WHITE PAPER

Unique Cybersecurity Considerations for Community Colleges

It's no surprise that higher educational institutions are prime targets for cybercriminals. According to the 2022 Verizon Data Breach Investigations Report, system intrusion, basic web application attacks, and miscellaneous errors account for 80% of breaches among educational institutions.[1] The same report notes that the bad actors who carry out these attacks are overwhelmingly motivated by financial gain (95%).[2] As more educational institutions move more learning resources online, these assets offer a gold mine of personally identifiable information (PII) to cybercriminals.

All educational institutions undoubtedly need a strong security posture to protect their campuses and preserve the availability and confidentiality of sensitive information. However, community and technical colleges have several unique needs regarding cybersecurity, ranging from staffing challenges to the proliferation of students and faculty bringing their own devices to the school's network.

The education sector experienced a dramatic increase in ransomware attacks (30%) this past year.[3]

Staffing Challenges and the Ongoing Competition for Cybersecurity Talent

Security and IT staffing is a common challenge for community colleges. The Leadership Board for CIOs in Higher Education found that while nearly two in three institutions worldwide have hired CISOs—a 10% increase from a decade ago—the decision to hire or not hire usually is based upon the complexity of the organization.[4] The same study noted that large community colleges and systems are more likely to hire CISOs than smaller schools.[5] "Generally, the more complex an institution is, the more likely it is that they'll have someone in that role," says Michael Zastrocky, Executive Director of the Leadership Board of CIOs in Higher Education.[6] Additionally, retirements and resignations among community college faculty and staff members are occurring more frequently post-pandemic than in years past.[7]

Many community colleges cannot afford to hire a security leader from outside of higher education, and smaller colleges are less likely to have someone at the management level who does a CISO's job. Often the IT Director will task someone within the IT office to run security and manage other IT-focused duties. Others are creating more non-CISO roles or merging the scope of supervisory security duties into a shared CISO role with other similar colleges in their area. Some of the larger community college districts with functional CISOs are providing advisory services to other institutions in their geographical area.

IT leaders at community and technical colleges are increasingly finding creative solutions to help them create or develop strong cybersecurity practices as well as attract and retain security talent. For example, in Yakima, Washington, at Yakima Valley College, the IT Director is working to establish a cybersecurity-focused capability within the IT team that will address ongoing security operations and work toward a more secure campus network. He is now looking for the right talent and exploring unique staffing strategies, including offering additional work and study opportunities for undergraduate and graduate students from area universities, as well as providing research and service projects to first and second-year students attending classes at the college.

Five Essential Strategies for Strengthening Security Among Community Colleges

While talent recruitment and retention are ongoing concerns for many community and technical colleges, the more pressing issue is whether an adequate cybersecurity strategy and program lays the groundwork for a risk-based approach to securing that campus. Yet even faced with resource constraints, IT leaders can still take simple steps toward strengthening their respective institution's security posture.

These are the most important aspects to consider when creating or enhancing a community college's security program:

1. **Look for integrated security solutions:** The community college attack surface is rapidly expanding for many reasons, including a geographically dispersed student population, multiple campuses, and the need for around-the-clock connectivity. The first step in securing the community college network is to find a platform that features seamless integration for all security components and rapid detection and remediation of security events. Next-generation firewalls with threat-intelligence sharing are the heart of effective institutional security—they provide a high level of security while maintaining reliable network performance.

2. **Prioritize secure remote access:** Mobile device proliferation and the advent of the Internet of Things (IoT) mean that clever attackers have a growing number of possible entry points into a school's network. IT teams need solutions that provide visibility and control for all devices attached to the network. Endpoint protection against malicious threats extends effective security to the individual device. Access management, including two-factor and one-time password authentication, can offer an additional layer of protection.
3. **Take advantage of artificial intelligence (AI) and sandboxing:** Advanced exploits penetrate perimeter defenses and move through the network to wreak havoc and steal valuable information. That's why community colleges need solutions with intent-based segmentation to limit lateral threat movement, as well as sandboxing capabilities to isolate unknown threats. Top-tier security solutions use AI and machine learning (ML) to extract actionable insights and facilitate post-breach forensics.
4. **Automate operations and response actions when possible:** The complexity of legacy systems and advanced threats hinder staff productivity and lengthen the time required to resolve issues, all of which can easily strain under-resourced IT teams. To meet this challenge, community colleges need single-pane-of-glass management, zero-touch provisioning, and orchestrated, automated responses to mitigate threats in real time. These capabilities meet the needs of lean teams by enhancing productivity and speeding threat mitigation.
5. **Centralize or consolidate threat intelligence:** Obtaining top-quality threat intelligence services can help community colleges keep ahead of bad actors and other common threats impacting the education sector.

Many community colleges across the nation are enhancing their cybersecurity curriculum and, as a result, increasing their enrollment.

When it comes to community college cybersecurity, the whole must be greater than the sum of the parts, and the most effective way to achieve this is to consolidate security technology and ideally converge those tools into a single operating platform. The convergence of security technologies is particularly helpful for institutions such as community colleges that are often resource constrained, offering lower total cost of ownership, reduced operating expenses, stronger security for remote and mobile devices, and faster breach detection and mitigation.

Community Colleges Are Training Grounds for the Next Generation of Cybersecurity Professionals

Beyond the obvious need to keep the campus, its students, and faculty cyber safe, a strong cybersecurity posture is essential for community colleges for another reason: Many of these institutions offer degree programs for learners interested in entering the cybersecurity industry. To continue growing these programs and attracting new students, community colleges must "walk the walk" when it comes to security.

Many community colleges across the nation are enhancing their cybersecurity curriculum and, as a result, increasing their enrollment. For example, when Whatcom Community College (WCC) in Bellingham, Washington, began offering cybersecurity courses, the school's enrollment jumped by 17% in just a year.[8] The school was also awarded a $7.5M grant—awarded to institutions that "develop innovative approaches in educating highly skilled technicians for in-demand industries—by the National Science Foundation (NSF) with the goal of growing its cybersecurity program.[9]

Another example comes from Edmonds College, which has offered cybersecurity and digital forensics courses since 1999, making it one of the longest-running community college cybersecurity programs in the nation. The school was recently awarded a $1.5M grant from the Washington State Board for Community and Technical Colleges to enhance its security education and training programs.[10]

Private-sector organizations also frequently partner with community colleges to train and recruit skilled cybersecurity professionals. There are numerous examples of these public-private partnerships. LaGuardia Community College in New York City works with Mastercard to offer on-the-job security training.[11] MassBay Community College located near Boston, Massachusetts, has a Center for Cybersecurity Education that offers students security-related projects and internships with local industry partners.[12] And in November 2021, Microsoft announced that the company would provide cybersecurity instructional training to faculty at 150 community colleges around the country, as well as scholarships and other financial support to 25,000 community college students pursuing cybersecurity education.[13]

The Most Important Step Community Colleges Can Take to Secure Their Networks

Community colleges have a sizeable job when it comes to security. Small IT teams need to employ successful physical and cybersecurity strategies to keep the campus, students, and faculty safe, recruit and retain security talent, and even use these efforts and "lessons learned" to educate the next generation of cybersecurity professionals.

While IT leaders at community colleges inevitably wear many hats, there are simple steps to take now that can increase efficiencies and improve effectiveness when it comes to security. One of the most advantageous steps a community college can take is to consolidate its security technologies into a single platform and reduce the amount of individual use cases or best-of-breed point products that are not designed to work together. This allows for much tighter integration, increased automation, and a more rapid, coordinated, and effective response to threats across the campus network.

[1] "2022 Verizon Data Breach Investigations Report," Verizon, May 24, 2022.

[2] Ibid.

[3] Ibid.

[4] "Managing a Changing Threat," The Chronicle of Higher Education, 2020.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Smalley, Suzanne, "Corporations, Community Colleges Partner on Cybersecurity Training," Inside Higher Ed, November 4, 2021.

[9] Ibid.

[10] "Edmonds College Receives $1.5 Million Cybersecurity Grant," Edmonds College, August 29, 2022.

[11] Smalley, Suzanne, "Corporations, Community Colleges Partner on Cybersecurity Training," Inside Higher Ed, November 4, 2021.

[12] Ibid.

[13] Ibid.

FORTINET®

www.fortinet.com

January 4, 2023 10:00 AM

1853793-0-0-EN