




# Three Cybersecurity Gaps Inadvertently Leaving Your University Vulnerable (and How to Fix Them)





*Higher education institutions were pushed to their limits at the start of the pandemic as they pivoted almost overnight to deliver education in a remote environment.*

IT departments rallied to reengineer crucial processes to allow universities to continue to serve their constituents. According to [a report](#) by The Chronicle of Higher Education, 63% of schools said the pandemic sped their adoption of cloud services.

**But did they do enough to enhance cybersecurity?**

A survey of more than 130 leaders from higher ed institutions by Arctic Wolf and Higher Ed Dive's studioID found that many universities might not be adequately prepared for increasingly sophisticated cyber threats.

The survey responses identified three key gaps that universities must address to protect their infrastructure and data as their reliance on technology increases.

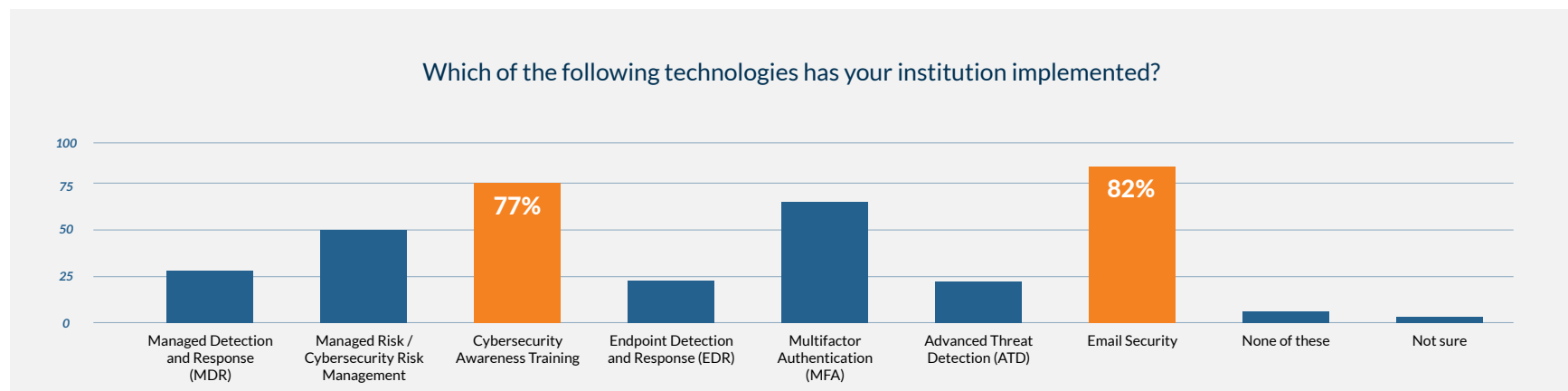


of schools said the pandemic sped their adoption of cloud services.



**GAP 1:**

**While many higher education institutions say they have invested in adequate security, in reality they may just be “checking the box.”**



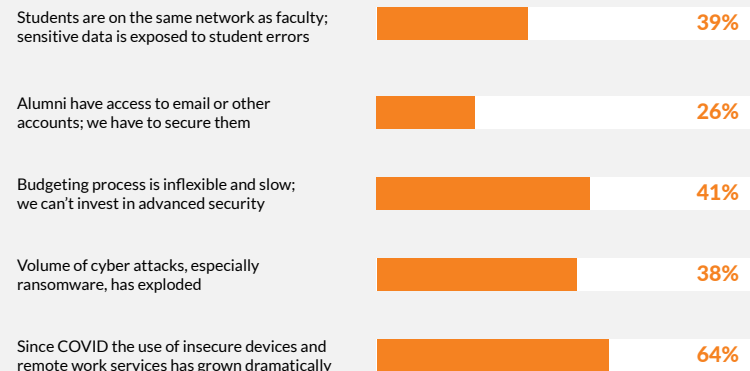
Looking at the investments that most higher education institutions have made, they have covered enough basics to accurately tell a risk manager they have a cybersecurity plan. However, the most commonly cited activities are limited in scope: For example, the **top two interventions** they have **implemented are email security (82%)** and conducting **cybersecurity-awareness training (77%)**.

Far fewer have invested in detection and response, such as endpoint detection and response and advanced threat detection, which were each reported by just 22% of higher education executives.



*Measuring information security success in dollars and cents saved undercuts the real value of cybersecurity. Just as institutions would never forgo adequate insurance, cybersecurity investments serve a similarly necessary proactive, protective function.*

### Which of the following security challenges, if any, does your institution face?



Two likely factors are at play. The first relates to a lack of funds: **Forty-one percent noted that inflexible and slow budgeting makes it challenging to invest in advanced security.** To be sure, most universities have a dwindling budget for new investments. Educause's report, [Top IT Issues, 2021: Emerging from the Pandemic](#), noted: "Any investments or initiatives to introduce new technologies or improve business processes will have to demonstrate rapid and sizable savings."

And yet measuring information security success in dollars and cents saved undercuts the real value of cybersecurity. Just as institutions would never forgo adequate insurance, cybersecurity investments serve a similarly necessary proactive, protective function.



In addition, many institutions may be unaware of what's available for funding; for example, some may be eligible for COVID-19 relief grants. They may need to think outside the box to identify funding sources, because higher education will continue to be a higher target for breaches.

There's a second element that could lead to a hesitation to adopt more effective cybersecurity detection, even among those who realize a gap. Many schools face a conundrum in determining how to address their security deficit — what you might consider a “chicken and egg” issue.

They might understand they lack the right tools and capabilities but don't know how to rectify it. And they might know they need to hire but are challenged with aligning needs that are yet to be defined with a new role. Then, even once they bring in someone with the appropriate level of expertise to identify necessary tools, capabilities, and processes, much of their subsequent work may well be focused on managing alerts and day-to-day security operations. Being forced to focus on alert triage, rather than more challenging and strategic work, security professionals may feel their career growth limited and experience burnout. This, in turn, presents a barrier for organizations to retain top-level talent.

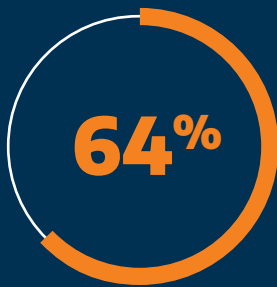
**The upshot? Colleges fail to implement a more holistic solution that offers meaningful cybersecurity.**





## GAP 2:

# Higher education institutions underestimate the threat of a ransomware attack.



Since COVID the use of insecure devices and remote work services has grown dramatically.

We're accustomed to reading about high-profile cyber attacks, often targeting financial institutions, large retail chains, or health care operations, but universities might be inadvertently downplaying their risk. In fact, education is a perennial target of data breaches, and colleges account for two-thirds of attacks on education. This prompted the FBI's Cyber Division to issue an advisory notice warning of a ransomware scam targeting education institutions in March 2021.

Colleges and universities are ripe targets for ransomware and cybercrime for a number of reasons. First, they hold vast amounts of personally identifiable information, given their large student populations, combined with alumni and employee data. Think about the extensive trove of valuable information they collect: financial data, bank account information, Social Security numbers, birthdates, driver's license and other government-issued ID numbers – all data that has immense value to hackers on the dark web as they work to identity theft scams.

Most universities also have proprietary research information, which has economic worth in and of itself. Consider the case of the University of California San Francisco (UCSF), which had been working on a COVID-19 vaccine when it was hit with ransomware demanding a \$3 million payout in June 2020. After several days of negotiations, UCSF paid the hackers \$1.14 million in return for the data they had already obtained and a tool to unlock the data they

had encrypted. Of course, costly as it was, that sum was probably far lower than it would have cost to recover the data any other way.

And finally, institutions tend to have a low tolerance for downtime. That means that in their desire to get back online quickly, they may be more susceptible to paying the ransom to get their functionality back.

That might be especially true when attackers focus on moments when institutions are particularly vulnerable or when they can cause maximum disruption, such as during class registration. For example, in fall 2021, Howard University suffered a ransomware attack at a particularly sensitive time: The attackers exploited the confluence of the end of registration, the start of a new term and a holiday

weekend to hit the university when it was vulnerable and when they needed to be sure systems were running for a smooth transition.

However, despite the prevalence and potentially debilitating effects of cyber attacks, higher ed leaders don't prioritize this risk as highly as others. In the survey, **64% cited the dramatic growth in the use of unsecured devices and remote work services since COVID-19 began as the top security challenge their institutions face.** Only 38% of respondents recognized that the increase in risks was, in part, due to the drastic increase in the volume of cyber attacks, especially ransomware.

Unfortunately, many universities may be unaware of how much sensitive information they have or the damage that can be done until it's too late.



### GAP 3:

## Higher education institutions overestimate their ability to recover from a ransomware attack.



Ransomware attack? A relatively easy fix, said nearly 40% of higher education leaders, who said they could recover from a successful ransomware attack in under two days.

One recent report estimated organizations experience an average of 21 days of downtime from when a breach is initially

discovered until full remediation, which is especially challenging for colleges and universities, when every day of a semester counts. Howard University officials would concur with the magnitude of an attack; soon after its ransomware incident, one warned in a news report that remediation would be a “long haul.”





*In the survey conducted by Arctic Wolf and studioID, **19% of respondents said it could take up to six days to resume functionality.** While that might sound like a manageable duration, even one week is a huge disruptor in a traditional 12-week semester.*

In the survey conducted by Arctic Wolf and studioID, 19% of respondents said it could take up to six days to resume functionality. While that might sound like a manageable duration, even one week is a huge disruptor in a traditional 12-week semester.

Some of the issue could lie with semantics. When leaders estimate a recovery timeline for a ransomware attack, they need to consider the whole universe of ongoing effects from a serious cyber attack such as ransomware.

For example, leaders may consider recovery in the most basic of terms, referring to the point when compromised networks and devices are back up and functioning. But that fails to take into account lingering effects and work overhang associated with the disruption, or more serious consequences that could arise because of the sensitive information universities hold.

The waterfall effect can be significant, given that higher education institutions are highly distributed environments technologically. They host a variety of complicated networks, with a lot of people coming and going. And they use a breadth of different systems that hold financial information, personal information, health data, athletic program data, admissions information, and academic records, just to name a few, with all the different details each of those categories encompasses.

While information might be compromised, other data just might be gone. But unrecoverable data can be a serious ongoing problem. For example, how might a university deal with the fact that transcripts from 1980 to 2000 can no longer be requested or that an entire semester's work has gone missing?

Considering this wide array of long-lasting effects, it's quite possible IT leaders with optimistic estimates of their ransomware recovery timelines might not have considered all these aspects, and it certainly points to the need for comprehensive cybersecurity. They may fail to grasp the extent of the disruption if these systems and data were no longer available.





## Is Your Institution Making the Grade on Cybersecurity?

According to IBM's Cost of a Data Breach Report 2021, the average cost of a data breach is estimated at \$3.86 million, making an investment in proactive, ongoing cybersecurity a wise one.

While universities may lack the budget and personnel to handle these issues holistically, turning to a vendor can allow them to operate more securely, which protects both their data — and their reputation.

That's where a partner like Arctic Wolf can come in with a solution that combines a proprietary security operations platform with the people and processes necessary to deliver security outcomes at a technical level that's simultaneously personal.

With visibility into both on-premise and cloud networks, its professionals can help mitigate and manage risks through a solid understanding of the vulnerabilities higher education institutions have and the threats they face.

Curious how Arctic Wolf's approach to security operations would provide a line of sight to everything that's going on in your university to help you proactively manage risks and quickly remediate threats?

Visit [www.arcticwolf.com](http://www.arcticwolf.com) today.



Arctic Wolf® is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit [arcticwolf.com](https://arcticwolf.com)



# studio / ID

## BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

[LEARN MORE](#)