CASE STUDY

Transforming Princeton's Security Culture Through Awareness

Security awareness and training programs (also known as user awareness programs) educate users about computer security and organizational policies and procedures for working with IT resources. User awareness programs can reduce information risk and, in some cases, enhance user experience or productivity by improving security-related behaviors and the overall security culture at an organization.

According to the ISACA® *2018 Cybersecurity Culture Report*, 95 percent of global survey respondents identify a gap between their current and desired organizational culture of cybersecurity.[1] This gap is reflected in the reality that most security breaches have user errors (or worse) as part of their causal chain.

Security culture is the collection of behaviors toward and perceptions about security in a computer user community. Universities and other higher education institutions are known to have relatively open cultures as they pursue their teaching and research missions in a spirit of collaboration with institutions and individuals around the world. Unfortunately, in the open culture that is so desirable for learning, there is sometimes a lack of diligence about facing higher education's cyberrisk.

As a major US Ivy League institution, Princeton University (New Jersey, USA) has considerable cyberrisk. Since 2016, the Princeton Information Security Office (ISO) has pursued a user awareness program to improve its security culture, providing a valuable case study in the process.

Dan Blum, CISSP, Open FAIR
Is an internationally recognized strategist in cybersecurity and risk management. His recently published book is *Rational Cybersecurity for the Business: The Security Leaders' Guide to Business Alignment*. He was a Golden Quill Award-winning vice president and distinguished analyst at Gartner, Inc.; has served as the security leader at several startups and consulting companies; and has advised hundreds of large corporations, universities and government organizations. Blum is a frequent speaker at industry events and participates in industry groups such as ISACA®, FAIR Institute, IDPro, ISSA, the Cloud Security Alliance and the Kantara Initiative.

David Sherry, CISM, CISSP
Is chief information security officer at Princeton University (New Jersey, USA). He is responsible for developing university policy and strategy regarding matters of information security. He plays a critical role in addressing the larger institutional issues of security policy and practice, data governance, risk assessment and business continuity, and the compliance requirements that span the university. Prior to Princeton, Sherry worked as chief information security officer (CISO) at Brown University (Providence, Rhode Island, USA), vice president for enterprise identity and access management at Citizens Bank, and as manager of information technology with the United States Postal Service. Sherry sits on a number of committees that fall under the EDUCAUSE Higher Education Information Security Council. He shares his vast knowledge of information security as a presenter at conferences; as a guest lecturer at several institutions; and as a contributor to publications such as *Information Security Magazine*, *Security Currents* and *SearchSecurity*.

Tara Schaufler, CPACC
Is the information security awareness and training program manager at Princeton University. Schaufler has been at Princeton University for 16 years, spending the last eight years focusing on training and technical communications, and in the past four years has built a robust security awareness and training program from the ground up. She is a member of the EDUCAUSE Higher Education Information Security Council Awareness and Training Working Group and a frequent speaker at EDUCAUSE events.

University Background

Princeton University is a private Ivy League research university in Princeton, New Jersey. Founded in 1746 in Elizabeth as the College of New Jersey, Princeton is the fourth-oldest institution of higher education in the United States and one of the nine colonial colleges chartered before the American Revolution. The institution moved to Newark, New Jersey, USA, in 1747, then to the current site nine years later.

Securing Princeton is like securing a city. Princeton has six undergraduate residential colleges, each housing approximately 800 freshmen, sophomores, some juniors and seniors, and a handful of junior and senior resident advisers. Princeton also has one graduate residential college, an art museum, a chapel, an extensive library system, health services, campus police, parks and a cogeneration power plant. The university hosts two Model United Nations conferences. It is home to numerous interdisciplinary research efforts, such as the Princeton Environmental Institute (PEI), which includes large-scale, long-term research centers through which academic and industry partners across the United States and around the world collaborate on researching environmental challenges.

The Princeton InfoSec Program

When David Sherry came on board in 2016 as Princeton's chief information security officer (CISO), there was no active security awareness and training program. Over the next three years, he worked to establish a strong security program. The user awareness program, led by Information Security Awareness and Training Program Manager Tara Schaufler, is a key component of delivering the ISO's mission.

Per Princeton's InfoSec website:

> *The mission of the Princeton University Information Security Office (ISO) is to make information security programmatic and cultural on campus in order to support the University in its mission in teaching and research.*[2]

User awareness is one of the three pillars supporting the ISO mission:

> *The ISO's comprehensive posture increases security and reduces risk while securely enabling access to information for those who need it. Supporting this mission are three pillars: an appropriate governance and policy structure; robust and scalable security architecture, solutions, and operations; and an expansive and continuous security awareness program.*[3]

User Awareness Challenges

"In an ideal world," Schaufler muses, "We would have been able to say 'You have to do this training.' But people were not ready. We needed to get out there and build relationships, and make people understand the threat is real." Sherry and Schaufler (the "awareness team") believe the Princeton user awareness program faces the following challenges:

- Reaching a diverse target audience including students, staff and faculty
- Establishing relationships with security culture influencers
- Overcoming resistance to mandatory security training
- Maturing the awareness program

Reaching the Audience

As of 2016, Princeton's security function had been buried in IT, and University students, faculty and staff had little or no knowledge of the nascent security program.

Sherry and Schaufler needed to publicize the security program, identify effective communications channels, and create high-quality awareness and training content that would be worthwhile for the audience. They also needed to draw the audience to awareness events or communications and deliver training.

Working against them has been one of the basic communications challenges all awareness teams face: getting people's attention. Constant flows of emails, phone calls, text messages and other communications clamor for that attention. Perhaps more than most, the University audience lives in an information-rich environment. Between University and academic websites or libraries and the public Internet, the Princeton community has a dizzying array of content choices and the content is continuously changing.

> "TO BRIDGE THE GAP BETWEEN 'I AM AWARE' AND 'I CARE' IN THE UNIVERSITY CULTURE, THE AWARENESS TEAM HAD TO TAKE IT LOW AND SLOW."

Getting the audience's attention and feeding it awareness content is necessary but not sufficient to improve security outcomes. "Even if someone is aware, that doesn't mean they care," Perry Carpenter wrote in his book Transformational Security Awareness, "And even if they understand and care, we can't guarantee that they understand to the extent that they'd be able to correctly apply the information… If you aren't reinforcing, your audience is forgetting."[4]

Not only must Princeton's security-related communications stand out and cut through the noise in the here and now, they must adapt themselves continuously to a fluid environment.

Establishing Relationships With Influencers

The awareness program comprises just one full-time person plus subject matter expert (SME) assistance from the small InfoSec team of fewer than six staff members. There is no way the team can engage with an audience of more than 17,000 persons without the help of others in the Princeton community.

Early on, Schaufler identified computing support professionals—who number in the hundreds and are spread all over campus—as the force multipliers the program needed. Schaufler notes, "We can't be everywhere. But we can communicate via the Computing Support email list and go to their monthly staff meetings. They help us push the information out and make sure it gets to individual departments. They are like our army. We help each other."

To get to this point, the team had to get to know influencers and managers in the computing support organization. It had to spread the message that it is customer-service-focused and an important resource for computer support and the University. This was a winning strategy from the onset.

Overcome Resistance to Mandatory Security Training

"Who are these 'InfoSec' people? Why should we *have* to take their training?" was a reaction the team sometimes sensed during the early days. More so than in other organizations, university communities value a sense of independence. Faculty members can be a particularly difficult audience to engage due to their notions of academic freedom, which are also imparted to students and staff.

To bridge the gap between "I am aware" and "I care" in the University culture, the awareness team had to take it low and slow. They had to get to the audience's "why"—to make them understand that threats of cyberattacks, intellectual property theft, identity theft, financial fraud and other risk drivers are real, and then connect to different audience segments with convincing imagery and stories to gain their support.

Mature the Program

As of mid-2020, the initial program pain points have been substantially overcome. The team has reached large segments of the Princeton community, has a strong collaborative relationship with Computing Support and other influencers, and has gotten many in the University community to accept the notion of mandatory training. Today's challenge is to expand mandatory training, provide additional advanced training modules online and report metrics.

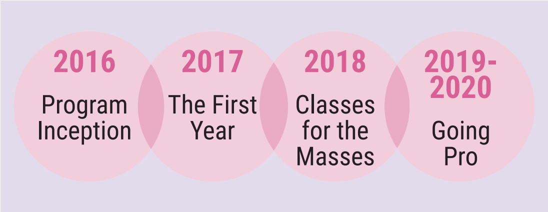
Establishing the User Awareness and Training Program

Princeton's user training and awareness program journey has already passed from program inception and its first training classes to broadening the audience and expanding the content delivered.

The Journey

David Sherry started at Princeton in 2016 and did not have a full risk-based infosec program. His initial strategic plan had a strong focus on awareness and training, which was included in his rollout plan and the proposal for initially hiring a staff of four (**figure 1**).

Figure 1—Princeton's User Awareness Program Journey



> "ARMED WITH VALIDATED IDEAS AND INFORMATION ABOUT GOOD PRACTICES, THE TEAM CREATED INITIAL TRAINING CONTENT AND HELD CLASSES."

Program Inception

After approximately four months at Princeton, Sherry recalls, "The [chief information officer] CIO asked, 'If I asked you to build your team one position at a time, which would be your number one hire?' I said the awareness and training [A&T] person and he agreed. My reasoning was that IT security mechanics were already being handled well at the University and, therefore, of all things we could do, improved awareness would have the most incremental impact. As it was, all four initial staff were hired within a few weeks of each other. Tara Schaufler was the last to actually join due to a transition from her previous university job, and she presented her first class within 90 days."

By appointing Schaufler to the A&T role, Princeton in effect followed what later became one of Carpenter's signature recommendations in the *Transformational Security Awareness* book: Hire an awareness leader who comes from outside the security field and have them come up with a program that satisfies the technical experts.

Schaufler reflects, "When David Sherry posted the awareness and training position, I worked in Princeton's Office of Development as the SharePoint administrator, handling the intranet site's information architecture, overall maintenance and continuous expansion. I was also tasked with leading and organizing training, writing quick reference guides and producing training communications. A lot of what I did in development prepared me for the years ahead in the ISO. I had a lot of excitement and vision on how to train people and could not wait to create this new awareness and training program under David Sherry's direction."

It is important to note that although Schaufler had a technical background as a developer, she began her career in awareness from a nonsecurity background. This is considered a good practice so as not to lose the user's perspective. Having a bachelor's degree in the social sciences and master's degree in human resources (HR) and nonprofit development also provided a solid foundation for working in security awareness—the people part of cybersecurity.

2017: The First Year

The team began by assessing the current situation and learning about the work at hand. Attending meetings about awareness at EDUCAUSE, a nonprofit association that helps higher education elevate the impact of IT, and sharing ideas with peers at other colleges proved very helpful, especially for someone new to security awareness. Armed with validated ideas and information about good practices, the team created initial training content and held classes.

Princeton's first security awareness classes were well attended; two January 2017 presentations on privacy drew an audience of 75. Because the campus seemed hungry for information, the team built on early successes with lunch-and-learn events. These events featured a different topic each month in varied campus locations. The ISO also began recording webinars in 2018 and created a library to broaden accessibility to the information.

> “BECAUSE THE CAMPUS SEEMED HUNGRY FOR INFORMATION, THE TEAM BUILT ON EARLY SUCCESSES WITH LUNCH-AND-LEARN EVENTS.”

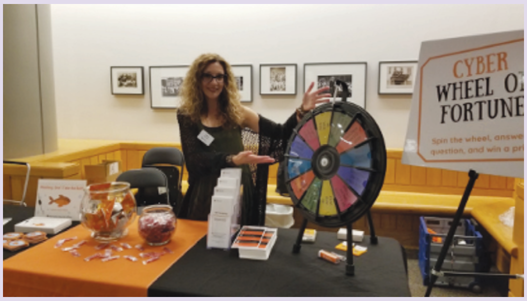
Throughout this time, other influencers began to emerge. “We created strong alliances with public safety, University services and the communications team,” said Sherry. “They became advocates of our mission and our services, requested our training more frequently, and told others.” These activities led to more influential areas of alignment, including the executive vice president (EVP) office, the office of the provost, and the computer science faculty and academic research areas. As a result, the ISO is positioned for success in all areas of the campus.

2018: Classes for the Masses

The years 2017 and 2018 represented a period of learning for the program. The team discovered it could piggyback onto other on-campus events and expose security concepts in fun ways to make security awareness content more compelling.

Students especially liked events featuring games and prizes, such as power banks, cell wallets, Universal Serial Bus (USB) hubs or clear event backpacks. At a campus FluFest event, Princeton also promoted online health. Altogether, several thousand people spun the Cyber Wheel of Fortune (**figure 2**), enough that attendees briefly held up the queues exiting with their flu shots as they waited for their moments of security awareness.

Figure 2—Cyber Wheel of Fortune



Schaufler explains, “The general idea behind these games was to bring interest to our information tables—not just paper handouts and Swedish Fish (although these gummy red candies are always a hit). We wanted a way for people to engage with us, learn and have a little fun.”

The Cyber Wheel of Fortune game requires the player to correctly answer an information security-related question to win the prize displayed on the wheel. The Web Cookie Cornhole game requires players to “feed cookies” to the Internet Monster (**figure 3**). Offered in celebration of Data Privacy Day, players were given a handout explaining privacy risk, and prizes were awarded if they successfully fed the monster (only benign information, of course).

Figure 3—Web Cookie Cornhole Game

During this period, the team realized it needed to provide more in-depth 100- and 200-level classes to the campus community. To motivate audience members at this level, it was helpful to focus on topics with personal relevance or value that also impart beneficial information to improve security-related behavior when working with University information assets. Early 100- and 200-level classes included Securing Your Home Network and Parental Controls.

2019 and 2020: Goin' Pro

Beginning in 2019, the team began to provide 300-level classes on topics such as Secure Remote Administration, Red Team Attack Methodology, and other topics that could improve security capabilities in IT and security operations.

The team worked to expand the audience for introductory security information and get the word out on Princeton security tools and policies by:

- Incorporating security awareness training into the campus-wide LastPass Password Management rollout
- Renting local theaters for movie events and facilitating discussions on films such as *Robot and Frank*, *WarGames* and *The Circle*
- Holding holiday open house events with wine and cheese, festive desserts, and security-themed poster board sessions

For 400-level security training, Princeton utilizes the (ISC)^2 Certified Information Systems Security Professional (CISSP) program, taught by an (ISC)^2 certified Princeton staff member. The ISO's goal is to extend the security program by establishing a CISSP on every devops team and in every department. Up to the present time, the ISO has funded training for 19 additional staff to earn their CISSP certification.

As with every organization, the Princeton ISO's 2020 agenda has been dominated by coronavirus concerns. For security awareness, COVID-19 demands a big emphasis on online training.

The Princeton Security Awareness Tool Kit

The Princeton tool kit includes awareness tools and processes, awareness programs, training programs, and security culture improvement initiatives.

Tools and Processes

Princeton uses the ProofPoint email and web security technology solutions, which provide automated threat detection and user-facing features such as Hover to Discover (enabling one to get information on blocked malicious web pages).

The team recently also added the ProofPoint Security Awareness and Education Platform to its repertoire. This platform provides additional content that can be repurposed for online training.

Princeton maintains its own Phish Bowl website[5] with descriptions of the latest phishing attempts and information on how to report phishing, antiphishing information and other resources.

> “PRINCETON MAINTAINS ITS OWN PHISH BOWL WEBSITE WITH DESCRIPTIONS OF THE LATEST PHISHING ATTEMPTS AND INFORMATION ON HOW TO REPORT PHISHING, ANTIPHISHING INFORMATION AND OTHER RESOURCES.”

Awareness Programs

The awareness program now includes multiple offerings:

- In person awareness events, such as an information table during freshman move-in
- Online awareness content, such as short videos and webinars
- Question-and-answer (Q&A) sessions
- Road shows
- Blog posts, email communications and posters
- Social media presence on Twitter and Facebook
- Annual celebration of both National Cyber Security Awareness Month (NCSAM) and International Data Privacy Day

> “ALREADY, THE CULTURE HAS MATURED TO THE POINT WHERE THE ISO IS SEEN AS AN ENABLER, AND THE IDEA OF MANDATORY SECURITY TRAINING OR POLICIES IS ACCEPTED BY STAFF AND MOST OTHERS IN THE COMMUNITY.”

Training Programs

Princeton offers training for University-standard tools such as the LastPass Password Manager. The inventory of training class includes:

- 100 level—Building Better Passwords
- 200 level—Securing Your Home Network and Segmentation
- 300 level—Technology-Specific Secure Remote Support and/or Administration classes for operating systems and security tools such as Crowdstrike or Rapid7
- 400 level—CISSP training

Red Team Findings as an Object Lesson

To drive the message of cybersecurity risk home to multiple audiences, the ISO has held multiple red team engagements to find pockets of vulnerability and gaps in their capabilities, processes and response. The departments involved often react with a healthy level of shock: “I cannot believe an outsider got this information! How did that happen?” Knowing that their information was exposed made stakeholders more interested in cybersecurity due to the major issues that leakage or exposure could create.

Security Culture Improvement

The awareness team’s ultimate goal is to strengthen Princeton’s security culture. Already, the culture has matured to the point where the ISO is seen as an enabler, and the idea of mandatory security training or policies is accepted by staff and most others in the community. Today, the awareness program pursues the goals of enrolling many active supporters, or security champions, for Princeton cybersecurity.

Many of the team’s awareness and training efforts—from events to games to giveaways or swag—have been undertaken with a marketing and branding mindset. In promoting the value and reasons for cybersecurity, however, the team needs to align its general messaging and approach to the higher education climate for cybersecurity.

For example, although the ProofPoint platform has the capability to perform phishing tests, Princeton does not currently use them. Schaufler explains the awareness program’s mindset and vision for security culture: “We never say end users are the weakest link. They are guardians at the gate to us, the last line of defense. After all, whatever they are seeing came through all the filters. With positive messages we can change their thinking. We want the entire University to be security champions.”

Looking Back on Lessons Learned

As of 2020, the awareness team has completed its first three-year strategic plan. It has used influencers in Computing Support and other departments to get its messages across and synchronized awareness training with security solutions rollouts, such as the Password Manager. It has found ways to make awareness and training content more compelling to the community; successfully contextualized messaging to students, faculty and staff; and used gamification to stimulate interest. Along the way, the team has learned the following lessons:

- **Less is more**—Along the way, the team had to work with the audiences' limited time and attention levels. As it pushed out a great deal of content, putting it into smaller chunks proved to be more effective.
- **Stay in context**—It is critical to couch information in each audience's frame of reference (e.g., How does it impact me? What is my risk?) to open their eyes and get their attention. The classes that people sign up for are those contextualized to their own lives and situations. The team has provided classes on personal cybersafety (i.e., protect the kids). After the Equifax breach, the company featured content on how to protect oneself from identity theft. During the first semester of 2020, with faculty and students thrust into distance learning and the potential for "Zoombombing," web conferencing security became a popular topic.
- **Highlight the risk**—For any audience, it is important to make people understand that the threat is real. Princeton has used The Phish Bowl website to:
  - Indicate the number of incoming phishing messages
  - Answer the common question "Why would anyone want to attack me?"
  - Explain the kill chain in layman's terms

Metrics

As the team optimizes the program and matures reporting capabilities, metrics are becoming important. **Figure 4** identifies some metrics Princeton is collecting as of 2020 and that may also benefit readers at other organizations.

Benefits

Princeton's awareness and training program has delivered multiple benefits, including:

- **Improved cybersecurity outcomes**—Due in large part to the awareness program, Princeton users exhibit better password management, reduced phishing risk, understanding of the threat to both their personal and professional lives, and a heightened awareness of appropriate actions and responses for cybersecurity:
  - After only one year Princeton counts 1,100 LastPass accounts, 75 percent of which are used regularly, out of a 2,500 staff target.
  - More than 16,500 visits to Princeton's Phish Bowl page have been logged since its inception in 2017.
  - A "Danger Banner" is universally visible on suspicious messages with very few reported false positives.
- **Increased engagement**—There has been more engagement with the security program due to outreach and training programs:
  - More than 30 University departments made unsolicited requests for and received the "Getting Started With LastPass" training.
  - The annual Protect Yourself, Protect Princeton Campaign events are experiencing increased attendance.
  - There is consistently high engagement with Web Cookie Cornhole, Wheel of Fortune and Cyber Assessment gamification programs
- **Better audit results**—Princeton's internal and external auditors have moved from citing security awareness as a gap to expressing satisfaction with the program's progress.

Next Steps

Today's challenge is to mature the program. The team plans to add 20-minute online training modules customized for multiple constituencies, starting with new hires this fall. Through rolling six-month plans, the awareness program is building capability to reach 100 percent of the audience with mandatory training, provide additional advanced training modules online, and measure and report on the results.

Figure 4—Security Awareness Metrics

Metric	Results
Available program content	**Data or comment from Princeton**
Number of training classes	94
Number of awareness events	24
Number of online classes or programs	15 webinars
Number of other informational artifacts (i.e., knowledge base articles and position papers)	23 position papers
Audience engagement	**Data or comment from Princeton**
Number of awareness event attendees	7,365
Number of training class attendees	1,996
Number of online webinar attendees	493
Influencer engagement	**Data or comment from Princeton**
Number of active supporters	Undisclosed, but useful to collect
Number of CISSPs	25 in total (including 10 in IT operations and 12 others in the campus community)
Compliance	**Data or comment from Princeton**
Percent attending mandatory training	Planned
Incidents and cybersecurity	**Data or comment from Princeton**
Number of phishing attempts reported	Counting, but undisclosed
Number of phishing incidents	Counting, but undisclosed
Number of IT artifacts (e.g., password quality metrics, help desk traffic, undesirable events seen in logs)	Under consideration
Perceptions of cybersecurity	**Data or comment from Princeton**
Survey feedback results	Under consideration
Adoption of promoted security tools	
LastPass	1,000+ active users

Endnotes

[1] ISACA® and CMMI® Institute, *2018 Cybersecurity Culture Report*, USA, 2018, *https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html*

[2] Information Security Office, Princeton University, New Jersey, USA, *https://informationsecurity.princeton.edu/*

[3] Information Security Office, "Information Security Office (ISO) Mission Statement," Princeton University, New Jersey, USA, *https://informationsecurity.princeton.edu/*

[4] Carpenter, P.; *Transformational Security Awareness*, Wiley, USA, 2019

[5] Information Security Office, The Phish Bowl, Princeton University, New Jersey, USA, *https://informationsecurity.princeton.edu/phish-bowl*