Career and Workforce Development

Table of Contents

✓ **Getting Started**

Career development is all about *you*: Enhancing the skills that you rely on as an information security professional and inspiring you to be more proactive in your career development. These resources will help you explore the next steps as a security professional, whether it's transitioning into a management or CISO role, or broadening your perspective to take on challenges outside information security. Regardless of your career level, the size of your organization, or the financial and time constraints you face, there are numerous opportunities that will help you improve your skills and establish a career path to support the institutional mission.

Workforce development is all about *others*: As a leader, you understand the cybersecurity workforce is at the forefront of protecting data, infrastructure, and networks. Organizations must be strategic in their human resource strategies in order to hire and retain the right information security professional to protect their assets. These resources will help you explore understanding workforce needs and skills gap; hiring the right people for clearly defined roles; enhancing employee skills once they enter your organization; and creating an environment and implementing programs that retain top talent.

Understand how to advance your information security career or strengthen the careers of the individuals in your information security program with these popular HEISC resources.

- View the Advance Your InfoSec Career toolkit to ensure that you are staying connected in your field.
- View the Training and Certifications toolkit to ensure that you are staying current in your field.
- Grow your team by reviewing sample job description templates for common information security positions such as CISOs, Awareness and Training Coordinators, Security Engineers, and Forensic Analysts.
- Learn about the skills needed to be an information security leader.

Top of page

Overview

Professional and career development activities are critical for today's information security practitioner and higher education information security programs. Our field changes quickly and maintaining an up-to-date skills set is critical to protecting the data, technologies, and systems entrusted to us.

Professional development has benefits for both the institution and underlying individual. For the institution, professional development opportunities give individuals the skills that they need to accomplish the purposes for which they were hired. When individuals are properly trained and able to do their jobs efficiently, institutions benefit. Institutions also benefit when employees are satisfied with their careers and employee turnover is reduced.

Individuals also benefit from professional development. Ongoing professional development ensures that one continues to be competent in his or her chosen profession--especially over time and in an area like information security where rapid change is the name of the game. Professional development opportunities also directly benefit the underlying individual by enhancing his or her career skillset. While that skillset is useful for success in a current job, it is crucial when searching for a new position (either within higher education or in another industry).

Top of page

Information Security Program Resources

Since 2012, hiring and retaining members of the IT workforce has consistently been in the top half of the EDUCAUSE Top 10 IT Issues list. Retention issues are especially important in higher education, where information security skillsets continue to be in short supply in higher education (see The Higher Education IT Workforce Landscape, 2016). Security-based organizations such as ISACA and the Center for Cyber Safety and Education, formerly the ISC (2) Foundation, report similar shortages of cybersecurity professionals across all industries. These shortages mean that, across all industries, most organizations take three to six months to fill open security positions (ISACA, 2016 State of Cybersecurity Report). This means that hiring professionals with the information security skills needed to do a job and then retaining them is of critical importance.

Learn more about IT workforce issues generally and view resources to prepare job descriptions for some common information security program roles:

- CISO Job Description Template
- Toolkit for New CISOs
- The Higher Education IT Workforce Landscape, 2016 (ECAR research report)
- GRC Analyst/Manager Job Description Template (draft)
- Security Awareness Coordinator Job Description Template (*draft*)
- Information Security Intern (*draft*)
- Other job descriptions - Security Engineer, Forensic Analyst, and CPO (*in development, winter 2017*)

List of potential online locations to post IT or information security job openings:

- ASIS International
- CareerBuilder
- The Chronicle of Higher Education (Vitae)
- Dice
- EDUCAUSE Career Center
- HigherEdJobs
- Inside Higher Ed
- ISACA
- (ISC)2 - *for members only*
- ISSA
- Tech Ladies

Top of page

Personal Information Security Professional Development

Recent EDUCAUSE research shows that higher education CIOs and managers agree that expanded professional development opportunities are important to maintaining today's IT workforce. This same research shows that higher education IT staff members think that taking formal technical training classes and attending conferences focused on higher education IT contribute most to their professional growth and development. (See The Higher Education IT Workforce Landscape, 2016.)

Learn more about conferences, training and certifications, and other professional development activities intended for all information security professionals:

- Advance Your InfoSec Career
- Successful Security Awareness Professional Resource List
- Training and Certifications
- Toolkit for New CISOs

Top of page

Ethics for Information Security Professionals

Information security professionals generally follow a standard of conduct or code of ethics established by one or more certifying organizations. Some institutional IT departments may also have a publicly posted policy describing a code of conduct or ethics (e.g., Harvard University). The Ethics Working Group also provides a framework of ethical principles for security professionals that can be adopted by information security organizations. And the Center for Internet Security also provides some considerations when determining responsible behavior.

Learn more about some of the professional codes of ethics that are tied to specific information security certifications:

- (ISC)2 Code of Ethics
- ISACA Code of Professional Ethics
- GIAC Code of Ethics
- SANS IT Code of Ethics
- ISSA Code of Ethics
- ASIS Code of Ethics

In addition to professional obligations for those in the information security field, there can also be legal obligations, organizational policies, and personal values to consider when following standards of conduct or codes of ethics.

Note: If an ethical issue arises on campus, it may be appropriate to consult with the HR department or legal counsel team about appropriate actions or next steps.

Recommended Reading: Ethics and the IT Professional by Melissa Woo

Top of page

Information Security Leadership and Research

Information security is "now acknowledged as a field in which 'perfection isn't nearly good enough.'" (see 2016 EDUCAUSE Top 10 IT Issues). This means that leadership roles within information security are not for the faint-of-heart. Information security leaders, regardless of title, are expected communicate effectively, engage in strategic thinking and planning, and manage increasingly complex projects and relationships. To accomplish this, an information security leader must adeptly navigate the landscape between IT groups and other campus business and academic leaders.

Explore information security leadership issues:

- Technology in Higher Ed: InfoSec Leadership
- Collaborating with Faculty
- Collaborating with Staff
- Mentoring Toolkit
- CIO Minute: CIO and CISO (video)

Top of page

Resources

HEISC Toolkits/Guides

- Advance Your InfoSec Career
- CISO Job Description Template
- Collaborating with Faculty
- Collaborating with Staff
- Mentoring Toolkit
- Toolkit for New CISOs
- Training and Certifications

EDUCAUSE Resources

- Technology in Higher Ed: InfoSec Leadership
- The Higher Education IT Workforce Landscape, 2016
- Retaining the Higher Education IT Workforce
- Continuing Education for Information Professionals

Initiatives, Collaborations, & Other Resources

- National Cybersecurity Workforce Framework
- National Initiative for Cybersecurity Education (NICE)

Top of page

? Questions or comments? ℹ Contact us.