AN EDUCAUSE EXECUTIVE BRIEF

Foundations of Information Security:

Institutional Implications for Safeguarding Data

AUGUST 2014

EDUCAUSE

Introduction

Hardly a week goes by without a media report about a data breach that exposes sensitive personal information such as Social Security numbers, credit card numbers, or health information. Education (K–20) has some of the highest numbers of reported data breaches among industry sectors including retail merchants, health care operations, and the U.S. federal government. From 2005 to early 2014, there were 562 reported data breaches at 324 unique higher education institutions. About 7% of all U.S. higher education institutions have had at least one data breach, and one-third of these institutions have had more than one.[1] The estimated cost of a single breach is $8 million, not counting reputational costs or loss of productivity.

Data are the lifeblood of institutions of higher education. Without the exchange and transmission of data, students could not enroll and their progress toward a degree could not be tracked, employees would not be paid, and research could not take place. Institutions use data in operational and strategic ways every day. However, if individuals perceive that an institution will not safeguard their sensitive personal data, or if regulatory bodies discover that an institution does a poor job of safeguarding the data entrusted to it, then the future exchange of data is threatened. Data are central to the mission of higher education.

The purpose of information security is to balance the institution's need to use both data and IT resources (openness) with the competing need to secure those data and resources from external and internal threats (risk control). This balance is often precarious, with additional tension coming from external laws and regulations, funding sources, complex systems, distributed environments, business process stakeholders, and institutional culture. Good institutional information security encompasses the technologies, policies and procedures, and education and awareness activities that maintain balance. Although this process is delicate, reports indicate that higher education generally does a good job maintaining that balance and will lean toward openness (see figure 1).[2]

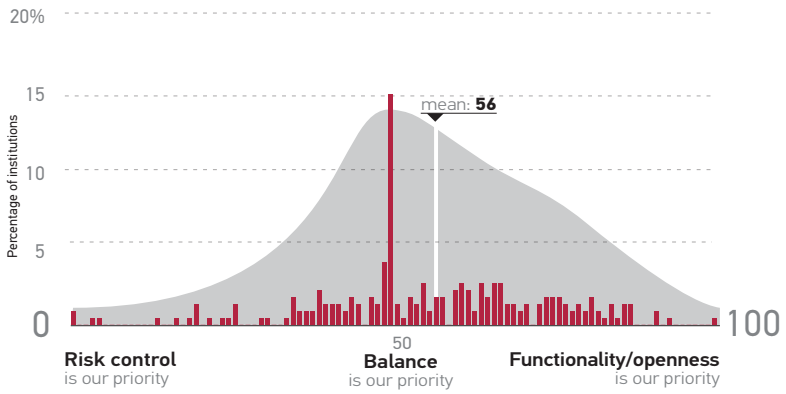

Figure 1.
Institutional balance of IT risk control and functionality/openness

[1] Joanna L. Grama, *Just in Time Research: Data Breaches in Higher Education*, just in time research (Louisville, CO: ECAR, May 20, 2014).

[2] Jacqueline Bichsel and Patrick Feehan, *Getting Your Ducks in a Row: IT Governance, Risk, and Compliance Programs in Higher Education*, research report (Louisville, CO: ECAR, June 2014), available from the ECAR IT GRC Research Hub.

STRATEGIC IMPORTANCE

Colleges and universities are entrusted with large amounts of data: student data regarding grades, degree progress, and even visits to the student medical center; employee data including personnel files, tax and financial information, and health insurance claims; research data including raw results, test-subject identifiable information, and data for patents and other intellectual property protection; and the institution's own business data such as financial and budget forecasts, expenditures, and historically significant records. Due to their collection of so many different types of data, much of which is regulated by state and federal law and industry regulation, institutions are under significant pressure to properly safeguard and use that data. Good information security bolsters trust in the institution, reduces institutional risk, and ensures reliable operations.

- **Trust**. Information security ensures that data remain confidential. This means that only the right people, with only the right amount of access privileges, can access the data that the institution stores in both electronic and paper form. Information security accomplishes this by making sure that people with no affiliation to the institution cannot access institutional resources and data. It also ensures that individuals within the institution can only access data relevant to their jobs. Faculty, students, parent, alumni, government agencies, and other key members of the community lose trust in the institution if it cannot protect the privacy of sensitive data. Loss of trust affects the institution's reputation and could even lead to the loss of alumni donations or other external funding.
- **Risk**. Information security risks (such as data breaches, intentional or unintentional data exposure by employees, or lost storage media) carry a host of negative institutional consequences. These consequences can be financial, such as the direct costs of notifying the institutional community of a data breach; operational, such as the loss of data or systems needed for critical operational functions; and reputational, such as negative media reports. Institutions with lax information security practices are often remembered, and vilified, by name. Good information security practices help reduce an institution's exposure to risks and mitigate the adverse consequences of those risks.
- **Operations and Decision Making**. Information security ensures that institutional IT systems and the data within them are available when the institution needs them for business and academic processes. It also makes certain that the data in institutional systems are accurate and can be relied on for operational and strategic decision-making purposes. Without reliable and robust systems, IT systems and the data within them might not be operational during high-use periods, could be susceptible to intrusion by outside actors, and could contain erroneous information that could negatively influence institutional decisions

Examples

The following examples illustrate some of the ways institutions approach information security:

System Information Security Oversight

In 2012, the University of Hawaii settled a class-action lawsuit regarding data breaches at the university. As part of the settlement, the university agreed to provide continuous credit monitoring and enhanced identity theft recovery services. The lawsuit stemmed from a series of data breaches that occurred at the university from 2009 to 2011. While all of the breaches occurred in violation of university information security policies, they led to a renewed culture of data protection on system campuses. As part of that renewed culture, the University of Hawaii System developed a strategically oriented, system-wide information security program. The program focused on several areas for improvement, including data governance and oversight, audits and risk assessments, policies and procedures, identity management and access controls, and training and awareness. Each campus designated an IT security lead, and the system created a Data Security Leadership Council composed of senior campus leaders. Ongoing efforts include regular meetings of the leadership council, random audits, compliance assessments, improved incident response plans, and reports to the system board of regents. The new program has led to visible due diligence, as well as mechanisms to assess the state of information security within the system.[3]

CISO as Strategic Role

The University of Arkansas is the flagship higher education institution in the state, with a $500 million annual budget and 25,000 students. Prior to 2013, it also had no designated chief information security officer (CISO). Rather than have a designated official responsible for information security, security activities were buried deep within the IT organizational chart, with little cross-department organization. The role of the new CISO was to elevate information security from an operational IT function to a strategic program for the benefit of the entire institution. This required both a technical understanding of information security operational activities and strategic planning experience. The new CISO initially focused on building relationships with other departments and colleagues on campus, creating a campus security team (from no designated security staff to a small team of two staff members) and responding to questions from campus departments interested in improving information security. As part of this process, the new CISO created a collaboration toolkit that helped departments cross organizational-chart boundaries to improve security practices. Future initiatives include security (staff and resources) capacity planning, identity and access management activities, and revisions to the university's information security policy.[4]

[3] Information on the University of Hawaii's information security program was presented at the 2014 Security Professionals Conference and is available online.

[4] The CISO at the University of Arkansas presented his first-year experiences at the 2014 Security Professionals Conference. A video of the session is available online.

Learning from Incidents

In the fall of 2013, Washington University in St. Louis experienced a phishing attack targeted primarily at faculty in its medical center. The phishing e-mails were made to look as if they came from the university's IT services and human resources departments and were designed to steal the victims' IT account credentials. The criminals then used the compromised credentials to change the victims' direct deposit bank account information to divert payroll payments from the institution. Thirteen individuals fell victim to the scam, of whom 11 had their direct deposit information changed. In the incident, a total of $97,210 was stolen from those changed accounts, of which $91,470 was recovered. The university quickly made changes to defend against this threat and rethought the current incident response capabilities to better handle widespread and targeted attacks. The university experienced a similar targeted attack in January 2014. This time 17 people were fooled but only 4 had their direct deposit information changed. Due to new verification mechanisms enacted following the previous incident, the university was able to quickly identify and halt payroll payments to the changed accounts. No money was stolen in the second incident.[5]

[5] Information on the Washington University in St. Louis phishing attack was presented at the 2014 Security Professionals Conference and is available online.

[6] EDUCAUSE Core Data Service, 2013 results, Module 7, Question 9, regarding security technology deployment. For more information, please see the CDS website.

Technology

Some technologies are staples for higher education information security operations. Different technologies are used in concert to secure an institution's infrastructure and data. Firewalls are the most widely used security technologies at colleges and universities. Access control lists (ACL), used to manage user and process permissions, and intrusion prevention systems (IPS), used to monitor networks and block malicious activity, are also deployed widely in higher education. The use of network access control (NAC) and data loss prevention (DLP) technologies is also on the rise. NAC technologies assess the security of equipment connecting to an institutional network and prevent access to the network until identified vulnerabilities on the equipment are resolved. DLP technologies are used to protect institutional data by monitoring for a potential data breach during data storage and transmission (see figure 2).[6]

The increasing prevalence of the bring-your-own-everything (BYOE) phenomenon stresses the importance of sound information security practices. User-provisioned technologies are often seen as bigger security issues because

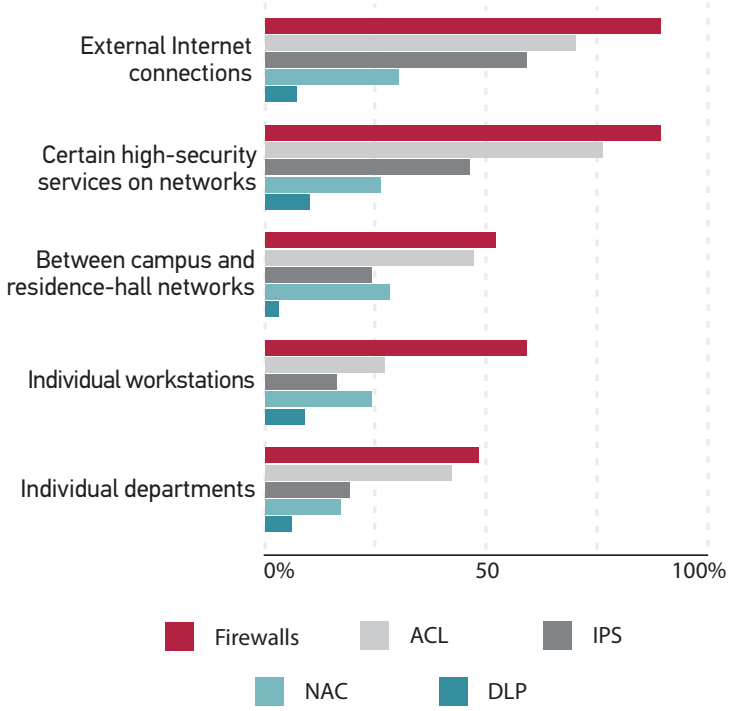

Figure 2.
Deployment of information security technologies in higher education

institutions and their IT departments have little or no control over the devices that users introduce to the institutional network. Thus, security practices designed to protect data—as opposed to protecting the delivery mechanism—are important. Implementing and improving mobile security for data is a high or essential priority at 55% of institutions. BYOE security issues are summarized in figure 3.[7]

Institutions plan to meet the BYOE phenomenon by securing data (60%), securing devices (49%), and preventing data loss (48%).[8] According to the EDUCAUSE Core Data Service, 8% of U.S. institutions have already instituted mobile device management technologies. Many institutions have also instituted e-mail encryption and database encryption to secure institutional data.[9] Making improvements in these areas is a good idea, independent of the use of mobile devices. Sound security practices protect institutional data holistically, not just in a device-dependent situation.

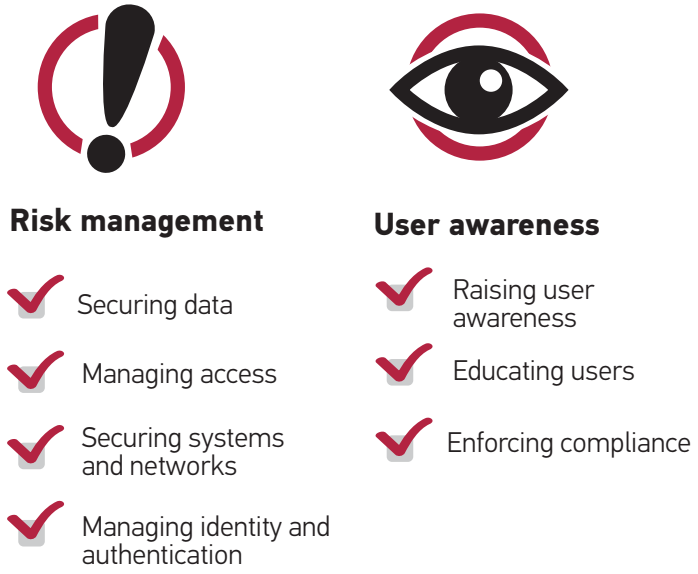

Figure 3. Important factors in BYOE security practices

[7] Eden Dahlstrom and Stephen diFilipo, with a foreword by Mark Askren, *The Consumerization of Technology and the Bring-Your-Own-Everything (BYOE) Era of Higher Education*, research report (Louisville, CO: ECAR, March 25, 2013) available from the ECAR BYOE Research Hub.

[8] Ibid.

[9] Susan Grajek, *Higher Education's Top-Ten Strategic Technologies in 2014*, research report (Louisville, CO: ECAR, February 20, 2014), available from the ECAR Strategic Technologies Research Hub. E-mail encryption is deployed at 19% of respondents, and database encryption is deployed at 25% of respondents.

Current Landscape

The strategic deployment and use of information security and related technologies is essential even if the application or data live in the cloud. Based on reports of current deployments, the use of cloud-based security solutions will more than double by 2016–17 (from 5% in 2013 to 16%).[10] Enterprise identity and access management solutions, used to identify and manage users entitled to access institutional IT resources and data, are in place at 33% of institutions, and that rate will more than double by 2016–17, to 72% (see figure 4).

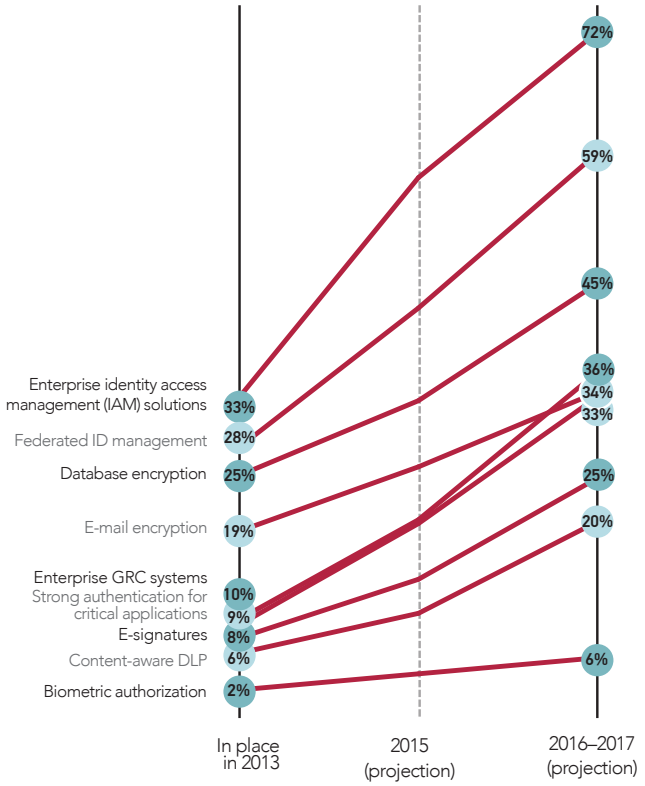

Figure 4. Implementation estimates for security and privacy technologies

The U.S. Department of Homeland Security suggests that higher education institutions are attractive targets for cybercrime due to their open and transparent environments, robust and complex IT infrastructure, and innovative research and development programs.[11] Consider the following:

- A community college's network was hacked, and personally identifiable information including birthdates and Social Security numbers was accessed. The attack originated from international IP addresses, and subsequent forensic analysis indicated that the attack was sophisticated.
- A data breach at an Ivy League institution disclosed personally identifiable information, including Social Security numbers, of individuals affiliated with the institution. The data were made publicly available when the files on institutional servers were indexed by a common Internet search company and returned to Internet users in relevant search results. It is unknown whether the data were subsequently accessed for criminal purposes.
- A group of hackers posted over 100,000 records on the Internet from more than 50 different universities. The group breached the security of institutional servers in order to retrieve the records. The records contained usernames, passwords, and contact information for students

[10] Ibid.

[11] YuLin Bingle, Marc Hoit, Lauren Kielsmeier, and Jenny Menna, "U.S. Department of Homeland Security Cybersecurity Engagement for Colleges and Universities," *EDUCAUSE Live!* webinar, July 24, 2014.

and faculty. The hacking group said that the reason for the attack was to draw attention to the state of higher education and poor network-security practices.

Technology alone cannot guarantee data security because not all threats are technology threats. Whereas hacking, or electronic trespass by an outside party, accounts for about 36% of reported breaches in higher education, unintended disclosure (posting sensitive information on a website or otherwise mishandling such information) and insider threats (intentional breach of information by someone with legitimate access) account for 33% of reported breaches (see figure 5).[12] To mitigate accidental disclosure and insider threats, good information security relies on a mixture of processes and technologies. This means that cross-institutional collaboration is required to ensure information security in individual departments and units that handle institutional data.

Information security safeguards are generally classified as technical, administrative, or physical. Physical safeguards are actions that an institution makes to protect its tangible resources, such as building secure data centers or installing video surveillance in designated areas. Administrative

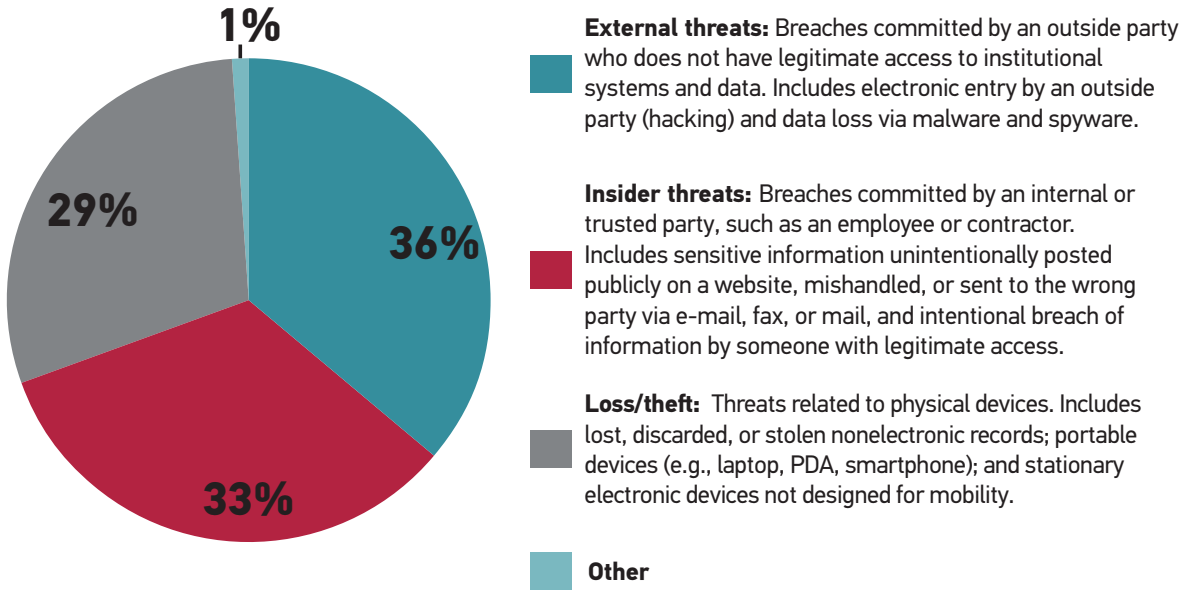

Figure 5. Types of data breaches in higher education

[12] Grama, *Data Breaches in Higher Education*.

safeguards are those based in policy that set forth the rules in the workplace for dealing with IT resources or institutional data. An institution's policies on the acceptable use of IT resources or on how electronic transactions should be handled are administrative in nature. Technical safeguards are those controls implemented in the hardware and software of IT resources. These include implementing the technologies discussed above (firewalls, network access control, and intrusion protection systems).

Although 90% of central IT organizations have primary responsibility for institutional information security, central IT organizations do not singularly manage all information security activities.[13] Often central IT departments are responsible for implementing technical security safeguards, likely because these safeguards require a single, concerted, centrally managed effort to be effective. Administrative safeguards, however, require a multifaceted effort that touches business process practices, employee awareness, and unit- or process-specific technology implementations (see figure 6). Often responsibility for these practices is shared between central IT and another institutional unit.

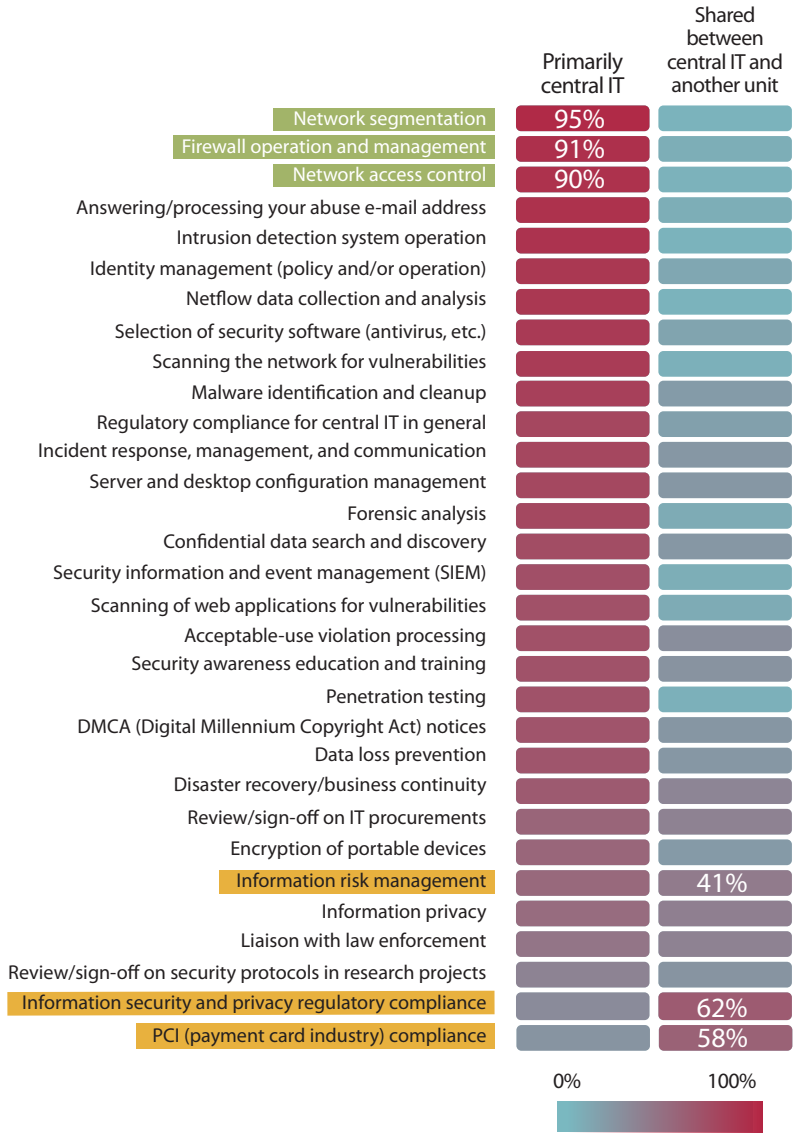

Figure 6. Responsibility for information security practices[14]

[13] Joanna L. Grama and Leah Lang, CDS Spotlight: Information Security, research bulletin (Louisville, CO: ECAR, July 10, 2014).

[14] Responses other than "primarily" or "shared with" central IT are not represented in this figure.

Risks and Rewards

The risks and rewards in the information security realm seem clear. Without good information security practices unsecured data may be impermissibly disclosed (breached). A number of direct costs can be attributed to a breach:

- Investigation costs, including staff time and fees to retain a forensic expert
- Notification costs, including staff time and the expenses of providing affected individuals with tools to mitigate their personal exposure from the breach, such as credit-monitoring services
- Regulatory or industry fines that vary depending on the nature of the breach and type of data exposed[15]
- The costs of responding to media and individual requests for information related to the breach
- The costs of legal representation, including the cost of litigation

There are also indirect consequences to be considered. Institutions can face reputational and consumer confidence losses that could lead to the loss of alumni donations, a decrease in students choosing to enroll at the institution, or decreased state or federal funding opportunities. Some sources estimate that the cost of a data breach in higher education is $294 per record breached.[16] This figure is intended to capture direct and indirect costs. If the average number of records exposed per higher education data breach is 27,509,[17] then the total costs to an educational institution for one breach incident could exceed $8 million. This is significantly more than the mean higher education institutional spend on information security and identity and access management combined.

Good institutional information security cannot eliminate the possibility of a data breach, but it can decrease the chances that an institution will experience a devastating breach. Good practices can also help demonstrate an institution's due diligence and good faith in the event of a breach, which can potentially lower regulatory or industry fines, litigation costs and settlement agreements, and other direct costs. In addition, robust information security practices ensure stakeholder confidence in the institution and may lessen the indirect consequences of a breach.

[15] In 2013, a state university agreed to pay $400,000 to settle alleged violations of the Health Insurance and Portability Act of 1996 due to the breach of unsecured electronic protected health information.

[16] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, May 2014.

[17] Grama, *Data Breaches in Higher Education*.

Strategies for Institutional Leaders

Understand that information security is an institutional issue. Institutional leaders who recognize that information security must be addressed by the whole institution and not just an IT department are in a better position to improve institutional information security in a strategic manner. An institutional culture of good information security cannot be built from the bottom up.

Designate an individual responsible for information security. According to the EDUCAUSE Core Data Service, institutions with a chief information security officer or other full-time staff member devoted to information security are more likely to have implemented security practices and related technologies such as scanning and patching institutional systems, encrypting data, and mobile device management. The individual responsible for information security should possess both technical skills and business acumen. This individual also should have sufficient visibility and authority within the institution to tackle and solve information security issues.

Use current IT governance, risk, and compliance structures to elevate information security concerns. Eliminate unnecessary fear, uncertainty, and doubt without reinventing the wheel. Information security cannot be successful without a concerted institutional effort and the ability to elevate information security concerns to the appropriate officials. Use existing IT governance, risk, and compliance programs to address information security holistically with other IT activities.

Take steps to ensure that information security is a collaborative process. Information security requires teamwork to be successful. Many stakeholders have a bona fide interest in information security. Stakeholders include, but are not limited to, business offices, human resource departments, legal and internal audit departments, and system owners. An approach that includes stakeholders and takes into account business processes, employee awareness, and campus and unit- or process-specific technology implementations is more likely succeed.

Ensure that all institutional community members are aware of how they can protect institutional resources and data. Institutions use IT systems and the data they contain every day. To be effective, institutional staff members need to know how to use those systems and data properly. Information security training and awareness programs address the threats to institutional resources and data and ways to avoid those threats. These programs ensure that the human factor does not thwart other institutional information security activities.

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. To read the other briefs and access related resources, go to Resources for Presidents and Senior Executives.

EDUCAUSE