INFORMATION SECURITY

What are the top strategic information security issues?

EDUCAUSE RESEARCH SNAPSHOT

Sustain and Improve Your Information Security Program

The Higher Education Information Security Council (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 jump-start campus information security initiatives. Don’t reinvent the wheel — get the Guide at www.educause.edu/security

Developing an effective information security strategy that responds to institutional organization and culture and elevates information security concerns to institutional leadership.

Ensuring that members of the institutional community (students, faculty, and staff) receive information security education and training.

Developing security policies for mobile, cloud, and digital resources (includes issues of data handling/ protection, access control, and end-user awareness).

Using risk-management methodologies to identify and address information security priorities.

Developing, testing, and refining incident response capabilities to respond to information systems/data breaches.

TOP 5 strategic information security issues for 2015

1. Developing an Effective Information Security Strategy

2. Ensuring that Members of the Institutional Community Receive Information Security Education and Training

3. Developing Security Policies for Mobile, Cloud, and Digital Resources

4. Using Risk-Management Methodologies to Identify and Address Information Security Priorities

5. Developing, Testing, and Refining Incident Response Capabilities to Respond to Information Systems/Data Breaches

Organizational capacity to provide information security

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All U.S.</td>
<td>2.9</td>
<td>2.5</td>
<td>3.1</td>
<td>2.6</td>
<td>3.0</td>
</tr>
</tbody>
</table>

2% of the IT budget at U.S. institutions is spent on information security.

ENSURING THAT MEMBERS OF THE INSTITUTIONAL COMMUNITY RECEIVE INFORMATION SECURITY EDUCATION AND TRAINING

From 2005 to 2013, unintentional human error (e.g., posting sensitive information on a website or other data mishandling) and insider threats (e.g., intentional breach of information by someone with legitimate access) accounted for 33% of data breaches in higher education, as reported in the Privacy Rights Clearinghouse.

For students

29%

For faculty

71%

DEVELOPING SECURITY POLICIES FOR MOBILE, CLOUD, AND DIGITAL RESOURCES

Institutions with these IT policies in place

AUP

ID management

Web access

Infosec

96%

65%

45%

27%

Using Risk-Management Methodologies to Identify and Address Information Security Priorities

Colleges and universities have central IT information security FTEs per 1,000 institutional FTEs.

0.1

Organizational unit responsible for incident management:

Central IT 80%

Shared 18%

System 1%

Not applicable 1%

Sustain and Improve Your Information Security Program

To further Education Information Security Council (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 jump-start campus information security initiatives. Don’t reinvent the wheel — get the Guide at www.educause.edu/security

Organizational capacity to deliver information security is measured in five areas: organization, policy, data security and management processes, access control processes, and information system security processes. Organizations with lower scores have less mature, ad-hoc programs; organizations with higher scores have optimized programs that regularly measure performance and manage risk.