CEP Magazine - February 2022

The privacy 'evolution to revolution' in higher education

By Decanda M. Faulk, Esq., RN, CIPP/US

Decanda M. Faulk (df@faulk-associates.com) is General Counsel of US Post-Acute Service Solutions in Union, New Jersey, and Founder of Faulk & Associates in Newark, New Jersey, USA.

Decanda M. Faulk

Protecting the personal information of students and employees is an ongoing concern for higher education institutions (HEIs), such as colleges and universities, that rely on modern information systems to store essential business and resource data. The security of these information systems must be adeptly handled by applying both technical and behavioral controls. However, the security culture in HEIs remains challenging because of the reportedly lax attitude of employees (particularly faculty, staff, leadership, and governing bodies) toward the HEIs' resources and their obligations to maintain their privacy and security. In addition, the ease and comfort with which students use technology, specifically social media platforms, increase the vulnerabilities of campus information systems and exposure to malware.

Thus, balancing traditional legal and regulatory compliance with contemporary threats to privacy (e.g., data protection, data governance) and cybersecurity are top priorities for HEIs. Yet navigating the legal and regulatory landscape when managing privacy and cybersecurity threats is becoming more challenging. The legal and compliance departments of many HEIs in the United States may not be as familiar with the complexities of data privacy laws and regulations or how to comply with these laws as other sectors. Today, the growth and expansiveness of data privacy laws and risks of ransomware attacks, which pose a threat of significant reputational harm and subject HEIs to penalties for noncompliance, make robust cybersecurity and privacy programs an important compliance endeavor for HEIs.

While security has been around much longer than privacy in HEIs and, therefore, is better established in most HEIs than privacy, this situation is changing. With the numerous pieces of privacy legislation that went into effect in 2020 and 2021, as concern over data breaches, use of data-tracking people's behavior, and biometric surveillance technologies became part of the national discourse, the privacy posture of HEIs is shifting. As privacy concerns grow, HEIs are taking a more deliberate approach to scaling up their privacy and cybersecurity efforts.

The privacy revolution in higher education

Although HEIs are falling behind other sectors in terms of privacy, some appointed privacy officers and security officers after the enactment of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. For example, the University of Pennsylvania was the first HEI to appoint a chief privacy officer (CPO) in 2001.[1] Eighteen years later, the university reportedly had seven full-time privacy staff members.

Over the past decade, as questions and concerns over privacy have become front and center in the public eye, HEIs have been forced to shift positions on privacy beyond the Family Educational Rights and Privacy Act

(FERPA). Today, more HEIs are creating designated CPO roles, and CPOs are now taking on ever-evolving responsibilities, such as working closely with chief information security officers (CISOs) and legal, compliance, and procurement departments. These are encouraging signs, and such actions demonstrate the marriage between privacy and security with respect to collecting, storing, and protecting the voluminous data HEIs are responsible for handling and maintaining.

Notwithstanding some HEIs not having the resources to hire both dedicated CPOs and CISOs, HEIs' recognition of the importance of privacy and privacy oversight beyond FERPA compliance (typically directed to other departments in HEIs, e.g., the registrar's office, the security office) is prompting them to add privacy issues to the agendas of existing committees, such as those for compliance, audits, policy, risk, governance, data stewardship, security, IT, transparency and accountability, physical security, and surveillance. Some HEIs have even added committees dedicated to addressing privacy not only for students but also for faculty and staff. Although subject to applicable laws and regulations, an HEI can generally take any approach it deems appropriate to develop its privacy program. Although some programs are more mature than others, the privacy initiatives of several HEIs began with policy statements and documents that demonstrate an understanding of the relationship between privacy and security and, specifically, how privacy and security domains and objectives are separate.

In 2018, several universities put in place early stage working groups to direct campus efforts on the European Union's General Data Protection Regulation. At that time, their goal was to identify affected systems and processes. In 2019, it was predicted that most HEIs would have privacy officers in the next five to seven years. Reportedly, the number of CPOs is rising and has increased slowly over the years. However, it is still more common for HEIs to have a CISO than a CPO.

Of the many examples that make the case for strong cybersecurity and privacy hygiene, the Accellion case best illustrates why adopting a strong privacy and cybersecurity posture is prudent and essential for HEIs. Vulnerabilities in the IT security company's file transfer software were exposed when it was exploited by cybercriminals in December 2020.[2] Several HEIs were victims of the data breach connected to the vulnerabilities in the file transfer software sold by Accellion.[3] According to reports on the technology news website Gizmodo, files were discovered on the dark web containing sensitive information from several universities: Stanford University; the University of Maryland, Baltimore; the University of Miami; the University of California, Merced; the University of Colorado; and Yeshiva University.[4]

Data files of the affected HEIs were shared on a website called Clop, whose users are known to share snippets of stolen information and demand a ransom in return for not publishing the rest of the stolen data. "Clop has posted data relating to multiple [HEIs], most, if not all, of which have already confirmed their breaches were Accellion-related."[5] Clop published the data from the Accellion breach on a staggered basis and continued to expose new victims, which suggested more HEIs may have been affected.

Where privacy meets security

Privacy is concerned with the collection, use, dissemination, retention, and other processing of personal (confidential, sensitive, private, protected, or whatever iteration is used) information. Personal information is declared by numerous laws as requiring protection from unauthorized, unintended, or unlimited disclosure, and when such information is captured and maintained electronically or through technology, it cannot be protected properly unless security is in place. Similarly, if the information is in paper form, it still requires protection to keep it safe, confidential, and released only as authorized and intended. Therefore, when technology is involved, the same security requirements concerning confidentiality, integrity, and availability must apply.

The intersection between privacy and security has existed since the advent of HIPAA. However, as the internet and social media platforms have grown, the intersection between cybersecurity and privacy has also expanded. Surprisingly, almost 20 years after HIPAA went into effect, the intersection between privacy and security remains elusive for some HEIs. Today, HEIs must improve their privacy and cybersecurity hygiene. To illustrate this point, "in July 2020, it was reported that 1,327 data breaches in the education sector had resulted in the exposure of 24.5 million records since 2005. Higher education accounted for three-quarters of those breaches."[6] Of the risks affecting HEIs in 2019–2020, data security was ranked as the number two liability concern, with this liability contributing, in part, to increasing annual insurance premiums for HEIs. It is estimated that HEIs' annual insurance premiums have grown an average of 10%–35% across their insurance portfolios over recent years.

Most organizations that engage in robust data collection and protection efforts support such endeavors through robust security efforts. However, unlike security, privacy is not merely about protecting data; it is much more significant because it requires individuals to have a say in and a degree of control over how others use or handle their information. Arguably, this aspect is what makes privacy differ from security. Individuals are not tied to a particular manner or method of data privacy protection, but they do expect those who collect, use, disseminate, and store their personal information to obtain the required permissions and protect such data from unauthorized, unlawful, and unlimited uses and disclosures.

Privacy programs versus security programs

Unlike an information security program, which focuses on protecting institutional data and the IT services that safeguard this data from cyberattacks and other types of unauthorized disclosure or access, a privacy program focuses on the laws, practices, and norms regarding how information is collected, used, and disclosed as well as surveillance and observation standards.

Currently, reports indicate more than 30 HEIs have appointed CPOs, and those HEIs have their standard privacy notices and privacy statement documents online; however, each HEI structures its privacy function differently. Privacy functions usually take into consideration an HEI's culture and campus structure. Several HEIs have separate privacy offices, while others have privacy as part of their compliance, law, risk management, IT, or security departments. Several HEIs have frameworks and privacy maturity models, and some have privacy compliance programs that follow a similar approach to developing such programs, which cannot be captured in this article. However, under the fiduciary obligations section herein, the boards of directors of HEIs have questions to contemplate.

The relationship between privacy and security

Many of the new privacy laws require reasonable security and enhanced cybersecurity safeguards to achieve privacy compliance. Therefore, when establishing a privacy program, it is critical to understand the relationship between privacy and security. HEIs can implement effective privacy and security measures if they understand how privacy and information security fit together and how their domains and goals diverge. Generally, a privacy program focuses on the laws, practices, and norms around how information is collected, used, and disclosed as well as norms around surveillance and observation. Standards for surveillance and observation have been coined "autonomy privacy," which refers to the ability of individuals to conduct activities (e.g., visit websites, conduct research, and compile related data) without fear of being observed.[7] An information security program focuses on protecting institutional data and the IT services that support it from cyberattacks and other types of unauthorized disclosure or access.

The information security function is critical for information privacy and protecting personal information (as well as nonpersonal information and infrastructure) from unauthorized access. Yet controls that strengthen information privacy (such as online monitoring) frequently weaken autonomy privacy. Thus, balancing autonomy privacy interests with information privacy interests as well as other values and obligations (such as transparency, accountability, functionality, and efficiency) requires each HEI to make a unique determination. Representing privacy in these conversations is a key responsibility of CPOs and supports maintaining the CPO role as distinct from but closely partnered with the CISO role, as an HEI's circumstance allows.

Because information is an important component in any organization, and information systems have become an integral part of managing its flow, HEIs are not immune from the risks posed by organizations that possess data. HEIs have heightened privacy concerns and face risks posed by ransomware in terms of the amount of information flowing through various departments for different uses. Administration, finance, academics, and research collaborations are key areas in HEIs for which progressive computer systems and computing is used to achieve desired goals. The need to secure a variety of resources in any HEI is crucial for stability and growth. Information security experts have highlighted the vulnerability of information and computing resources in HEIs because their systems are no less important than those of any other organization in terms of revenue and reputation. Therefore, the suggested security constraints and controls in HEIs should also be up to date, and they should be periodically revised to keep up with advanced threats and breaches. Generally, the security controls implemented in HEIs are meant to detect technical issues, such as malicious software, malware, and antivirus attacks through fake websites, and provide password protection and network virus detection, but they often ignore the negligent human aspect involved in the exploitation of resources and information.

Fiduciary obligations

"Contrary to popular belief, data security begins with the Board of Directors [or trustees], not the IT Department."[8] Although a 2018 study found that 89% of chief executive officers treat cybersecurity as an IT function, experience suggests that cyber risk management is a "whole business" issue. Some boards of directors delegate their cyber risk oversight duties to audit committees, while others have stand-alone cybersecurity committees at the board level. A recent study revealed that 60% of directors surveyed plan to improve their cybersecurity oversight role over the next year. In meeting their fiduciary duties and compliance oversight responsibilities for achieving data privacy compliance, boards of directors may want to include members with privacy and cybersecurity expertise in addition to those with legal, compliance, audit, and risk management backgrounds. It is imperative that boards of directors have answers to the following critical questions:

- What kind of data is the HEI keeping?
- Why is the HEI keeping the data it keeps?
- Where does the HEI store its data?
- Are the HEI's policies and procedures adequate for protecting the data?
- Are the HEI's actual security practices in line with its policies and public-facing statements?
- Are the HEI's security investments and expenditures in line with its security risks and threats?
- How is our HEI using the National Institute of Standards and Technology Cybersecurity Framework and/or systems and organizational controls to drive our cybersecurity measures?

HEI boards of directors must be equipped to deal with a rapidly changing environment, and they must critically assess their current structure and processes to ensure their institutions are engaged in a thoughtful process to implement adequate physical, electronic, and other security measures to prevent, manage, and respond to data breaches.

Bring legal and cybersecurity together

As HEIs become more digitized and exposure to cybersecurity breaches logically increases, the confidence we place in HEIs requires that their digital infrastructure is trustworthy. Although it is not expected of a board to manage day-to-day privacy and security operations, a board should set priorities in these areas and ensure that the necessary resources are allocated to establish and maintain effective privacy and security measures within its environment. In this regard, HEIs, like organizations in other sectors, must maintain a holistic view of data management, which includes synergies between data protection and privacy regulations and a shattering of silos between cybersecurity and legal issues. Thus, it is prudent for boards of HEIs to promote taking a similar enterprise risk management approach to privacy and security operations and control as has generally been used with compliance.

Takeaways

- Boards should set priorities for privacy and security operations and allocate the necessary resources to achieve practical and effective information security controls.
- Do not mistake compliance for effective security. A strong data security program cannot be reduced to checking the boxes in demonstration of good cybersecurity hygiene.
- Managing information security in the higher education institution environment requires knowledge of applicable laws/regulations and best practices to create workable cybersecurity protocols for staff members.
- Chief information security officers should work closely with their cybersecurity teams to prevent, respond to, and recover from the myriad cyberthreats to networks and systems.
- It is impractical and cost prohibitive for higher education institutions to mitigate all cyber risks; however, they can be better prepared for worst-case scenarios.

[1] Elaine Wilner, “Penn Confidential,” *PennToday*, February 27, 2003, https://penntoday.upenn.edu/2002-03-28/latest-news/first-chief-privacy-officer-named.
[2] Andrew Moore et al., “Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion,” Mandiant, February 22, 2021, https://www.mandiant.com/resources/accellion-fta-exploited-for-data-theft-and-extortion.
[3] Lindsay McKenzie, “Secure File Sharing Compromises University Security,” Inside Higher Ed, April 7, 2021,https://www.insidehighered.com/news/2021/04/07/accellion-data-security-breach-latest-hit-universities.
[4] McKenzie, “Secure File Sharing Compromises University Security.”
[5] Lindsay McKenzie, “Universities Affected by IT Security Company Data Breach,” Inside Higher Ed, April 5, 2021, https://www.insidehighered.com/quicktakes/2021/04/05/universities-affected-it-security-company-data-breach.
[6] Elise Povejsil, “10 Concerning Stats About Cybersecurity in Higher Ed,” Collegis Education, May 24, 2021, https://collegiseducation.com/news/technology/10-concerning-stats-about-cybersecurity-in-higher-ed.
[7] University of California, “UC Statement of Privacy Principles,” accessed December 12, 2021,https://www.ucop.edu/ethics-compliance-audit-services/_files/compliance/uc-privacy-principles.pdf.
[8] Jared Ho, “Corporate boards: Don’t underestimate your role in data security oversight,” Federal Trade

Commission, April 28, 2021, https://www.ftc.gov/news-events/blogs/business-blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security.