The Third Time’s the Charm?  
Information Security at the Top of the List Again

Joanna Lyn Grama and Valerie M. Vogel, with Michael Corn and Sharon Pitt

For the third year in a row, Information Security tops the EDUCAUSE Top 10 IT Issues list. Only one other issue, Sustainable Funding, has topped the annual list more times in a row (a three-peat from 2003 to 2005 and again from 2009 to 2011).

We asked the co-chairs of the Higher Education Information Security Council (HEISC) to reflect on the third #1 placement of Information Security on the EDUCAUSE Top 10 IT Issues list.

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

Sharon Pitt, Vice President of Information Technologies, University of Delaware

Is it significant that Information Security is the top IT issue for the third year in a row? Why or why not?

Corn: I think it is significant. While colleges and universities continue to invest in information security, we security practitioners have failed to clearly define a strategy for cybersecurity, and thus our leadership feels “unmoored” in response to the public drama of large-scale data breaches. Thus, whatever the news of the day happens to be, we hear the constant question: “What are we doing in response?”

Pitt: Yes, it is significant. The continued appearance of this issue is a combination of our not yet having a handle on the issue as well as a changing and more sophisticated threat environment combined with increasingly demanding compliance responsibilities.

What is higher education, in general, doing well in the information security area?

Pitt: I believe we’re doing a great job of creating policy and of building awareness—in part because these are low-hanging and perceptually inexpensive fruits on the secure institutional “tree.” We’ve got a lot of people time—and that time can be repurposed toward building capability in areas that don’t require us to spend new dollars on security.

Corn: While each of our institutions has its own idiosyncratic strengths and weaknesses, collectively we’re exceptionally tuned to focus on high-value practices. Few cybersecurity programs can afford to be inefficient; thus we coalesce around effective technologies and practices, and our culture of information sharing (as exemplified in the EDUCAUSE HEISC program) can be seen as an emergent property of our collective practices.

How do data breaches such as the September 2017 announcement of the Equifax breach impact higher education?

Pitt: That’s an interesting question. I believe people are more furious that Equifax executives may have benefitted personally from the breach than they are about the breach itself. We’ve almost become inured to breaches, in the sense that so many of us have experienced one in some form or another. Of course, the data stolen from Equifax (and from the U.S. Office of Personnel Management in 2015) will allow more-sophisticated phishing to take place. So, the onus for higher education is continuing to focus on security awareness training, as well as putting multifactor strategies in place to protect institutional (and, by extension because of good security practices, personal) assets.

Corn: My first thought was, why on earth do we keep apologizing for the state of information security in higher education when this one breach is probably fifteen times the sum total of all higher education breaches in aggregate? Individually, even the tiniest breach is a bad thing for our communities and reputations, but in aggregate, we’re a footnote. Still, the breach does underscore our role as research and teaching institutions and the as-yet-unmet need for better technical solutions and for more trained security professionals.

What is the top information security concern (strategic or operational) that keeps you up at night?

Corn: The world has been transformed by the easy exchange of information. We’ve crafted all these wonderful tools for sharing data, and it should come as no surprise that people use them—often inappropriately, from the security perspective. As security professionals, most of us have grown up in environments where we literally control the software ecosystem. Those days are long gone. Yet I’m not sure we’ve created a professional framework that makes sense in a contemporary IT ecosystem. The very vocabulary “security control” is beginning to feel like an anachronism.

Pitt: I’m sleeping well, thank you, but a big worry is the inevitable breach, because it’s an unknown. Will it be an internal or an external threat? Will our team be capable of handling...
the technology challenges associated with the breach? Will our institutional leaders keep their heads on straight and respond with aplomb and dignity? All of these are wildcards. The best that we can do is train, put procedures in place, and practice for the inevitabilities that we will never be able to specifically define but for which we can outline a broad "cone of impact."

Institutions that face a breach are likely to take a big hit to their reputation based on how they respond to it. Look at Equifax: because of the manner in which the breach was handled—from executive mismanagement of information to the perceived inability to sue (and of course, the fact that the company is a credit bureau)—its reputation has suffered.

What do you think small institutions struggle with the most in creating and maturing their information security programs?

Pitt: Prioritization, combined with growth capacity. With very limited funds, an institution can find it quite easy to allocate all resources toward one aspect of a security portfolio—and then be done, with no more resources to commit to security. Determining how to continually make progress, from year to year, toward a justifiable security stance is a huge challenge. Smaller institutions can take advantage of the many resources available from HEISC (e.g., security-awareness campaign materials, template policies, assessment tools), as well as explore innovative strategies to share security staff and security resources across institutions.

Corn: Scope. The portfolio of the security professional at Whatcom U with 500 students is almost the same as that faced by those of us at very large state schools. As Sharon says, prioritizing and being strategic on the small scale is really challenging. Fortunately, more and more smaller schools are finding creative ways to partner with others, and many security practices are now becoming cost-effective as vended services.

What do you think large institutions struggle with the most in creating and maturing their information security programs?

Pitt: Culture, although culture likely impacts institutions of all sizes. There is a tendency for IT staff to believe that security is the responsibility of the security operations team, rather than of all members of the IT staff. And of course staff such as device-support professionals, client-support professionals, and network professionals are all engaged in creating a justifiably secure technology environment.

Larger institutions may be more engaged in sponsored research than are smaller institutions (I realize this is a very stereotypical statement, since some smaller institutions are heavily engaged in sponsored research). This activity has its own requirements around data loss protection and compliance. In the past few years, many of us at larger institutions have struggled with how to deal with export control and with the National Institute of Standards and Technology's new requirements around research activity.

Corn: Culture. (You can see why I like working with Sharon.) But I have a different perspective on this. I see too many schools where the broader distributed IT culture is seen as a problem, rather than as the solution to many of our resource challenges. As is the case at many other institutions, at UC San Diego the central IT organization represents only around 25–35 percent of the full IT workforce. If I can support and empower that other 65–75 percent of IT staff so that they put merely 5 percent of their time into effective security practices, that's a huge force multiplier for my office and the university.

What last piece of advice would you give to institutions as they consider their own information security programs?

Corn: Participate. Whether I'm working with the REN-ISAC (https://www.ren-isac.net/) or in one of the EDUCAUSE HEISC workgroups or discussion forums, I've always reaped much more than I've sown from participating.

Pitt: Breathe. It takes time to build mature capability in this area. You're likely doing more than you think you are doing to invest in an appropriate security stance for your institution.

Notes
1. HEISC (http://www.educause.edu/security) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. HEISC publishes the Information Security Guide, which features toolkits, case studies, and best practices to help jump-start campus information security initiatives.
2. Voting for the EDUCAUSE Top 10 IT Issues was open from August 28 to September 7, 2017. The Equifax breach was announced on September 8. Our analysis shows that Information Security convincingly held the top spot in the voting on September 7. We observed negligible variations in the ratings given to Information Security after the breach announcement. Even in the days immediately following the announcement, respondents consistently gave ratings similar to those before the announcement. Thus, the Equifax data breach appears to have had no effect on the positioning of Information Security at the top of the IT Issues list for 2018.

© 2018 Joanna Lyn Grama, Valerie M. Vogel, Michael Corn, and Sharon Pitt. The text of this work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Joanna Lyn Grama (jgrama@educause.edu) is Director of Cybersecurity and IT GRC Programs for EDUCAUSE.

Valerie M. Vogel (vvogel@educause.edu) is Senior Manager of the Cybersecurity Program for EDUCAUSE.