FORTINET

University Networks Face Growing Threats as Attack Surface Expands

Table of Contents

Executive Overview

The typical university's network attack surface is perpetually expanding. Bring-your-own-device (BYOD) policies enable students to bring myriad personal devices to campus each year. Professors are increasingly introducing new learning technologies, and facilities and operations staff are increasing campus efficiency by implementing Internet-of-Things (IoT) equipment.

Meanwhile, universities are generating an ever-increasing volume of data that is highly valuable to hackers. In many cases, this data is siloed, reducing the ability of the central IT team to effectively detect and respond to threats. For all these reasons, higher-education CIOs face security challenges that are expanding as quickly as their network attack surface.

Introduction: Failing to Prioritize Security Is Short-sighted

Serving as CIO for a large university involves juggling many competing priorities. Higher-education budgets are perpetually under pressure, so IT staffing tends to be lean. Still, the CIO is responsible for delivering a high-performance network that provides adequate bandwidth to meet a wide and diverse range of faculty, staff, and student needs.

University IT teams often focus on meeting expectations around network speed, efficiency, and related goals. It can be easy to let amorphous concerns about unseen network security threats take a back seat to the issues that are highly visible campuswide. Such an approach may be shortsighted, however. Consider that Iranian hackers were charged in 2018 with attempting to steal the passwords of hundreds of thousands of U.S. professors.[1] Higher-education networks are targeted by cyber criminals, both foreign and domestic.

CIOs of large universities, in particular, need to revisit their cybersecurity strategies. This eBook outlines three key reasons universities should make a proactive security strategy a top priority.

"Many institutions have extremely limited to no real insight regarding the depth of their security risks in schools, departments, and labs. They can range from exceptionally well-managed servers and devices to those that are compromised or unpatchable."[2] — Bradley C. Wheeler, CIO, Indiana University

01 Universities House Vast Stores of Highly Desirable Data

Like many organizations, universities store valuable personal information on the people who work for them and who use their services. This means large universities collect a great deal of personally identifiable information (PII) on thousands of students, faculty, and staff.

They store financial data for purposes of enrolling students, securing their tuition, tracking student loans, and paying faculty and staff. On-campus health clinics keep sensitive medical information on everyone who uses their services. In addition, data such as students' academic records may be attractive to individuals with nefarious intentions.[3] For identity thieves and other cyber criminals, large universities have a treasure-trove of desirable personal data.

The research that large universities undertake is another highly valuable target for many attackers.[4] A report released in March 2019 found that 27 institutes of higher education in the United States, Canada, and Southeast Asia had recently been attacked by Chinese hackers looking for military secrets.[5] When the U.S. government relies on university CIOs to secure sensitive information, failing to properly protect this data may potentially put military strategy, tactics, or even lives at risk.

"In our current data- and technology-driven world, higher education relies on secure data to support our core teaching, learning, and research missions, and we are entrusted by our students, faculty, researchers, and staff to make certain that data is protected."[6]

“The national state actors might change. But work going on at U.S. institutions will always be of interest to someone.”[7]

— Ravi Pendse, CIO, University of Michigan

The areas that are most likely to interest attackers include scientific, medical, and defense research, as well as studies of public policy matters, nuclear issues, and economic forecasting.[8] Properly securing research data is not only in the university's best interests but often in the national interest as well.

In addition to the sensitive data they store, universities' culture of supporting public access to information can also present challenges.[9] Giving broad access to public data complicates the task of securing data that needs to remain private. Locking down the entire network is not a realistic option.

Effective CIOs and security professionals at large, public universities must find a solution to this challenge, and quickly. Cyberattacks at institutes of higher education are on the rise.[10] One recent study found that in the first half 2018, the education sector suffered 86 data breaches, which accounts for 9% of all the breaches discovered during that period across all industries.[11]

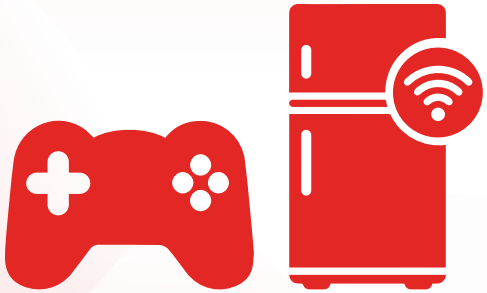
9% of all data breaches in the first half of 2018 were attacks on the education sector.[12]

02 The Number of Devices Accessing University Networks Is Skyrocketing

Knowing that hackers place a high value on some of the data stored on campus can make it even more disconcerting for university CIOs to consider their constantly expanding attack surface. Still, it is necessary to understand the risks.

Every year, schools allow more and more devices to access their networks. This is partly because technology is becoming ubiquitous in learning environments.[13] Many universities have adopted digital textbooks and research tools. Some professors utilize online polls during class to test students' knowledge or opinions. Others use Wi-Fi technologies to digitally take attendance each class period.

Network access for personal use is also on the rise, as students are bringing increasing numbers of their own devices to school. This is especially true for those who live on campus. College students today arrive with an average of eight or nine personal devices.[14] And each of these devices arrives on campus with its own software and security, or lack thereof.



“Gaming consoles, tablets, smart speakers, minifridges that text you when you run out of beer—these are just some of the internet-connected items students are now bringing with them to their residence halls.”[15]

The growing number of devices that university CIOs feel compelled to accommodate creates a growing number of potential access points for attackers.

Allowing in a large number of student devices presents numerous risks to valuable information assets and network resources, yet universities are under pressure to provide open networks and to support BYOD policies. Students and prospective students expect Wi-Fi to be ubiquitous on campus. That is why many universities are investing heavily in installing wireless access points.[16] Ohio State University, for example, recently spent $18.6 million to expand its number of outdoor wireless access points from 32 to 1,000, including bringing Wi-Fi to Ohio Stadium, which seats 100,000.[17]

At the same time, universities are increasingly investing in IoT technologies to improve the efficiency of operations management and make life easier for students and staff.[18] For example, IoT devices can automate the operation of lighting and air-conditioning units. They can also notify maintenance staff that equipment needs servicing before the problem becomes symptomatic. And parking monitors can alert students to available parking spaces. Such IoT devices tend to be considerably less secure, by nature, than the typical server or desktop computer.

Ohio State University recently expanded its number of outdoor wireless access points from 32 to 1,000, including bringing Wi-Fi to Ohio Stadium, which seats 100,000.[19]

A university's reputation depends on its ability to support access to the latest technologies. Achieving cost-efficiency goals may require IT to deploy IoT technologies. Yet, either approach expands the network attack surface.

03 The Expanding Attack Surface Leaves the Network at Risk

Liberal BYOD policies and use of IoT devices can make the entire university network considerably less secure than a corporate network in which only company-issued devices are welcome on the Wi-Fi. The situation becomes worse if CIOs do not fully utilize the security capabilities available to them.

In many next-generation firewalls (NGFWs), features such as intrusion prevention systems (IPS) place a drag on network performance. Students' expectation of high Wi-Fi performance can make university CIOs loath to introduce network latency. CIOs trying to balance network security with optimal network performance may be tempted to turn off certain features of their NGFWs and other devices. This may create security gaps at the network perimeter. Attackers who find those gaps may intend to move laterally once inside the network to access the university's valuable data stores.

Attacks on university networks are more frequently perpetrated by students than by organized criminal hacking groups.[20]

The attacks are not all coming from the outside. Students may be looking for personal advantage, such as delaying a test, manipulating the registration process, or acting out in aggression. One study found that attacks on university networks are more frequently perpetrated by students than by organized criminal hacking groups.[21]

When an attack does happen, universities may lack the transparent visibility into security that they need to respond effectively. It is common for sensitive data to be siloed in university departments. On-premises research facilities housing critical information may exist entirely outside the CIO's purview.

Cloud-based solutions generally also reside outside the CIO's jurisdiction. Use of cloud-based applications and data storage solutions are ubiquitous on university campuses. They are often deployed independently within university departments, without the input or security oversight of the school's central IT function. Cloud solutions frequently store valuable and vulnerable information, so they require protection equal to the core university network, which can create a dilemma for the CIO.

A network with data silos—whether on-premises, in the cloud, or both—reduces the ability of the CIO and the central IT function to recognize developing threats and respond rapidly if a breach occurs. These challenges are exacerbated when the university relies on security solutions that fail to communicate with one another. Gaining a campus-level view of security activities may require security staff to cobble together information from a variety of systems and dashboards, which necessarily reduces visibility and slows threat response. Data silos also undermine attempts to build a universitywide security posture.

Conclusion: Security Needs to Be a Top Priority

Maintaining a reputation as a leading-edge institution requires protecting all the data with which the university is entrusted. An ever-expanding attack surface, data silos, and security gaps combine to reduce the effectiveness of the security infrastructure in the typical university. These are challenges that CIOs at large universities must overcome. The data housed on their campuses is too important, and too valuable to prospective attackers, for CIOs to accept a suboptimal approach to network security.

"Security breaches bring with them the fear of reputational risk, unknown financial costs, and concerns about service disruptions. Information security has become a business challenge [for institutions of higher education], not just a technology issue."[22]

[1] Lindsay McKenzie, "On Red Alert," Inside Higher Ed, March 6, 2019.

[2] Ibid.

[3] Abhay Raman, et al., "Cybersecurity in higher education: the changing threat landscape," EY Canada, August 25, 2016.

[4] "Strategies for Research Cybersecurity and Compliance from the Lab," Internet2 Global Summit, March 8, 2019.

[5] Lindsay McKenzie, "On Red Alert," Inside Higher Ed, March 6, 2019.

[6] "Technology in Higher Education: Information Security Leadership," EDUCAUSE, 2016.

[7] Lindsay McKenzie, "At What Cost Wi-Fi?," Inside Higher Ed, April 17, 2018.

[8] Lindsay McKenzie, "On Red Alert," Inside Higher Ed, March 6, 2019.

[9] Brian Basgen and Tammy Clark, "Leading an Effective Briefing with Board Executives about Information Security," EDUCAUSE, January 11, 2016.

[10] Abhay Raman, et al., "Cybersecurity in higher education: the changing threat landscape," EY Canada, August 25, 2016.

[11] "The Reality of Data Breaches," Gemalto, 2018.

[12] Ibid.

[13] Lindsay McKenzie, "At What Cost Wi-Fi?," Inside Higher Ed, April 17, 2018.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] "Ohio State University trustees approve contract with Apple to launch Digital Flagship initiative," Ohio State News, April 6, 2018.

[18] D. Christopher Brooks and Mark McCormack, "Higher Education's 2019 Trend Watch and Top 10 Strategic Technologies," EDUCAUSE, March 14, 2019.

[19] Naveen Goud, "Students are responsible for cyber attacks on Universities and Colleges," Cybersecurity Insiders, accessed July 2, 2019.

[20] "Ohio State University trustees approve contract with Apple to launch Digital Flagship initiative," Ohio State News, April 6, 2018.

[21] Naveen Goud, "Students are responsible for cyber attacks on Universities and Colleges," Cybersecurity Insiders, accessed July 2, 2019.

[22] "Technology in Higher Education: Information Security Leadership," EDUCAUSE, 2016.

FORTINET

www.fortinet.com

407931-0-0-EN

July 2, 2019 10:22 PM

eb-university-networks-growing-threats