Looking back at the Top 10 IT Issues from 2002 through 2020, we see a transformation of the idea of “security” in higher education. Most recently, the word strategy has been added to information security. This addition is important and very different from the management and operational connotations of previous years and signals that a transformation is under way. Privacy is also in transition. Whereas there has long been a focus on compliance with regard to privacy, we are now seeing a shift toward the ethical use of private data. In higher education today, privacy discussions are looking at the societal expectation of privacy.

Four members of the Higher Education Information Security Council (HEISC) Advisory Committee offer their perspectives on these shifts.

Michael Corn
Chief Information Security Officer, University of California, San Diego

Micki Jernigan
Chief Privacy Officer, University of North Carolina at Chapel Hill

Patricia Patria
Vice President for Information Technology and CIO, Worcester Polytechnic Institute

Kent Wada
Chief Privacy Officer and Director, Policy and Privacy, UCLA

Please share your thoughts on the importance of Information Security Strategy being #1 on the Top 10 IT Issues list again this year.

Patria:
As both threats and regulations continue to increase, it becomes increasingly important to have a security strategy based on risk that is established in accordance with acceptable thresholds set by senior leadership, not by the IT organization. If campus leadership establishes acceptable levels of risk for the institution, information security professionals can focus their efforts on the risk that the institutional leadership deems most important and can then build long-term strategies to address those risks. This approach moves from transactional security to strategic security.

Corn:
It’s impossible to review the news without seeing some discussion of information security and how it’s playing out on the national and international stage. Coupling this with the increasing challenges of regulations, such as CUI (controlled unclassified information), leaves me not at all surprised that security remains at the top of the list. I was really happy to see the word “strategy” appear this year. As practiced, security creates so much pressure toward tactical thinking that it’s healthy for those of us in the field to try to step back and ask: “What the heck are we doing, and where are we going?”

Can you discuss your approaches to and thoughts on risk-based security strategies?

Patria:
The first step in building a risk-based strategy is to create a risk register, which is a prioritized listing of all of your risks. Once you have that in place, you need to review it with the senior leadership team at your institution and determine risk threshold and buy-in. From that point, you can create a security strategy around those prioritized risks.

Corn:
Most of us instinctively take a risk-based security strategy. But creating a register and allowing the prioritization of it to drive your annual work plan applies a higher level of discipline toward making your program risk-centric. We do need to acknowledge, however, that this tacitly codifies our security strategy as “prioritize risks and tackle them in that order.” This is operationally appropriate but really just reframes strategy as a series of tactics.

Information security professionals have long advocated for having a “seat at the table” and for security being considered earlier in
the process (rather than as an afterthought). Is being #1 a point of pride? Does this recognize security as an enabler? Is security vital to the success of other institutional issues?

Patria:  
If you have a defined governance process, information security professionals should have a seat at the table, and you should be able to vet the security of products before they are selected. Although this is an important part of the process, I see security shifting even more. Boards are becoming more aware of cybersecurity as a risk, and I think many boards will start to ask more questions around how institutions are managing cyber risks. This elevates the seat at the table to have much larger conversations. Having a seat at the table elevates the conversation and engagement.

Corn:  
Don’t overlook the idiosyncratic nature of leadership at our institutions. Being able to communicate with campus leaders, in their own terms, about information security and risk builds trust. Formal processes of governance are helpful, but that trust results in a larger embrace of the role of information security.

How do we shape the future of information security strategies?

Patria:  
In the past decade, many IT organizations built programs that focus on protecting devices and the perimeter. That perimeter no longer exists; ubiquitous devices and cloud computing have added complexity to the threat landscape. Over the next few years, I think we will see a shift in how employees interact with soft assets like data and an increased use of behavioral analytics tools that leverage artificial intelligence to find threats on the network. Because security resources are very scarce and hard to find, I also foresee a shift to managed service providers for security.

Corn:  
We’re going to have to retool in order to reflect the tactical realities of highly skilled state actors becoming our most threatening high-risk threats. But as we mature as a field, we’re going to need to develop a strategy that allows us to focus our resources on mission activities. If we don’t, we face becoming entrenched as merely a cost center for our institutions.

Working in information security can be a highly stressful job that sometimes leads to burnout. What words of wisdom or encouragement can you share with other higher education information security professionals?

Patria:  
There is no question that security is a 24/7 job and that burnout is real. I think it is important to build redundancy among security teams where possible, allowing staff to take time for vacations and professional development. I also see some organizations looking to outsource basic Security Operations Services (SOC) so that third parties can deal with the off-hours, low-end threats, leaving on-site staff to deal with the more complex work that needs to be done during normal office hours.

Corn:  
We need to change the framing of this issue. Sure, burnout is a challenge, especially with limited resources. But we need to stop talking about how expensive security is, especially with staff. We’re not expensive: we’re valuable.

Wada:  
Privacy is about people. It can mean the privacy we expect in the bedroom, the ability to keep our thoughts to ourselves, or the quiet enjoyment of a life not under constant surveillance by paparazzi. Often, we mean information privacy, the control over and use of data about ourselves—data generated as we go about our daily lives, data-radiant devices and services in hand. The vast opportunities for innovation from a data-rich world benefit both individuals and institutions alike, but both also suffer the risks and consequences of failure. Nowhere is this more evident than with big data and algorithms, which hold promise for great human benefit, potential for basic infringement of individual autonomy, and implications for our efforts in diversity, equity, and inclusion. Finding an appropriate balance, in real time with technological advancement, is the challenge for those of us working in colleges and universities.

Jernigan:  
Privacy is a concept that governs the access, use, and disclosure of data. Generally in higher education, laws, regulations, and policy guide these actions. Too often, however, those inside higher education focus on the disclosure aspect because that is generally the highest risk for fines, penalties, civil actions, and reputational harm. Other areas of concern are the inherently internal access and use of the volumes of data that a college or university possesses. Higher education institutions should not focus strictly on student data privacy. Vendor contracts should be closely scrutinized to ensure that the institutions’ data, especially identified data, is not being inappropriately used or accessed by that vendor.

Corn:  
I feel we’re at the point where we need to tease apart what privacy means within higher education as distinct from the broader conversations about privacy in the public sphere writ large. Our use of data in higher education is fundamentally distinct from what Facebook or a credit agency
does with personal data. We need to tune our approach to privacy to reflect that.

Over the last eighteen months, there has been a bifurcation in the privacy conversation, with a focus on regulatory privacy (e.g., GDPR) and a shift toward ethical use. What do you see? Is there another way to frame the conversation?

Corn:
In general, the field seems to be tending toward compliance. The response to (or embrace of) GDPR as a rallying cry underscores that.

Jernigan:
The privacy discussion often begins with the regulatory requirements, but it should not end there. Attorneys general provide the answers to specific questions and no more. Privacy officers go beyond that, into data governance principles. Data governance necessarily includes the ethical concept of “should we” allow something to occur with the data. Each institution must define what it deems appropriate regarding regulatory requirements, ethical considerations, reputational risk, and general risk-tolerance. A privacy officer must be able to balance all of these aspects to build, grow, and maintain a privacy program.

Wada:
In the 2019 Top 10 IT Issues list, 94 percent of institutions indicated agreement or strong agreement that they respected privacy rights in conducting student success studies. On the surface, this is difficult to reconcile with the explosion of discussions (or arguments) around the appropriate use of the vast troves of student data in student analytics. These discussions are happening at every level of the educational sector—by state governments passing legislation and, of course, by our own institutions, if in no other way than asking the pointed questions about how private-sector partners derive value from these data assets. These are some of the “should we?” questions.

Last year Privacy was #3 in the Top 10 IT Issues list. This year security and privacy move even closer together, with Privacy at #2. In 2019, Valerie Vogel and Joanna Grama proposed that risk brought the two together. What do you think?

Jernigan:
Privacy and security are very closely tied but do have different risks associated with each. As a privacy officer, I have worked to protect both the institution and the data. By default, this is a protection for individuals as well. The internal use and access of data, or use and access by entities we share data with, are the areas that need continued focus. One example is an IT vendor that has template language in its contract allowing full access to and use of the data entered into its system. Some vendors add the ability to combine the data with that of other customers. Some even state that they may sell or lease the data they create to other parties. How often is this being challenged in your institution? Is this practice seen as an issue, or is it simply the cost of doing business?

Other examples are cameras or scanners on campus. There is generally a stated purpose for each of these (e.g., physical security and tracking), but once the data is collected, can it be used for other purposes? Should it be? Generally the answer is “maybe.” Are there policies in place to define this use? Privacy is a very factspecific discipline in which the situation and types of data can influence the recommendations from the privacy officer and, ultimately, the decisions made.

Wada:
Information security and information privacy working hand-in-hand to safeguard information about people is a smart, tactical approach to enhancing operational effectiveness. However, risk to the institution and risk to the individual are not always aligned. Using Micki’s example of an agreement, the remote possibility of a privacy breach could be acceptable risk to an institution—based on contractual financial remedies and cyber-insurance. But for affected individuals whose data would be out in the wild, there is no actual cure. As a privacy officer, I also consider myself a voice of those not at the table and try to ensure that we consider both risk equations explicitly.

How important is trust in terms of privacy in higher education?

Wada:
I’d argue that privacy is a basis for trust, rather than the other way around. Privacy also underpins other words: respect and dignity.

Jernigan:
I agree. Students trust that an institution will do what it is “supposed to do” with their data. Patients trust that their health providers will do the same. And so on . . . Strong data governance processes or programs are inherently built on the trust of the individuals from which the data is derived.

Note

© 2020 Brian Kelly, Valerie Vogel, Mike Corn, Micki Jernigan, Patricia Patria, and Kent Wada. The text of this work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.