CASE STUDY

Collaborations in Cybersecurity

How colleges work together to defend against cyberthreats

WITH SUPPORT FROM paloalto NETWORKS®

THE CHRONICLE of Higher Education®

A MORE
SECURE
EVERYWHERE

Collaborations in Cybersecurity

Brian J. Kelly, chief information-security officer at Quinnipiac University, says would-be hackers attack his institution "every second of every minute of every day," with probes that easily number 100,000 daily.

The university in Connecticut isn't alone — every college is a prime target for cybercrime. Some bad operators seek to steal the personal data that institutions keep on students and staff members. Others want to grab research results and valuable intellectual property. Still others "phish" for ways to trick college staffers into giving up information or money.

Few institutions have the resources — technological, financial, and human — to fully protect themselves from cyberthieves. That reality has led many institutions to band together in the fight against hackers.

In 2012, for example, Kelly and a colleague held a meeting so that IT-security staff members at private and public colleges across Connecticut could share notes about cybersecurity. After 40 attendees from 24 colleges showed up, they decided to continue getting together.

The meetings "foster collaboration and conversation around what we are doing well and collectively where we need help."

Today the Connecticut Higher Education Roundtable on Information Security meets quarterly, hosted by a different in-

Collaborations in Cybersecurity was written by Stephen G. Pelletier. The Chronicle is fully responsible for the report's editorial content.

stitution each time. Participants share details about hacking attempts and learn from colleagues about strategies that work to protect institutional IT systems and data assets. Hot topics recently have included securing the cloud and blocking "phishers."

The meetings "foster collaboration and conversation around what we are doing well and collectively where we need help," Kelly says. "It really sometimes feels like group therapy."

Colleges in other states and regions hold similar meetings. For example, the NorthWest Academic Computing Consortium sponsors workshops on network and information security, peer networking, and other ways for members to share information. Marty Ringle, the consortium's president, says there are tangible benefits. For example, cybersecurity specialists in his group report that "the information they are currently sharing about the recent uptick in university-targeted spear phishing has been beneficial in protecting their campus constituents." ("Spear phishing" refers to the targeted use of malicious email sent to help steal data or money.)

Flagship research universities, whose research repositories and intellectual property make them a juicy target for hackers, are also collaborating. At the University of Texas at Austin, for example, the information-security office offers two services: CyberPosse, which costs money, and Dorkbot, which is free. Cam Beasley, chief information-security officer at Austin, says his office offers CyberPosse as a tool to share research and expertise with universities that may not have a deep bench in cybersecurity talent. With Dorkbot, he says, "we've engineered our solution to be able to efficiently scale to cover a very large population of campuses."

Members of the Big Ten Academic Alliance have shared ideas, policies, and strategies for protecting information technology since the early 1990s. Two years ago, however, five

Tom Davis helped form a university coalition to combat threats: "We can't continue to be so inwardly focused in cybersecurity in higher education."

EMILY STERNEMAN.

EMILY STERNEMAN.

Five public research universities formed the Omni Security Operations Center, or OmniSOC, to better monitor cyberattacks.

members of the alliance decided to collaborate more definitively. Indiana, Northwestern, Purdue, and Rutgers Universities and the University of Nebraska at Lincoln jointly created the Omni Security Operations Center (OmniSOC, pronounced "omni sock").

MONITORING THREATS

From OmniSOC's headquarters, at Indiana University at Bloomington, staff members actively monitor security information and data from member networks and search for specific threats that may have slipped through those institutions' robust firewalls. If it spots a threat, OmniSOC notifies members — at 2 a.m., if necessary — so they can take steps to mitigate those risks on their networks. The cost to join OmniSOC varies based on the size of an institution and the types of services it uses.

Tom Davis, the group's executive director and chief information-security officer, says OmniSOC reflects a recognition in higher education that cybersecurity is getting more complicated. Another reason for institutions to share information about cyberthreats, he says, is that universities typically cannot compete with the salaries that the private sector can pay for top IT experts who might screen such attacks. "We can't do this alone," Davis says, "so we have to be really smart and efficient about how we bring current resources to bear collaboratively to combat this threat."

"The fact that OmniSOC receives security-alert and -event data from multiple institutions provides us a unique vantage point," Davis says. "When we observe a particular threat at one member's institution, our security engineers are able to quickly see if the same threat is present on any of our other members' networks." Recently, for example, OmniSOC identified malicious software threatening a member university. "Not only did we work with the member's security team to handle the event," Davis says, "we quickly identified the same threat on another member's campus."

OmniSOC shares details about breaches like that with colleges and universities outside its membership via the Research Education Networks Information Sharing and Analysis Center, an organization that started in 2003 and today serves more than 600 colleges and scientific institutions worldwide. The center has worked with Educause, an academic-technology association, and others to help ensure that IT products developed by companies have better built-in protections against hacking. One product of that collaboration has been the Higher Education Cloud Vendor Assessment Tool, designed to make sure that cloud-based solutions are vetted for security and privacy.

STAFFING CYBERSECURITY

Valerie M. Vogel, interim director of the cybersecurity program at Educause, says recent surveys show that more colleges now have a person on campus who is primarily responsible for IT security. Educause found that 34 percent reported having such an administrator in 2016; last year the figure rose to 41 percent. While the rise is significant, she says, those percentages also highlight the fact that more than half of institutions don't or can't staff that critical cybersecurity role. "That's why you're hearing more about shared cybersecurity services like OmniSOC or CyberPosse and about people leveraging other campus's cybersecurity services and tools whenever they can," Vogel says.

Some small, private colleges have taken that leveraging a step further by sharing cybersecurity staff members. According to Vogel, for example, Franklin & Marshall College and Susquehanna University — 85 miles apart in Pennsylvania — share a single chief information-security officer who splits time between the two institutions.

Other institutions collaborate through consortia. In May, the Colleges of the Fenway, in Boston, hired an information-security officer who works for two of the consortium's five members. The officer divides his time equally between the two campuses, which are across the street from one another. Claire Ramsbottom, executive director of the consortium, says that the participating institutions know that if one campus has more-complex issues in a given week, the the staff member might spend more time there. Since this is the third shared position that the consortium has created — the others are in emergency planning and environmental health and safety — Ramsbottom says administrators are open to the idea of sharing expertise, and understand that how the officer divides his time between institutions "is going to even out in the wash."

The New York Six Liberal Arts Consortium, meanwhile, contracts with a company to provide IT security for its six members. The consortium contracts for a number of hours of the vendor's time each year for shared services, says Amy D. Cronin, the group's executive director. "Some of those hours are set aside for collective work that is common to all the schools. And then each school gets its own bucket of hours, if you will, that they can use for specific projects or needs that they have," Cronin says. "It's really worked out quite well, because the schools are getting 365-day-a-year, 24-hour cybersecurity

> **"We can't do this alone, so we have to be really smart and efficient about how we bring current resources to bear collaboratively to combat this threat."**

service, at a far lower cost than they would have been able to achieve separately. They each pay $50,000 a year for the service, and there's no way they could hire an information-security officer for that."

Given that universities today face the double challenge of coping with a proliferation of cyberthreats in an era when institutional budgets are squeezed, it's likely that we will see more collaboration on IT security. Davis, for example, says that as part of its commitment to all of higher education, OmniSOC hopes to expand its scope to serve institutions outside the Big Ten.

"We can't continue to be so inwardly focused in cybersecurity in higher education," Davis says. "The threats change and the market has changed, so we need to figure out ways to collaborate more holistically across the higher-education space."

"The schools are getting 365-day-a-year, 24-hour cybersecurity service, at a far lower cost than they would have been able to achieve separately."

THE CHRONICLE
of Higher Education®

1255 Twenty-Third Street, N.W.
Washington, D.C. 20037
(202) 466-1000 | Chronicle.com