S
ome concepts in life are naturally linked, considered to be both intertwined and incongruous. Night and day. Young and old. Peanut butter and chocolate. Security and privacy. For the first time, the last two yin and yang concepts appear on the annual EDUCAUSE Top 10 IT Issues list.

Security: The Veteran
Information security is no stranger to the Top 10 IT Issues list, having topped the list for the past three years. In 2019, Information Security Strategy again headlines the list. Higher education institutions intrinsically recognize the importance of securing the many different types of data needed to “run the business.” Personally identifiable academic, administrative, health, benefits, and research data fills the basic bucket of the very sensitive data that colleges and universities handle every day. As discussed in this year’s Top 10 IT Issues article, everyone at an institution has a role to play in protecting the data that is entrusted to higher education institutions. To be done well, information security requires a risk-focused, multilayered strategy.

But what exactly is information security strategy? Most of us understand that it is about protecting data. However, from an information security practitioner standpoint, “protecting data” boils down to three fundamental concepts: confidentiality, availability, and integrity. Confidentiality is the security concept that comes closest to being inextricably linked with privacy topics. We understand confidentiality to mean that only the right people with the right permissions can use certain IT resources and access the data in those systems. Many of the functions that are very common in campus and IT units, such as identity and access management practices, exist to properly manage users, their roles at the institution, and the data they can access. These processes help to ensure confidentiality. When these processes fail, sometimes an unauthorized exposure or breach of sensitive data can result. These types of data exposures are a failure of information security confidentiality.

Availability and integrity are two other important information security strategy concepts that are often given short shrift. Availability means that institutions and users of institutional IT resources (and the data contained in those resources) can depend on those resources being operational when they are needed. Integrity means that users of IT resources can rely on the accuracy (sometimes called cleaneiness) of the data in those systems and of the system processes using that data. When the campus network is running slowly, or when students and faculty can’t log in to a learning management system, a failure of information security availability has occurred. If a campus webpage is defaced or if institutional analytics data is suspect, a failure of information security integrity has occurred.

Higher education has been aware of the importance of protecting data and securing institutional IT resources for a long time. The Higher Education Information Security Council (HEISC) was formed in 2000 in recognition that colleges and universities could work together to improve information security practices across higher education. EDUCAUSE has reported numerous times on the rise of the campus Chief Information Security Officer, and today over one-third of institutions have a dedicated individual whose primary responsibility is information security.

Privacy: The Rookie
For the first time, Privacy made the Top 10 IT Issues list, landing in the #3 spot for 2019. It’s not entirely surprising that privacy was on the minds of higher education IT leaders in 2018: the May 2018 enforcement date for the European Union General Data Privacy Regulation (GDPR) was an oft-discussed topic throughout the year. That law grants EU data subjects (i.e., natural persons) significant privacy rights, and it requires covered organizations to put safeguards in place to protect a data subject’s personal information. Although it is a European law, GDPR causes potential concern for US higher education institutions with respect to personal data collection for international student recruitment and admissions activities, study-abroad programs, international faculty and staff recruitment, and international research activities. The ripple effects of GDPR are already being felt in the United States. For example, the state of California has already enacted (and amended) a consumer data privacy regulation.

But what exactly is privacy? Privacy is a simple term that refers to concepts that apply to society and to discrete individuals. In the United States, a societal notion of privacy limits the government’s power to interfere in the autonomy of its citizens. This right to be free from governmental interference is a core privacy concept for many Americans, flowing from the US Constitution.
For individuals, privacy means the right to control their own data and to specify how that data is collected, used, and shared. This is the concept of privacy that is codified in the GDPR. The US Federal Trade Commission has issued five Fair Information Practice Principles (called FIPPs) that provide best-practice guidance for the collection, use, and protection of personal information:

1. Notice/Awareness: Individuals are provided with notice about the collection of their personal data (before data collection happens) in order to allow them to make an informed choice about participating in the data collection.

2. Choice/Consent: Individuals have a real choice as to how their information will be used. This notion of consent extends beyond the stated purpose for which the information was originally collected, and individuals can withdraw their consent at any time.

3. Access/Participation: Individuals have the right to review any information that an organization collects about them and to request that the information be corrected if it is inaccurate or incomplete.

4. Integrity/Security: An organization must properly protect the personally identifiable data that it collects, and an individual has a right to ask organizations to correct inaccurate data.

5. Enforcement/Redress: Individuals can hold an organization accountable for complying with the FIPPs.

In higher education today, privacy discussions focus less on the societal expectation of privacy and more on individuals’ privacy. These discussions are often very complex and include deep inquiry into the FIPPs concepts to determine whether or not the use of personally identifiable data is justified in the campus setting. Typical examples of privacy discussions in the higher education context include how to best comply with the many federal and state laws addressing privacy; student education records use and disclosure; the responsible use of big data and predictive analytics; open records laws and academic freedom; research (particularly human subjects research); and the privacy impact of emerging technologies that collect personal information.

The growing complexity of these discussions has led to the creation of a new, specialized role: the campus Chief Privacy Officer (CPO). The CPO title is commonly used for the senior-most individual responsible for the institution’s privacy department or program. This role has been emerging steadily on campuses since about 2002, when the University of Pennsylvania appointed its first privacy officer. As the higher education data privacy community has continued to grow, EDUCAUSE has offered resources to help campus leaders navigate privacy discussions.6

**Risk Brings the Veteran and the Rookie Together**

The two Top 10 IT issues of Information Security Strategy and Privacy are similar and closely related, but they are not the same. For example, information can be private (meaning that it is collected and used according to the FIPPs concepts), but it is certainly not secure if that information were to be shared indiscriminately with the world. Conversely, information can be secured (meaning that the concepts of confidentiality, integrity, and availability are adhered to), but it is certainly not used in a privacy-protective manner if it was collected without consent or if an individual has no opportunity to correct inaccurate data. This is the yin and yang of security and privacy.

Perhaps the one concept that unites both security and privacy and provides a framework for dealing with complex conversations is the concept of risk. A security or privacy misstep can have a negative impact on an institution, from a loss of system availability to unfavorable publicity and damage to the institution’s reputation. Thus, treating security and privacy issues as business risks that must be identified, assessed, prioritized, and managed helps the institution provide reassurance that it can meet its mission and goals.

While risk management is never a one-size-fits-all proposition, to get started with managing security and privacy risk in 2019, campus leaders should consider taking the following steps:

- Catalogue the institution’s most critical IT resources and data, focusing on those assets that are most critical to the institutional mission or that have the most regulatory-compliance requirements.
- Identify the threats and vulnerabilities to those resources, concentrating in particular on threats to the security of resources and data and any FIPPs-like vulnerabilities that may be present with respect to personally identifiable data.
- Evaluate potential negative consequences to the institution if any of the potential threats and vulnerabilities (together these are called risks) in the previous step were to be realized; prioritize the risks in terms of likelihood of occurrence and impact to the institution.
- Create a forward-looking strategy for managing the potential negative consequences, including specific steps to mitigate the identified security and privacy risks.

The presence of both Information Security Strategy and Privacy on this year’s Top 10 IT Issues list provides higher education leaders with an opportunity to elevate IT risk management activities to the enterprise level. The push-and-pull, complementary-yet-independent, yin-and-yang nature of these topics provides leaders with the opportunity to develop strategic partnerships across the campus to address data protection in a comprehensive and proactive manner.

**Notes**

2. It should be noted, however, that the US Supreme Court didn’t explicitly recognize a constitutionally granted right to privacy until 1965, in Griswold v. Connecticut.

© 2019 Valerie M. Vogel and Joanna Lyn Grama. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.