The 2016 Top 3 Strategic Information Security Issues
Joanna Lyn Grama and Valerie Vogel

Information security is a perennial favorite on the EDUCAUSE annual Top 10 IT Issues lists, appearing 13 times since 2000. In 2016, information security returns to the top ranking (a spot it previously occupied in 2008). To help us better understand the nuance of information security issues in higher education, members of the Higher Education Information Security Council (HEISC)—including Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT directors and managers, and IT staff members—drilled down into the topic of information security and identified their top 3 strategic information security issues: (1) Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training; (2) Developing an effective information security strategy that responds to institutional organization and culture and that elevates information security concerns to institutional leadership; and (3): Planning for and implementing next-generation security technologies to respond to evolving threats.

#1: Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training
This issue was #2 on the 2015 list. There was great agreement this year that education and training is the most critical information security issue facing higher education. It was the top issue identified by all respondent roles—CIOs, CISOs, and IT directors, managers, and staff (see figure 1)—and was also the top issue at Associate, Masters, and Doctoral institutions (see figure 2).

Institutions continue to make headway providing information security awareness and training opportunities for students, faculty, and staff. In 2014, information security training was mandatory for faculty or staff at 71 percent of institutions and for students at 29 percent of institutions. Since its inception in 2004, many institutions have also promoted National Cyber Security Awareness Month each October with campus activities, events, and targeted campaigns. To help institutions do an even better job with security awareness in 2016, the HEISC Awareness and Training working group has prepared ready-made content that security professionals and IT communicators can integrate into campus information security education communications (http://www.educause.edu/securityawareness).

#2: Developing an effective information security strategy that responds to institutional organization and culture and that elevates information security concerns to institutional leadership
This issue was #1 on the 2015 list. This year it features prominently in the top 3 issues for all institutional Carnegie classifications (see figure 2). Information security strategies outline the high-level priorities and goals of an information security program. These strategies demonstrate how information security relates to an

![FIGURE 1. Top 10 Strategic Information Security Issues, by Responder Role](image-url)
institution’s overall mission and how information security helps support the institutional mission and core values. “An information security strategy provides focus and direction for the institution,” said Melissa Woo, CIO and Vice Provost for Information Services at the University of Oregon and HEISC co-chair. “It provides the campus a means for prioritizing resources and investments in information security.”

#3: Planning for and implementing next-generation security technologies to respond to evolving threats

Although this issue did not appear in the top 3 issues in 2015, it seems fitting that a technology-focused issue would round out the list this year. With increasing concerns about cloud security, the Internet of Things, and other emerging, more sophisticated threats—as well as the ongoing challenge of limited campus resources (both financial and human)—finding new tools and technologies to help identify and mitigate threats more efficiently will continue to be of utmost importance to security and IT professionals. “Planning for next-generation security technologies must be done in concert with other technology enhancements and replacements,” said Cathy Bates, Associate Vice Chancellor and CIO at Appalachian State University and HEISC co-chair. “This planning ensures that security technologies are an integrated component of IT architecture and infrastructure roadmaps and are represented in the overall budget needs for a secure and stable infrastructure.”

Information security is of paramount importance to all colleges and universities, and with our connected world, this won’t change anytime soon. We encourage institutions to continue the tradition of openly collaborating and sharing ideas to help move our community forward in the information security space.

### Notes

1. HEISC supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. The HEISC Information Security Guide, created by practitioners for practitioners, features toolkits, case studies, effective practices, and recommendations to help jumpstart campus information security initiatives. For more information, see the EDUCAUSE Cybersecurity Initiative: [http://www.educause.edu/security](http://www.educause.edu/security).


© 2016 Joanna Lyn Grama and Valerie Vogel. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License ([http://creativecommons.org/licenses/by-nc-nd/4.0/](http://creativecommons.org/licenses/by-nc-nd/4.0/)).

---

<table>
<thead>
<tr>
<th>RANK</th>
<th>AA (n=9)</th>
<th>BA (n=10)</th>
<th>MA (n=19)</th>
<th>DR (n=52)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training. (66.7%)</td>
<td>Developing an effective information security strategy that responds to institutional organization and culture, and that elevates information security concerns to institutional leadership. (70.0%)</td>
<td>Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training. (87.5%)</td>
<td>Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training. (42.3%)</td>
</tr>
<tr>
<td>2</td>
<td>Developing an effective information security strategy that responds to institutional organization and culture, and that elevates information security concerns to institutional leadership. (66.7%)</td>
<td>(one additional issue tied for first place omitted from graphic)</td>
<td>(second place issue omitted from graphic)</td>
<td>Planning for and implementing next generation security technologies to respond to evolving threats. (42.3%)</td>
</tr>
<tr>
<td>3</td>
<td>Planning for and implementing next generation security technologies to respond to evolving threats. (33.3%)</td>
<td>(third place issue omitted from graphic)</td>
<td>Developing an effective information security strategy that responds to institutional organization and culture, and that elevates information security concerns to institutional leadership. (42.1%)</td>
<td>Developing an effective information security strategy that responds to institutional organization and culture, and that elevates information security concerns to institutional leadership. (34.6%)</td>
</tr>
</tbody>
</table>

Figure 2. Top 10 Strategic Information Security Issues, by Institutional Carnegie Class