Key Questions for Information Security:
Institutional Implications for Safeguarding Data

Data breaches and other information security incidents may be one of the biggest risks facing colleges and universities. Information security encompasses the technologies, policies and procedures, and education and awareness activities that maintain the balance between an institution's need to use data and IT resources to achieve its mission (openness) and the need to secure those data and resources from external and internal threats (risk control).

Is safeguarding information security a priority for your institution?

CIOs view information security and related issues (data privacy, regulatory compliance) as the most important IT risks in higher education (figure 1). Yet only 3% of central IT budgets and staff in higher education are devoted to information security and related identity management activities, compared to 5% in sectors other than higher education. Higher education spends 60% less per institutional employee on information security than is typical among all U.S. industries. Institutional attention to information security may be increasing. Although only about one in three (32%) colleges and universities had a full-time information security lead in 2013, this represented an increase from 27% in 2012. Smaller institutions view themselves as less effective at addressing information security and are less likely to have a full-time information security lead than larger institutions.

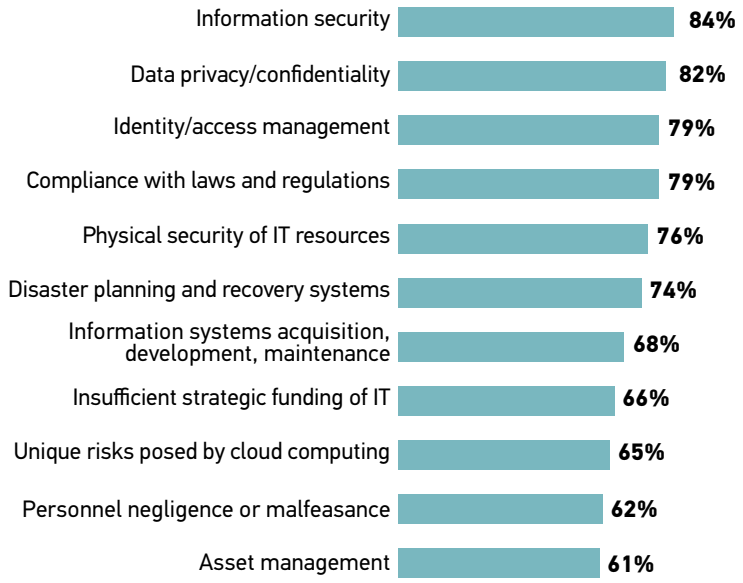

Figure 1. CIO rankings of IT risks in higher education

EDUCAUSE

Which information security practices do you have in place?

Information security relies on numerous practices to protect the network, servers, end-user devices, and data. Deployment of these practices is unique to each institution. According to the EDUCAUSE Core Data Service, various core technologies and information security practices are in place at colleges and universities (figure 2).

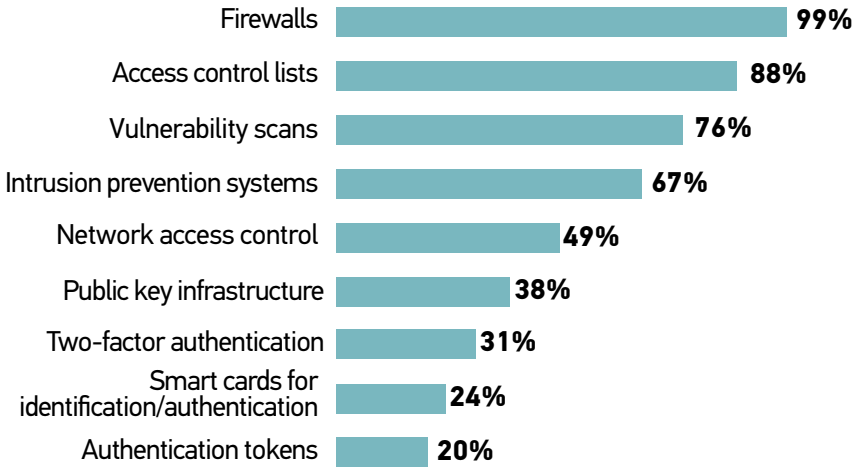

Figure 2. Deployment of various security practices

IT departments are actively implementing additional technical protections in response to changing and increasing threats (figure 3).

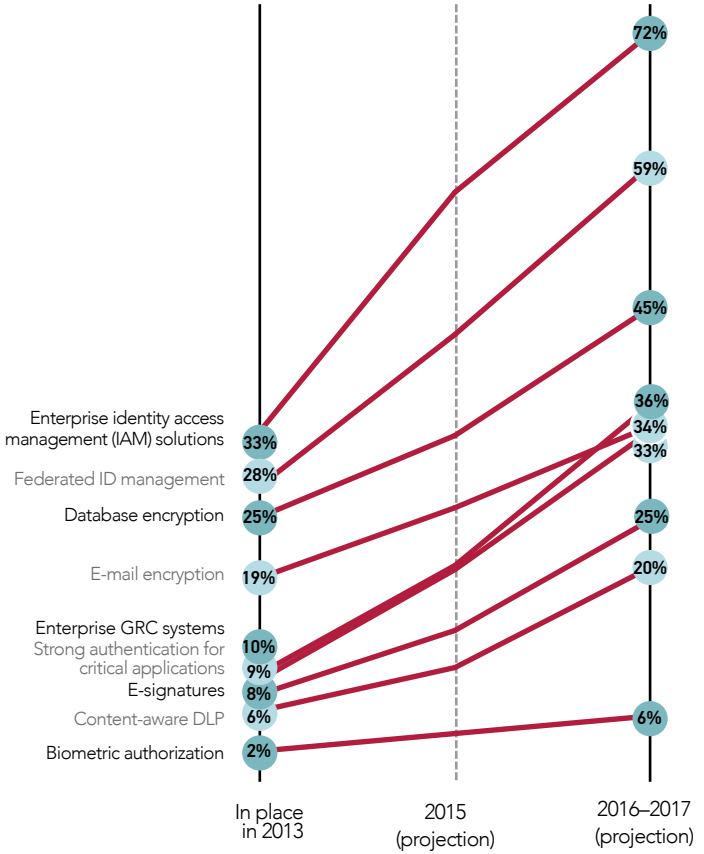

Figure 3. Projected increases in the deployment of information security protections

Which information security policies has your institution implemented?

Essentially all colleges and universities have implemented a core acceptable use policy (AUP, 99%) and engage in compliance-related practices (99%). Policies to protect critical systems are also widespread. Although personally owned devices are often used to transmit, process, and store institutional data, few institutional security policies extend to them (figure 4).

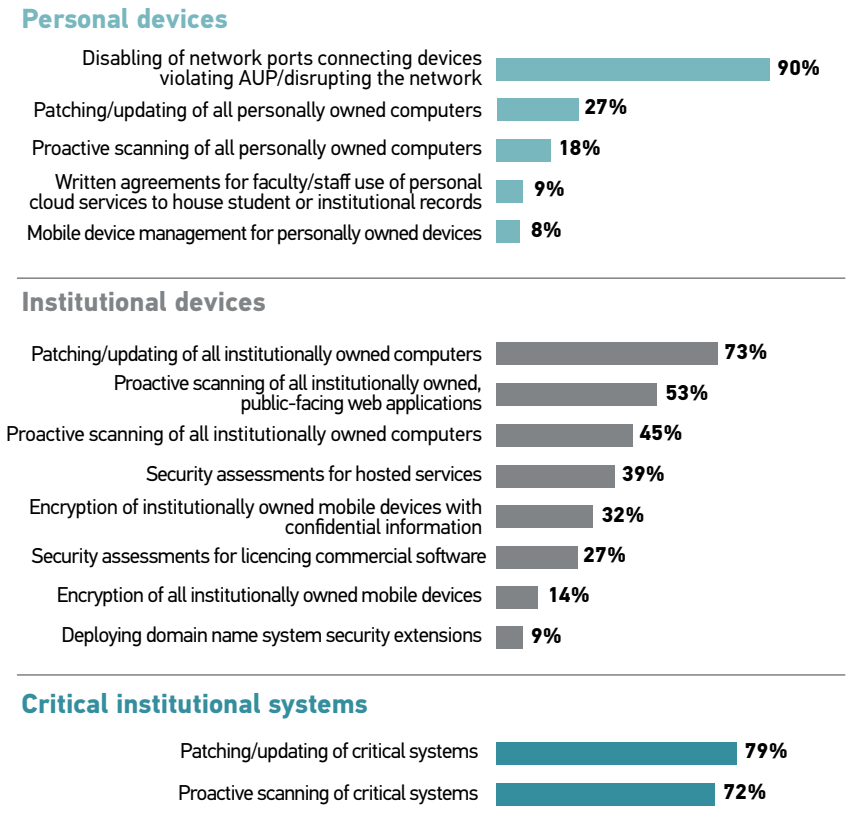

Figure 4. Level of adoption of security practices for various applications, devices, and systems

How effective are your institution's information security awareness and end-user protection activities?

Information security training and awareness programs are key elements of any strategy to protect institutional data and resources. However, fewer than half of faculty (48%) believe their institutions are facilitating a better understanding of information privacy and security. This gap may be due to lack of awareness or might imply the need to improve offerings.

Only about half of faculty report they have access to resources to keep their data secure; the same proportion are confident in their institution's ability to safeguard their personal information. However, the majority of faculty report that they themselves are taking sufficient measures to safeguard data (figure 5). Turning to another dimension, most institutions have instituted privacy and security policies that have not interfered with faculty productivity.

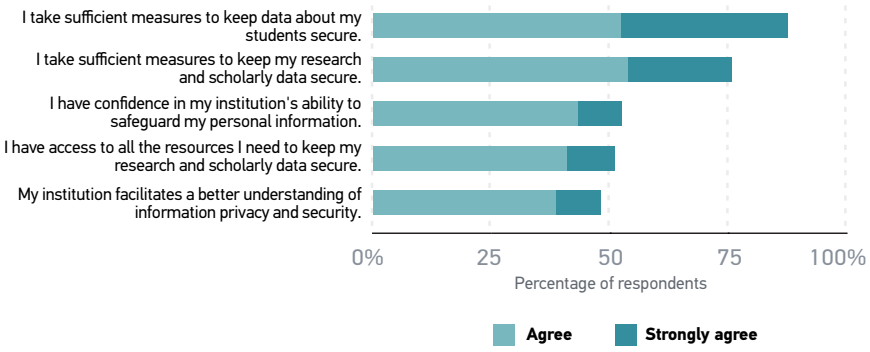

Figure 5. Faculty perceptions of personal and institutional security practices

How would you rate your institution on the maturity of these major elements of information security?

Maturity indices measure the capability to deliver IT services and applications in a given area. They examine multiple dimensions of progress—not just technical requirements—for IT effectiveness, such as culture, process, expertise, investment, and governance. Maturity indices enable institutions to determine where they are and where they aspire to be. EDUCAUSE has identified five dimensions of maturity for information security (figure 6).

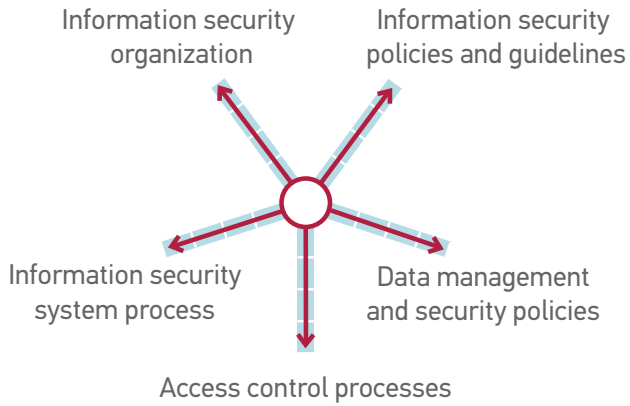

Figure 6. Information security maturity index

What is the single most important next step for your institution in information security?

The primary goal of good security is to safeguard data and identities. This means protecting the data that the institution uses to meet its mission, as well as protecting the identity information of the campus community. Foster an environment that strikes a realistic balance between controlling risk (with investments and policies that protect data) and facilitating the openness necessary to the academic enterprise. Ensure your institution has a qualified and empowered leadership role to understand how to apply contemporary solutions at your institution.

Implications

Threats to the security of institutional, research, and scholarly data are mutable and on the rise. The key to good information security is a strong partnership between IT, institutional risk management, and the institutional community to ensure that the institution is providing the necessary technologies, policies, and processes and that faculty, staff, and students are using them effectively and consistently.

About This Brief

This report is one of a series of executive briefs designed to help institutional leaders optimize the impact of IT in higher education. It was supported by a grant from the Lumina Foundation. To read the other briefs and access related resources, go to Resources for Presidents and Senior Executives.

EDUCAUSE

EDUCAUSE is a nonprofit membership association created to support those who lead, manage, and use information technology to benefit higher education. A comprehensive range of resources and activities are available to all EDUCAUSE members. For more information about EDUCAUSE, including membership, please contact us at info@educause.edu or visit educause.edu.

© EDUCAUSE This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.