Campus Report Cybersecurity

Making the Case for Your Cybersecurity Strategy

Here's how to help university administration understand what's at stake and why it's essential they support your security recommendations.

PRODUCED BY: CAMPUS TECHNOLOGY

SPONSORED BY: Spectrum ENTERPRISE

BLACKBAUD, PROCTOR U, SOLARWINDS. You recognize them all for what the companies have in common: Each has suffered cybersecurity break-ins, driving their customers — including numerous institutions of higher education — into maelstroms of breach disclosure, victim restitution and negative headlines. It's possible that people and systems within your own school may have been affected.

Yet, in spite of seemingly unending security problems, you may still find you still have to lobby hard for every dollar and resource needed to put up a solid security front that will keep the bad actors out.

Given the "when" not "if" nature of cybersecurity incidents, college executives and administrators need to acknowledge the importance of the topic and invite the experts in regularly to educate them on what's to be done.

> Getting a "seat at the table" requires development of an information security approach that supports the evolution and transformation of your institution as it grapples with the return to campus, following more than a year of seismic change. This white paper lays out the talking points for you to help your administration understand what's at stake and why it's essential for them to support your work in protecting campus data and systems.

The Pandemic Cybersecurity Fallout

STEP ONE, PRESENT THE PROBLEM. In 2019, the whole education sector suffered 819 incidents — more than a quarter involving confirmed data disclosures, according to a 2020 data breach investigations research project.[1] But by every measure, the pandemic has only accelerated the number of attacks on education. One analysis tallied a 400 percent rise in the number of attacks to educational organizations between the middle of March 2020, when remote learning surfaced as a response to COVID-19, and the end of August 2020.[2] Compare that to an increase in attacks across all industries of about 50 percent.

Why did education, and higher ed specifically, become so alluring? Some drivers have always existed:

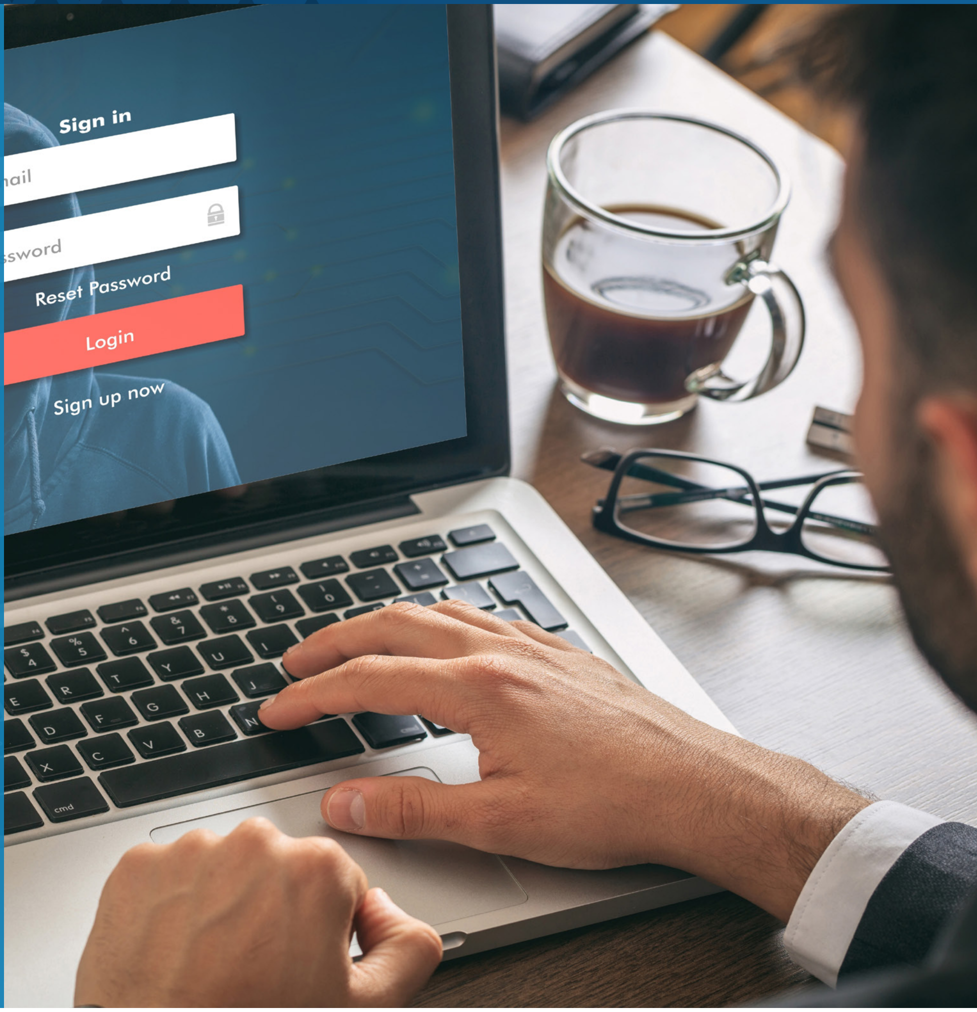
- **Universities hold valuable data about people and research, making for a rich bounty.**
- **The high-speed connectivity and roomy IT infrastructure available on many campuses pose an enticement for criminals seeking free rent to house their bots and other malware and to perform cryptocurrency mining under the radar.[3]**
- **There's a constant high-wire struggle that goes on between the dueling goals of promoting openness, sharing and academic freedom and locking down the network to prevent easy break-ins.**
- **Like any large, complicated organization, institutions turn to a mix of third-party vendors for certain essential services leaving potential gaps.**
- **Users tend to have varying levels of knowledge about cybersecurity, making it more likely that spear phishing exploits will eventually succeed.**

But the pandemic posed additional temptations because, as one reporter noted,[4] "there are, after all, few things a cybercriminal appreciates more than the opportunity to capitalize on chaos":

- **The perimeter was no longer defined by the borders of the campus. People worked from *wherever*, using devices not under IT control. Each individual's own computing practices became a ripe new potential attack vector.**

During the pandemic, the perimeter was no longer defined by the borders of the campus. People worked from *wherever,* using devices not under IT control. Each individual's own computing practices became a ripe new potential attack vector.

Spoofing became amazingly lifelike, with COVID-19 and relief funding specific phishing exploits persuading users to hand over credentials through fake websites impersonating the official ones for campus offices, local public health operations and agencies, including the Centers for Disease Control.[5]



- **Faculty increased the use of cloud services to brew a winning mix of engaging learning activities. Given the need to quickly stand up remote learning, the usual vetting process for new technologies may have been relaxed and skipped.**
- **Spoofing became amazingly lifelike, with COVID-19 and relief funding specific phishing exploits persuading users to hand over credentials through fake websites impersonating the official ones for campus offices, local public health operations and agencies, including the Centers for Disease Control.[5]**
- **People were just plain distracted with all the changes to daily life that the pandemic brought. As a recent *Harvard Business Review* article pointed out, "Social distractions have long been a primary threat, and the success rate with attacks is higher when everyone's attention is diverted elsewhere."[6]**

The rise in security incidents that hit their targets could also be said to have been boosted by an overworked IT organization, which had to deal with its own challenges:

- **Being pulled in multiple directions to deal with emergency response.**
- **Working with reduced numbers, especially in those teams that relied on the help of student workers, and from their own remote locations.**
- **Sensing that faculty were already overloaded and didn't need to worry about security training or pop phishing quizzes on top of everything else.**
- **Facing contractions in funding for projects, based on expected institutional shortfalls.**

Heading into the new year, the same obstacles remain. Although colleges and universities are beginning to predict a return to normalcy for fall 2021, especially with broad access to vaccines on the horizon, we could see the same kind of upending of plans that hit last fall, when, in spite of best intentions to deliver in-person instruction, nearly half of institutions (48 percent) eventually chose to go fully or primarily online and almost a quarter (23 percent) adopted hybrid learning.[7]

The Costs of a Break-In

ONCE YOU'VE LAID OUT THE REASONS FOR the heightened security concerns, it's time to communicate the costs of getting security protection wrong.

A biggie is the expense of mitigating a data breach. In the latest analysis by the Ponemon Institute, the average cost for an education breach in 2020 was $3.9 million worldwide. The cost per record was $3.90, covering expenses related to forensics work, escalation, notification, response and lost business.[8]

It's worth noting that, according to the same report, data breaches in the United States tend to be considerably pricier than those in other countries — nearly twice as high, for example, as those in Canada and more than twice as high than the ones in the United Kingdom.

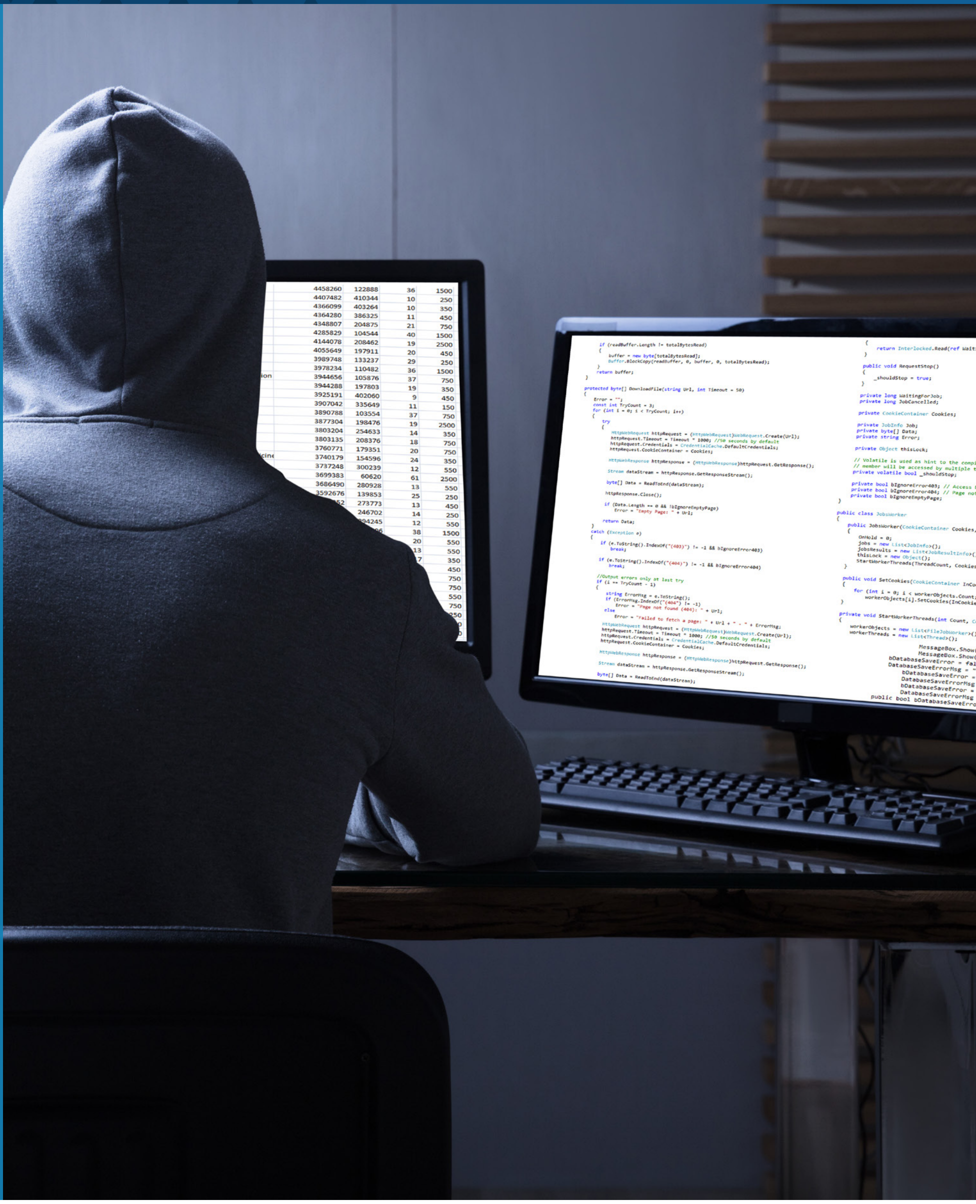
Also, cost is influenced by the type of break-in, Ponemon found. Those caused by malicious attacks (the ones made possible primarily through compromised credentials, cloud misconfiguration or a third-party software vulnerability), which make up nearly half of breaches in education (48 percent), cost more than those generated through system glitches (26 percent) or human error (26 percent).

While there are plenty of factors that increase the expense of dealing with data breaches, such as compliance failures and security skills shortages, according to the report, other elements reduce the cost. These include the ones you could probably predict — incident response testing, employee training, the use of ID theft protection — but also some you might not think of: having board involvement; having cyber insurance; and having the role of a chief information security officer to oversee the operation.

While the theft of personally identifiable information (PII) is certainly a draw for bad actors, it's not the only kind of data at stake in higher ed. There's valuable research and intellectual property they're on the hunt for. Besides the cost of mitigation tied to the loss of PII, today's breaches also frequently arrive with the extra sting of ransomware, which has taken on the form of what some security experts refer to as "double extortion."

> Besides the cost of mitigation tied to the loss of PII, today's breaches also frequently arrive with the extra sting of ransomware, which has taken on the form of what some security experts refer to as "double extortion."

Even when a payment is made and access to the data is returned to its rightful owners, that may just be the beginning of the extortion. Increasingly, additional demands are made for more money to prevent publication of the stolen data online.



First, your institution has to decide under a tight deadline whether to pay a ransom and trust that the criminals will do the right thing by returning the data. Last June, the University of California, San Francisco paid $1.1 million to cyber attackers who had stolen data.[9] In August, the University of Utah acknowledged that it had paid $457,000.[10]

But even when a payment is made and access to the data is returned to its rightful owners, that may just be the beginning of the extortion. Increasingly, additional demands are made for more money to prevent publication of the stolen data online.

And it gets murkier. As one security expert explained, the use of “ransomware as a service,” purchased on the deep web, allows for the creation of “ransomware cocktails out of bits and pieces.” Whoever pits the ransomware against a given organization “may not have all the keys to unlock it back to you.” They lose control, and so do you.[11]

The remedy to the old-fashioned form of ransomware, as we’ve all been told, is a backup implemented in such a way that it’s immune from change, including those introduced by malware. The institution can rebuild the data center and replace the infected files with untainted versions. Yes, it’s time-consuming and can rarely 100-percent mirror what was there before the attack. But when you also face the possibility of your institutional data being posted online and sold and resold to the highest bidders, backup by itself is no longer an adequate response.

Setting Up Information Security the Right Way

NOW IT'S TIME TO PROPOSE A SOLUTION, covering aspects that are already in place and new ones to add. The message is that you want to keep the malware out in the first place. You don't need to get overly technical in your explanation. Keep it simple and use two concepts to describe your basic philosophy:

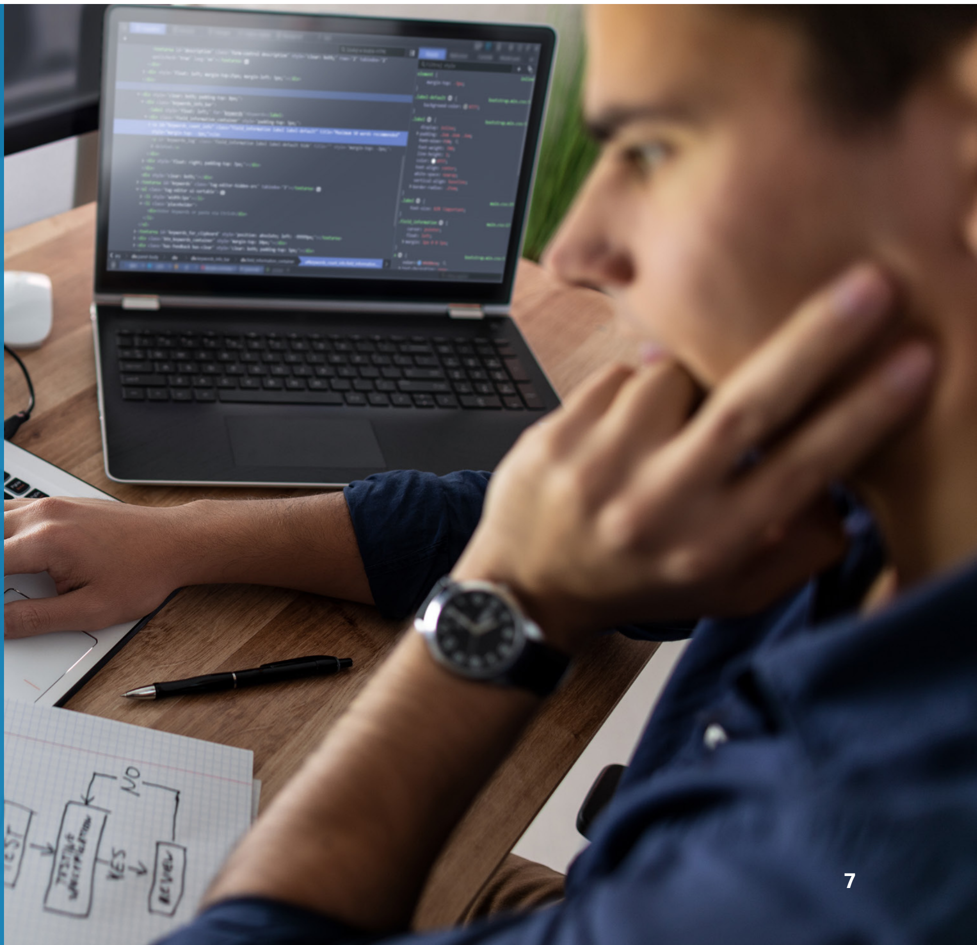
- ***Zero trust:*** **The network makes sure users are who they say they are, that they're working on a device that meets the threshold for access and that both user and device are located where they're expected to be.**
- ***Least privilege:*** **Users and systems are granted access only to what they need through network segmentation. Just as users are locked out of places they don't belong, so are the hackers.**

Supporting these two goals are activities including:

- **Doing automated patching of campus systems.**
- **Providing antivirus that's freely and abundantly available and monitoring it centrally.**
- **Enforcing user authentication and password practices that are prescriptive.**
- **Using effective data management and backup.**
- **Rooting out legacy systems that could put the whole network at risk.**
- **Performing periodic data recovery tests.**
- **Promoting user training and phishing tests.**

But other practices are making headway too that can give colleges and universities an edge in addressing cyber risk:

Now it's time to propose a solution, covering aspects that are already in place and new ones to add. The message is that you want to keep the malware out in the first place.



The right managed security services provider maintains a wide bench of specialists, is adept at security technologies and brings cross-pollination to the cybersecurity challenge. In addition, just as with the adoption of cloud applications, the arrangement incorporates scalability to address shifting needs.

Use of modern-day honeypots

As IDG recently described this practice, "deception technology" draws intruders to "mock networks" that serve as decoys, offering up fake password lists, made-up databases and false access — with the goal of alerting IT when the bait is taken. The challenge, as the IDG report explained, is that it's resource-intensive: Organizations must be prepared "to deploy, support, refresh and respond to deception alerts without hiring an army."[12]

Use of third-party assessment

Vendors can bring an objective viewpoint to checking a school's security posture in specific areas such as network security, IT controls and risk assessment; they can also perform penetration testing. While plenty of top-notch companies provide this service, so does Research & Education Networks Information Sharing & Analysis Center (REN-ISAC), with its "cybersecurity peer assessment service." REN-ISAC is a "trust community" specifically for higher ed and research institutions that promotes cybersecurity operational protections, maintains a threat intelligence repository, produces a "daily watch report" and delivers webinars and training on security protection and response.[13]

Use of managed security services

For campuses that lack sufficient internal expertise in specific areas, managed security services solve multiple problems. The right provider maintains a wide bench of specialists, is adept at security technologies and brings cross-pollination to the cybersecurity challenge. In addition, just as with the adoption of cloud applications, the arrangement incorporates scalability to address shifting needs.

The Ask: Where to Begin

THE "ASK" — what you hope to get out of your discussions with university leadership regarding security — needs to focus on the highest risks and greatest needs. Here are two current priorities we'd advise emphasizing:

Protecting the extended network

The network now has a perimeter as large as the reach of every one of your users' devices and the networks they use to access college resources. It encompasses people, their devices and their data, all of which need to go through authentication every time they re-enter the network. It should cover cloud apps, which have gained dramatic pickup in the last year. And it needs to include all the VPNs, access technology, random ports and other routes that could provide hidden tunnels to those trying to break in.

Nailing down data priorities

Some data are more important than others. Archives of social media posts might be important for settling a lawsuit down the road, but theft of PII or new research findings leading to scientific breakthroughs can have immediate and momentous outcomes. Institutional leaders need to identify the most valuable files and where they are, so that IT can figure out how those are currently being protected and backed up, who has access and what further actions should be taken.

Emerging transformed

A recent report from EDUCAUSE, sponsored by Spectrum Enterprise, described three scenarios for how the schools that make up its membership will come out of the pandemic: restored, evolved or transformed.[14] The first is to resume status quo; the second is to adapt to a new normal for students; and the third is to emerge stronger than before and ready to tackle nothing less than the makeover of education to be student-centered.

Cybersecurity takes a different form for each of these outcomes. In the "restore" mode, there's a need to be tactical and budget-conscious because the very survival of the institution is at stake.

Some data are more important than others. Institutional leaders need to identify the most valuable files and where they are, so that IT can figure out how those are currently being protected and backed up, who has access and what further actions should be taken.

The "evolved" campus takes a giant leap forward by developing a strategy that expands the security perimeter to include remote learning and remote work as well, with a mission of protecting students, faculty and staff wherever they're located.

The "evolved" campus takes a giant leap forward by developing a strategy that expands the security perimeter to include remote learning and remote work as well, with a mission of protecting students, faculty and staff wherever they're located. After all, many innovations brought in with the pandemic could remain in place as permanent fixtures.

For the "transformed" school, information security serves behind the scenes as a foundation supporting every other theme: institutional culture, technology alignment, technology strategy and so on. Without a robust cybersecurity strategy that takes into account all of the changes higher ed is undergoing right now, transformation efforts could easily be stopped in their tracks, akin to the internet going down.

Now more than ever IT needs to remain optimistic, motivated and proactive in taking the steps that will help the school stay secure and protected. You're also your institution's best hope for helping institutional leadership understand what the job requires.

ABOUT SPECTRUM ENTERPRISE

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable fiber technology solutions serving America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, and Voice and TV solutions. Spectrum Enterprise's industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs.

More information about Spectrum Enterprise can be found at ***enterprise.spectrum.com/highered***

Spectrum ENTERPRISE

[1] **"2020 Data Breach Investigations Report,"** Verizon, 2020.

[2] **"Not for higher education: cybercriminals target academic & research institutions across the world,"** Check Point, 2020.

[3] John Thomas, **"Understanding Cybersecurity, for Finance Professionals,"** Sikich, May 2019.

[4] Amelia Pang and Lauren Glenn Manfuso, **"COVID-19 Brings Cybersecurity Risks and Opportunities,"** EdTech, Sep. 30, 2020.

[5] Derek Johnson, **"CDC, IRS and other federal sites spoofed in global phishing scams,"** FCW, May 18, 2020.

[6] Lakshmi Hanspal, **"Cybersecurity Is Not (Just) a Tech Problem,"** Harvard Business Review, Jan. 6, 2021

[7] **The College Crisis Initiative@Davidson College,** undated.

[8] **"2020 Cost of a Data Breach Report,"** Ponemon Institute and IBM, 2020.

[9] **"Update on IT Security Incident at UCSF,"** University of California San Francisco, Jun. 26, 2020.

[10] **"University of Utah update on data security incident,"** University of Utah, Aug. 20, 2020.

[11] Amelia Pang, **"Q&A: Amid New Risks, Colleges Must Prioritize Valued Assets,"** Jan. 8, 2021.

[12] **"2020 Security Priorities Study,"** IDG, Nov. 19, 2020.

[13] **REN-ISAC**, undated.

[14] **"Top IT Issues, 2021: Emerging from the Pandemic,"** Educause and Spectrum Enterprise, Nov. 2, 2020.