Toolkit for New CISOs

This is a list of resources intended for Chief Information Security Officers (CISOs) and other security professionals new to their role in higher education. Recommendations are provided by members of the Higher Education Information Security Council (HEISC).

> ✓ **Are You the New CISO on Your Campus? A Few First Steps...**
>
> - Get to know your colleagues within the IT department, as well as key stakeholders across the institution.
> - Do a quick assessment within the first 60 days to determine the status of the IT security department's existing services and activities.
> - Find answers to questions in the *Information Security Guide: Effective Practices and Solutions for Higher Education*, a resource created *by* practitioners *for* practitioners featuring toolkits, case studies, effective practices, and recommendations to help jump-start your campus information security initiative.
> - Connect with local peers. The EDUCAUSE Member Directory allows you to identify peers according to functional role (e.g., CISO), area of interest (e.g., Cybersecurity), or location. Complete your member profile now and start connecting with professionals in your area!
> - Request a peer mentor or coach through our Mentoring Program for security professionals (visit our **Mentoring Toolkit** for details).
> - Listen to this 45-minute presentation from the 2017 RSA Conference, "Up for a Challenge? Learn How to Become a Successful Higher Education CISO."
> - View this 1-hour webinar, "Who Moved My Office? The Evolving Role of the CISO."
> - Read "A Tale of 3 CISOs," which provides highlights from a panel discussion with three prominent campus CISOs.
> - Review sample job descriptions for CISOs.
> - Browse the resources available below.
>
> *Still haven't found what you need? Please contact us and we'll try to help!*

EDUCAUSE Listservs: *Join any of these community discussion groups and engage with a large network of professionals.*

- Security Discussion List
- IAM Discussion List
- Policy Discussion List
- IT Communications Discussion List
- CIO Discussion List
- Interested in Cloud Computing, Data Administration, IT Accessibility, IT Architecture, IT Support Services, Mobile Technologies, or Small Colleges? EDUCAUSE hosts other discussion lists, as well.

Note: If you prefer not to subscribe to these listservs, please keep in mind that the listserv archives are fully searchable and may provide valuable insights and prior discussions relating to current (or future) issues and concerns.

Association & Industry Listservs

- IAPP (International Association of Privacy Professionals) Privacy List (*separate membership fee required*)
- REN-ISAC (*requires vetting and separate membership fee*)
- BugTraq
- PatchManagement.org
- RESNET-L
- US-CERT Mailing Lists and Feeds

Articles, Books, Magazines, & Newsletters: *Recommended reading.*

Articles

- "Information Security: Risky Business" (*EDUCAUSE Review*, January 2017)
- "The 2016 Top 3 Strategic Information Security Issues" (*EDUCAUSE Review*, January 2016)
- "Evolution and Ascent of the CISO" (*EDUCAUSE Review*, December 2014)
- "R.E.S.P.E.C.T.: The Way for CISOs to Get and Keep It" by Taylor Armerding (CSO Online, March 2015)
- "A New CISO's To-Do List: 'Make or Break' Actions for a Chief Information Security Officer's First Year" by Brian T. Nichols (Campus Technology, August 2006)
- "Keeping the Guard Up in a Down Economy: Investing in IT Security in Hard Times" by Brian D. Voss and Peter M. Siegel (EDUCAUSE Review, September/October 2009)

Books & Publications

- 2015 Strategic Information Security Issues Infographic (April 2015)
- *The Career of the IT Security Officer in Higher Education* (an ECAR Occasional Paper) by Marilu Goodyear, Gail Salaway, Mark Nelson, Rodney Petersen, and Shannon Portillo
- *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI* by Debra S. Herrmann
- *Computer and Network Security in Higher Education* edited by Mark Luker and Rodney Petersen
- *Cultivating Careers: Professional Development for Campus IT* edited by Cynthia Golden
- ECAR Research Publications
- *FERPA Guide* and *FERPA Quick Guide* by LeRoy Rooker (AACRAO)
- *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* by Peter Weill and Jeanne Ross
- *NIST Special Publications* (800 series)
- *Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith

- Note: Visit our Recommended Reading board on Pinterest for additional ideas.

Magazines & News Sources

- *EDUCAUSE Review*
- Computerworld Security News
- CSO (Chief Security Officer) Online Magazine
- EDUCAUSE Library
- IEEE Security & Privacy Magazine
- Information Security Magazine
- Network World Fusion
- SANS Internet Storm Center
- SC Magazine
- Security Magazine
- The Chronicle of Higher Education
- Inside Higher Ed
- Harvard Business Review
- Wall Street Journal

Newsletters

- Bruce Schneier's Crypto-Gram Newsletter
- CSO Online Newsletters
- IAPP Privacy News – The Daily Dashboard
- Microsoft Security Newsletter
- SANS Security Newsletters (NewsBites, @RISK, Ouch!)

Websites: *Visit these sites for recommended resources and links to other websites commonly used by CISOs in higher education.*

- Campus Computing Project
- Center for Internet Security (CIS): Critical Security Controls
  - Note: See how Virginia Tech is implementing the 20 critical controls as part of its overall security strategy in Randy Marchany's 2013 presentation, "The 20 Critical Controls: A Campus Security Strategy."
- EDUCAUSE Core Data Service (CDS)
- EDUCAUSE Cybersecurity Program & HEISC
- EDUCAUSE IAM (Identity and Access Management)
- EDUCAUSE Policy
- InCommon
- Internet2 Middleware
- Internet2 Security

Professional Development: *Face-to-Face & Online Events.*

- Security Professionals Conference
- Seminar on Establishing an Information Security Program (*typically offered on an annual basis at the* Security Professionals Conference)
- Additional EDUCAUSE career and professional development initiatives, including institute programs for management and leadership development
- Career Development for New and Aspiring CIOs (EDUCAUSE website)
- Internet2 offers a global summit, a technology exchange conference, and a variety of technical workshops.
- InCommon offers three different types of events for those who want to learn more about IAM-related issues: CAMP (Campus Architecture and Middleware Planning), Advance CAMP, and Day CAMP.
- EDUCAUSE Live! webinars (*free*)
- IAM Online webinars (*free*)
- EDUCAUSE Professional Development Commons blog series

Professional Organizations: *Consider joining a professional organization. Many offer local chapters with frequent meetings that allow you to build a local network of security practitioners and experts.*

- InfraGard
- ISACA
- (ISC)2
- ISSA (*separate membership fee required*)
- ISSA CISO Executive Forum (*separate membership fee required*)

Training & Certifications

- SANS Information Security Training
- Training and Certifications for Security and Privacy Professionals (CISSP, CERT, CIPP, CIPM, CIPT, CISA, CISM, CompTIA, GIAC, etc.)

Social Media: *Stay informed by connecting with others via Twitter, Facebook, YouTube, or LinkedIn.*

- EDUCAUSE Twitter page
- HEISC Pinterest page
- HEISC Twitter page
- HEISC YouTube channel
- Internet2 Twitter page
- InCommon Facebook page

- Internet2 Facebook page
- REN-ISAC Twitter page
- LinkedIn (search for Groups like EDUCAUSE, Internet2, REN-ISAC, Higher Education Information Security, and Information Security Community)

Connecting with Campus Colleagues: *It's crucial to continue developing relationships with as many people on your campus as possible.*

- CIO
- CPO
- Risk
- Audit
- Compliance
- CFO
- Registrar
- HR
- Faculty/Researchers
- Students

Security Organizations and Associations

- Association for Computing Machinery (ACM)
- Center for Education and Research in Information Assurance and Security (CERIAS)
- Center for Internet Security (CIS)
- CERT Coordination Center (CERT/CC)
- CIO Council
- Colloquium for Information Systems Security Education (CISSE)
- Computing Technology Industry Association (CompTIA)
- InCommon
- Indiana University Center for Applied Cybersecurity Research (CACR)
- Information Systems Audit and Control Association (ISACA)
- Information Systems Security Association (ISSA)
- InfraGard
- Institute for Information Infrastructure Protection (I3P)
- Internet Security Alliance
- Markle Foundation Task Force on National Security in the Information Age
- National Council of ISACs
- National Cyber Security Alliance (NCSA)
- National Information Assurance Training and Education Center (NIATEC)
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
- National Security Agency (NSA)
- REN-ISAC (Research and Education Networking Information Sharing and Analysis Center)
- SANS Institute
- Universities and Colleges Information Systems Association (UCISA)
- U.S. Department of Defense Cyber Security & Information Systems Information Analysis Center (CSIAC)
- U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS)
- Virginia Alliance for Secure Computing and Networking

Questions or comments? Contact us.