaught: Running a Security Program by Yourself, Presentation at the Security Professionals Conference, 2010
- The Shifting Landscape Strategic Security Model, Presentation at the Security Professionals Conference, 2010
- Top Information Security Concerns for Campus Executives & Data Stewards, Information Security Guide

Initiatives, Collaborations, & Other Resources

- Governing for Enterprise Security (GES) Implementation Guide, CMU/SEI Technical Note, 2007
- Information Security Advisory Council Charter, Appalachian State University, 2015
- Information Security Council Charter, University at Albany - SUNY, 2011
- Information Security Governance: A Call to Action, Corporate Governance Task Force Report, 2007
- IT Confidentiality Statement, University of Iowa, 2002

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 6**: Organization of Information Security **ISO 27001:2013** **ISO/IEC 27003:2010** **ISO/IEC 27004:2009** **ISO 27014:2013**	**800-100**: Information Security Handbook: A Guide for Managers **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO01.02** **APO01.06** **APO07.02** **APO07.03** **APO10.04** **APO10.05** **APO13.01** **APO13.12** **DSS01.04** **DSS05.01** **DSS05.03** **DSS06.03**	**Req 3** **Req 4** **Req 6** **Req 8**	**ID.AM-6** **ID.GV-2** **ID.RA-2** **PR.AC-3** **PR.AC-4** **PR.AT-2** **PR.AT-3** **PR.AT-4** **PR.AT-5** **PR.DS-5** **PR.IP-2** **DE.DP-1**	**45 CFR 164.308(a)(2)** **45 CFR 164.308(b)(1)** **45 CFR 164.314(a)(1)**

Top of page

Questions or comments? Contact us.