SPONSORED CONTENT

CAMPUS TECHNOLOGY

aruba
a Hewlett Packard Enterprise company

# SECURE THE MOBILITY-DRIVEN CAMPUS: YOUR BEST DEFENSE, IS OFFENSE!

The biggest cybersecurity challenge may be convincing users IT can stay ahead of threats.

**CYBERSECURITY CHALLENGES** on campus are rapidly evolving. The increasing level of sophistication and frequency of attacks, a vanishing perimeter, a mobility-everywhere preference and the growing proliferation of the Internet of Things (IoT) make for a huge attack surface on campus these days. The greater transparency and openness of the typical college or university, not to mention, a social and trusting student user group, also make education a ripe target for attack.

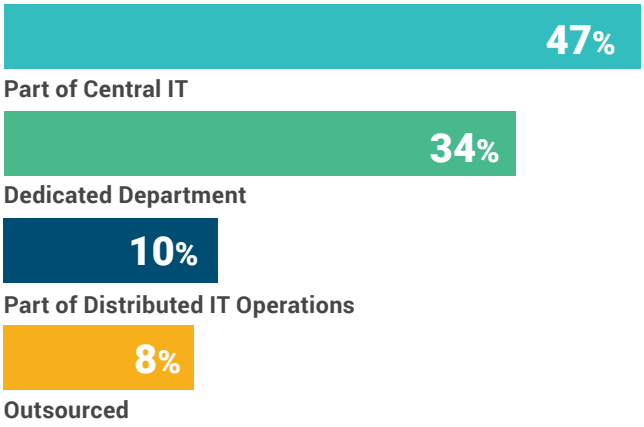
With users moving in and out of campus, all it takes is a bit of casual social engineering by a cybercriminal to uncover some detail from a harried staffer, student, or professor. With some patience, he can figure out with relative ease enough to take over that person's network account and move into other parts of the network. The university must then face the responsibility of explaining what happened, notifying users about the breach, and mopping up the mess at great expense.

Institutions face attackers not only from the outside, but also insider threats. As a recent data breach report pointed out, 19 percent of attacks in education originated from internal sources. The motivations for these insider attacks vary. Stealing personal data, locking down data in a ransomware attempt, and access to research are frequent reasons. Twenty percent of attacks on educational institutions were "motivated by espionage." Another 11 percent were undertaken for "fun."

To understand more about cyberthreats higher education faces, Campus Technology recently surveyed information technology, security, and other campus professionals about how they view their cybersecurity capabilities in areas such as security monitoring, threat awareness and detection, and user training. What stood out was a gap between how well the IT organization believes it is keeping users safe when they're on the network and how much confidence end users have in those security activities.

### Campus Security Structure

Nearly half of respondents (47 percent) reports their IT operations are part of the main IT organization on campus. Another third of institutions have dedicated IT security offices.




No matter who's providing IT security, respondents estimate security for the wireless network currently receives slightly more attention on average (52 percent) than the wired network (48 percent). While nobody would dispute that mobility is king on campus, what's important to remember is mobility wouldn't exist without a robust wired infrastructure in place.

Strong security management is a critical element in keeping both aspects of the network up and running. IT organizations that maintain controls for the wired platform separate from the Wi-Fi, for example, face an additional burden of oversight. That structure would require the monitoring two distinct dashboards. Integrated wired and wireless environments are simply easier to manage.

## EDUCATION FOR ALL

Almost a quarter of the institutions responding to the Campus Technology survey conduct no formal user security training. Among those with something in place, about a third (32 percent) publish security policies on their websites or intranet, but conduct no direct training related to those policies. Nineteen percent run a one-time program specifically for new hires. Another 32 percent mandate annual training programs for everybody. And a hearty few—17 percent—follow up training with testing. For example, they'll send phishing e-mails and follow up with those who click on them for additional education.

CAMPUS TECHNOLOGY

aruba
a Hewlett Packard Enterprise company

### Security Concerns

Survey participants shared their primary IT security concerns. While the answers were as varied as institutional mission statements, predominant themes emerged. Respondents overwhelmingly express concerns about malware, phishing, ransomware, and bots and the havoc they can reap in the form of data breaches and data destruction.

A near-equal number of responses focus on the broader anxieties posed by the growing number and sophistication of security threats, the seeming proliferation of hackers, and an overall lack of attention paid to the need for training of both end users and IT staff. It's hard to keep up, as one IT staffer reported. The big apprehension is the school wants to "maintain security while continuing to provide the services requested for current and new devices."

Way down on the list of concerns related to IT security were issues like internal threats, vulnerabilities posed by overall device insecurity, a lack of compliance to security policies and access management. It may be these categories of threats have already sufficiently addressed; or it may be respondents aren't aware of the possible problems they pose. As one respondent says, the biggest worry right now is "people not paying attention," or as another states, "employees who do not take proper steps to verify spam, viruses, or 'IT' people."

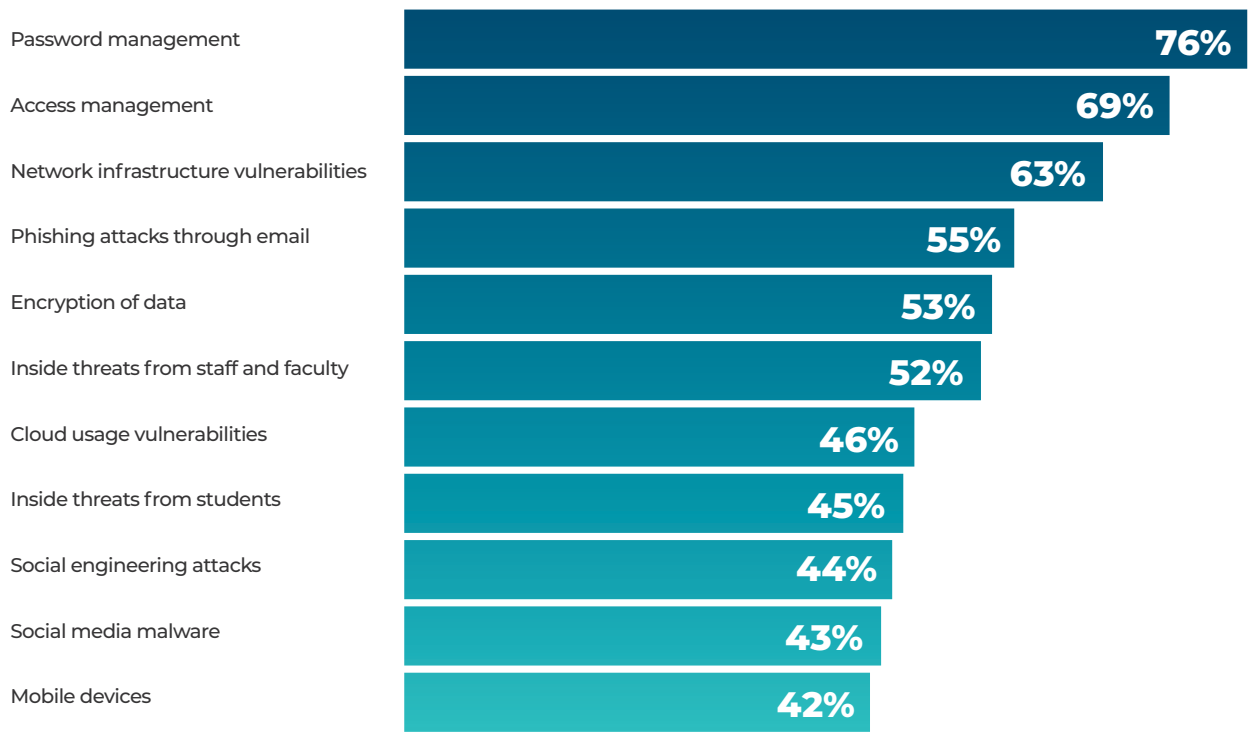
A handful of respondents also gave a glimpse into highly specific problems they're experiencing. One institutional person mentioned the "recent discovery of malware that has been embedded in systems for several years." A second suggests the school's registrar database "is fairly open."

Another speaks of out-of-date "security patches on HR/finance software." And a fourth references the lack of a "centralized monitoring tool to really monitor threats in real time." As this IT leader says, "We are still very reactive."

### Can IT Secure the Campus?

The level of confidence the college or university community has

## HOW CONFIDENT ARE YOU OF YOUR IT STAFF'S ABILITY TO MAINTAIN SECURITY IN THESE AREAS? (PERCENTAGE OF RESPONSES THAT SHOWED HIGH CONFIDENCE)



CAMPUS TECHNOLOGY

aruba
a Hewlett Packard Enterprise company

in its IT organization can influence budget and funding decisions. It can also determine whether those operations remain within the institution or get outsourced; and how much voice IT leaders will have at the executive table. Boosting IT security—and how it's perceived on campus—appears to be a significant area for improvement.

First the good news—password management gets a high rating by IT and non-IT employees and leaders alike. Seventy-six percent of all respondents said they had "complete" or "very high" confidence IT could maintain security in that area, but the assurance erodes from there.

More than half of the respondents (55 percent) say their institutions were on top of possible phishing attacks. A similar number (53 percent) say the same about data encryption. Fewer than half report feeling fully or very confident that IT could handle inside threats from students (45 percent), social engineering attacks (44 percent), or social media malware (43 percent).

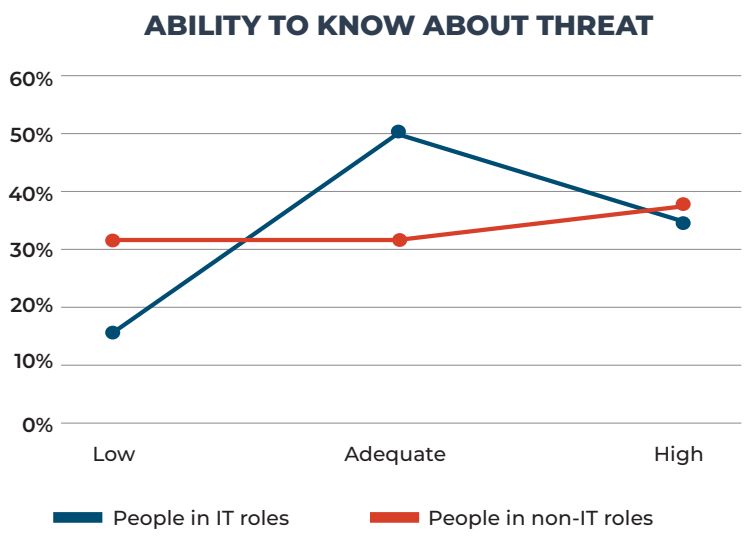
Four out of 10 survey participants (42 percent) were quite certain IT could oversee security tied to mobile device used on campus. This was the service category where people also expressed big concerns. Nearly a quarter (24 percent) said they were "not very" or "not at all" confident IT had the ability to maintain security in this area.

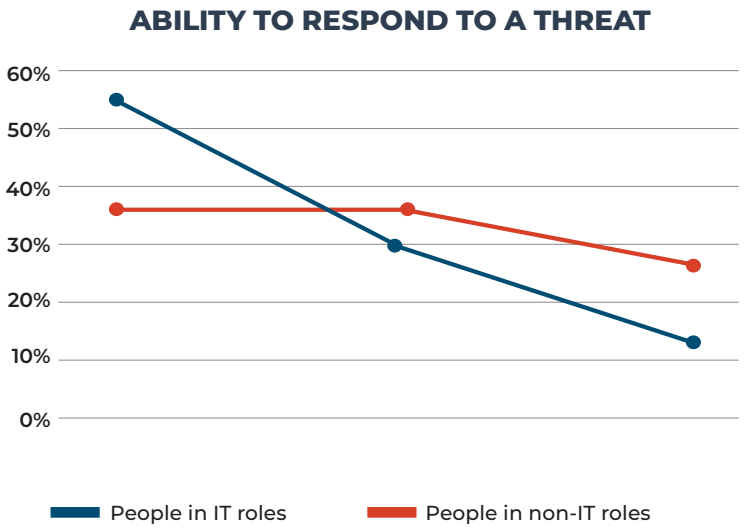
There's a distinct gap between how those in IT positions (both leadership and staff) and those in non-IT positions view the ability of IT to identify a threat as soon as it happens and mitigate damage before it has a big impact on the network. People in non-IT roles are more likely to express either the lowest confidence (31 percent vs. 15 percent) or the highest confidence (38 percent vs. 35 percent) IT would know about the problem. Those in IT roles show far greater confidence in being able to minimize the threat than those outside IT (56 percent vs. 37 percent).

In other areas, the greatest gaps between IT people and non-IT people are in the areas of data encryption and insider threats posed specifically by students. In both cases, IT people were more likely to show greater confidence they were on top of the situation than non-IT people (53 percent vs. 38 percent).

The potential vulnerabilities created by insider threats from staff and faculty created another rift between the responses of members of IT and those who had other positions on campus. Among those in IT, 58 percent have high confidence they can address the threats. Just 43 percent of non-IT people say the same.

There are five specific areas of threat coverage where IT security might consider examining how well it's doing and how well it's communicating those efforts to the broader campus audience. In each of these threat areas, non-IT people express the lowest levels of confidence in their IT security organization's abilities to address the risks:

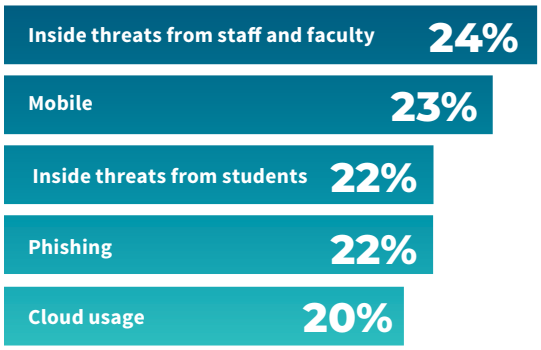


CAMPUS TECHNOLOGY

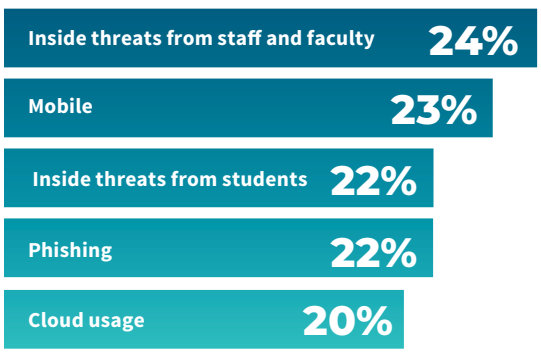
aruba
a Hewlett Packard Enterprise company

## SHARE OF NON-IT PERSONNEL WHO GAVE LOW MARKS TO IT FOR SECURITY PROTECTION




On the positive side, these same individuals give the highest grades to current coverage of these risk areas:

## SHARE OF NON-IT PERSONNEL WHO GAVE HIGH GRADES TO IT FOR SECURITY PROTECTION




### Connected Things: The Newest Vulnerability

Like leaders in any other type of organization, campus administrators are beginning to take note of the potential impact of the IoT on cybersecurity. A global study co-developed last year by Aruba Networks and Kevin Ashton (the analyst who coined the term, "Internet of Things") found 85 percent of enterprises expected to implement the IoT by 2019. This is driven by the need for innovation and efficiencies.

Yet among the 72 percent of organizations that had already introduced the IoT into the workplace, 84 percent had already experienced an IoT-related breach. The median time from compromise to breach discovery was a remarkable 146 days.

Since there is so little confidence in how well IT stays on top of mobile device security, the same is likely true for trackers, wearables, and sensors brought onto campus for facilities monitoring, security purposes, personal well-being, and other activities. Currently, just 32 percent of respondents say they're completely or very confident IT is aware of all the IoT devices on the network; 40 percent had adequate confidence; and 28 percent had low confidence.

Breaking those numbers down by roles, people in IT and IT security positions are far more likely to say they have strong confidence in IT's awareness of IoT devices on the network (37 percent vs. 27 percent). Non-IT people are more likely to have little to no confidence (33 percent vs. 23 percent).

"Our ITS group has done a fair job of stopping major security breaches from the outside and most from the inside," says one non-IT person at a four-year institution. "However, with more IoT devices showing up on campus, I am not sure that they are up to the task of handling breaches from these."

The biggest concern is, "nominally-qualified people and not many of them [are] working on these issues."

### Approaches to Campus IT Security

Nearly every college and university answering this survey has IT security policies in place (85 percent). The rest are in the process of developing those policies (13 percent).

There are myriad practices and technologies institutions use to enforce IT security policy. The top practice is monitoring network traffic to ensure authorized activity and detect intrusion attempts (79 percent). This is closely followed by campus firewall maintenance (75 percent).

The least used approaches (though still in place in at least half of respondent schools) include scanning campus computers for applications known to be attack vectors (50 percent). This is followed by blacklisting of certain types of executable files (53 percent).

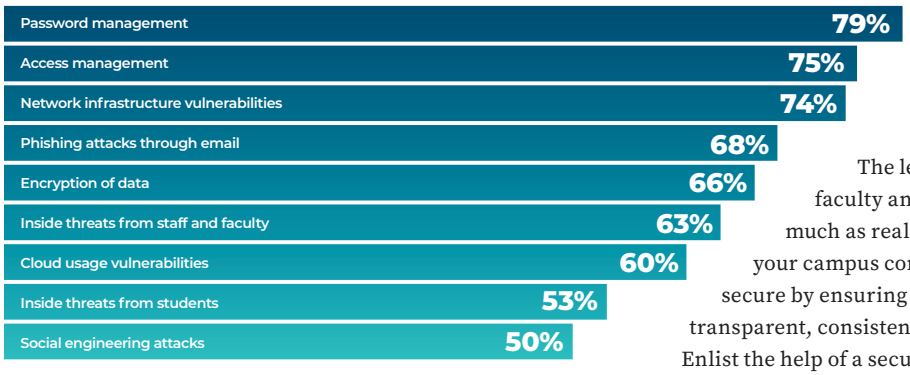
The top security technology colleges and universities use is authentication, cited by almost eight out of 10 respondents (79 percent). This ensures those getting on the campus network are indeed authorized to do so. Device profiling is far less prevalent, cited by just 31 percent of respondents. This automates the process of vetting anything plugged into the network—whether computers, mobile devices, game consoles, printers, or something else—to ensure the endpoint can be identified for authentication and it adheres to security policies.

Two forms of network security protection that have proven valuable—device quarantining and user and entity behavior analytics (UEBA)—have found little traction among campuses surveyed so far. Just 27 percent of respondents say they have an automated way to handle device quarantine—identifying and removing its authentication.

CAMPUS TECHNOLOGY

aruba
a Hewlett Packard Enterprise company

## HOW DOES YOUR CAMPUS ENFORCE IT POLICIES?




Only 20 percent use UEBA, a form of machine learning that detects wayward behaviors among network activities that could signal a security problem. This form of artificial intelligence monitors user and device behavior patterns while looking for anomalous activities that indicate potential threats.

When campuses integrate these two threat management technologies—one to identify the threat and another to sequester the device from the network—security decision-making and remediation is dramatically augmented. This helps the IT organization cut its response time from days or hours to minutes.

### Harden the Campus

Based on the survey findings, Campus Technology encourages institutions to take immediate action in three areas:

- **Develop sensible policies.** And ensure these include every kind of kind of device—computer, phone, or sensor—cropping up on the network and push those policies automatically through a smart security management application. Enlist technology to help IT security staff stay on top of mobility and IoT security.
- **Use pattern-matching software to identify new threats.** Even the simplest sensor does the same thing the same way over and over again. When that device suddenly begins behaving differently from every other device just like it, there's likely a problem.
- **Make security education a part of business-as-usual.** Audit the effectiveness of that training through testing to catch out those who aren't paying attention. Attacks initiated through e-mails and websites continue to harass higher education. If your college or university isn't already requiring regular user training to maintain access to the campus network, you should be doing so.

The level of confidence expressed by faculty and staff often reflect impression as much as reality. Boost the confidence among your campus community that they're safe and secure by ensuring your security efforts are more transparent, consistent, and reliable.

Enlist the help of a security partner with deep experience in both networking and the education segment. Partnerships can help develop an integrated approach to detect potential attacks more quickly and immediately take action to protect data and your network infrastructure.

*Methodology: Findings shared in this executive summary are based on a Campus Technology online survey open for invitation-only response in spring 2018. After filtering for appropriateness of affiliation, job roles and completeness of answers, survey results represent 131 respondents. Roles included: IT leaders (13%), other IT roles (41%) and non-IT staff roles (45%). Affiliations included two-year public institutions (18%), four-year public institutions (42%), four-year not-for-profit institutions (26%), four-year for-profit institutions (5%), trade/vocational institutions (5%) and other (5%). Responses in this executive summary may not total 100% due to rounding.*

## ARUBA NETWORKS' 360 SECURE FABRIC

Aruba Network's suite of security solutions goes beyond the popular ClearPass, its well-known network access control (NAC) and policy management solution for detecting, profiling, and monitoring devices on the network. The company's 360 Secure Fabric builds on the connective strength between networking and security operations. It starts with a secure core. Then there is embedded security built into networking infrastructure—access points, controllers, and switches—at the factory to "wire" in trust among those components (trust that disappears the moment somebody or something attempts to hack the device). When a new computing device, mobile device, or sensor attempts to get onto the network, ClearPass interrogates it to find out what it is and push the appropriate policy. ClearPass integrates with IntroSpect, Aruba's User and Entity Behavior Analytics (UEBA) solution, a machine learning technology that continuously assesses risk based on changing behaviors, whether from a device or a user. It can then make intelligent decisions for how to handle the anomalies. For more information, contact Aruba Networks.