Ransomware: A Very Different Learning Curve for Higher Education

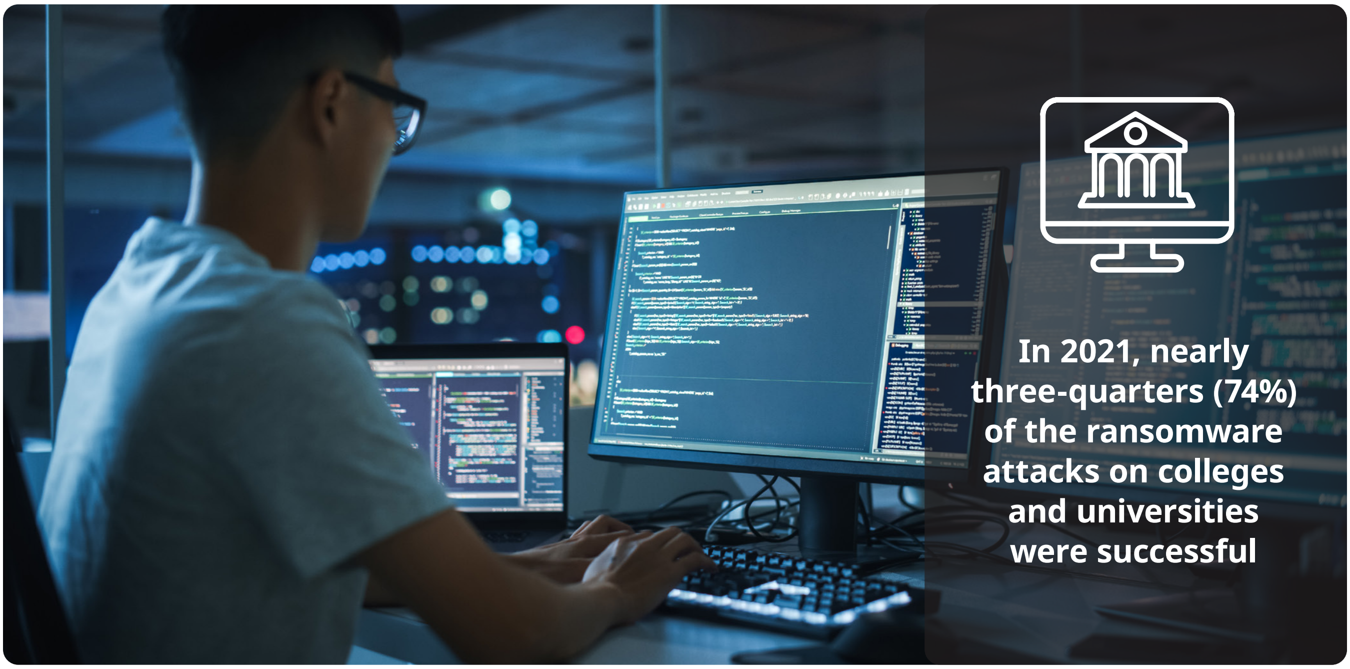
As the number of attacks increases, higher education organizations must bolster their cyber defense and recovery capabilities.

COLLEGE AND UNIVERSITY LEADERS have seen a sharp rise in the number of ransomware attacks on their network and data systems in recent years, and these attacks are costing their organizations significantly.

According to one report, at least 44 colleges and universities were victimized by a ransomware attack in 2022, up from 26 institutions the prior year. The actual numbers are likely higher, as these figures only account for publicly disclosed incidents.

PRODUCED BY: CAMPUS TECHNOLOGY

SPONSORED BY: COHESITY | aws



In 2021, nearly three-quarters (74%) of the ransomware attacks on colleges and universities were successful

During a ransomware attack, a malicious actor will infiltrate an organization's network and encrypt or corrupt numerous files, rendering them unusable. If a ransom is not paid, these files are often permanently locked or destroyed.

In a more recent trend, called "double extortion," the hackers will also attempt to exfiltrate student, employee, and/or operational data and hold this information hostage. They will threaten to publicly release or sell that data in an attempt to force a payment. That way, if the organization refuses to pay the ransom, the attackers still stand to profit.

Ransomware attacks can be quite costly, not only financially but in terms of lost instructional time. Ransomware attacks disrupted the final days of the spring 2022 semester at at least two U.S. colleges, **reportedly** forcing the cancellation of classes and the postponement of final exams.

These attacks can also do serious damage to an institution's reputation in the eyes of current and prospective students, parents, and faculty—potentially impacting long-term student recruitment and employee retention.

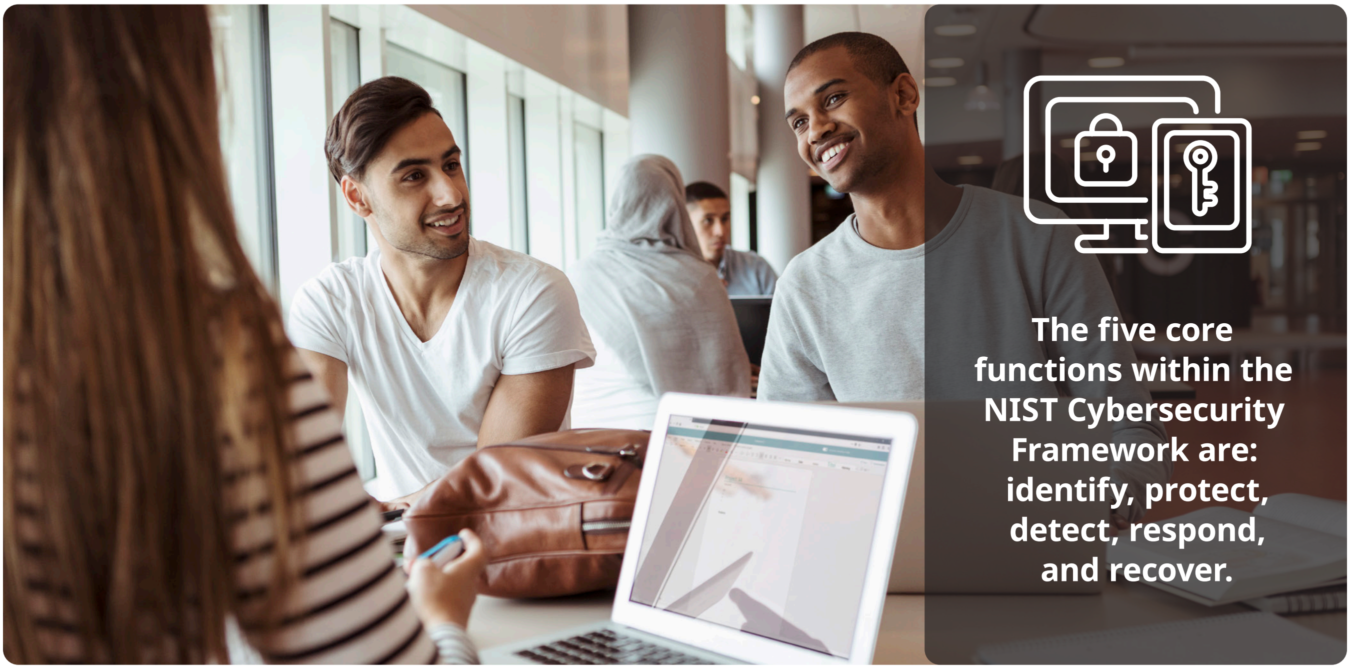
Higher Education Is an Attractive Target

Why are higher education organizations in particular under siege? For one thing, the nature of the academic community is highly collaborative. This inclination for colleges and universities to share data openly can make them appealing targets to cybercriminals.

"Colleges and universities are in an environment that is inherently about information sharing and research," said Ron Nixon, public sector chief information security officer for Cohesity, a data security and management company. "As a result, they are regularly being targeted by some of the best adversaries in the world."

This information-sharing culture can make cyberattacks more likely to succeed. According to a **2022 report from Sophos** that analyzed data from 2021, nearly three-quarters (74%) of the ransomware attacks on colleges and universities that year were successful.

Hackers' efforts in other industry sectors were not as effective, the report indicated:



The five core functions within the NIST Cybersecurity Framework are: identify, protect, detect, respond, and recover.

The global average data encryption rate in attacks across all sectors was 65%.

Challenges to Data Security and Management

These statistics show the importance of having sound data security and management practices in place to protect organizations from ransomware attacks.

Colleges and universities need stringent data access policies, moving away from a largely permissive approach to one of Zero Trust. They need identity and access management solutions that authenticate network users and restrict what information users are allowed to access. And they need consistent data backup practices and a system for recovering data quickly in the event of a successful attack.

The data security tools and strategies that institutions adopt should address the five core functions within the **National Institute of Standards and Technology (NIST) Cybersecurity Framework**: identify, protect, detect, respond, and recover.

Yet, aside from issues of culture, there are many other factors that make it challenging for colleges and universities to secure, back up, and recover their data effectively.

For instance, colleges and universities are complex IT environments, with various schools and departments each having different needs and circumstances. What's more, higher education organizations often must protect and recover data within a mix of on-premises and cloud-based systems.

Both of these factors can result in highly fragmented data management tools and policies, with IT staff using different solutions for various campus departments or ecosystems. Not only is this approach more expensive to deploy and manage, but the complexity leads to an increased attack surface that can make securing and recovering data much harder than it needs to be.

Colleges and Universities Take Longer to Recover

As a result of these challenges, when ransomware attacks against colleges and universities are successful, they tend to be costlier to resolve.

Although most of the colleges and

96% of higher education organizations with cyber insurance have upgraded their data security and management solutions.

universities victimized by a ransomware attack in 2021 succeeded in retrieving at least some of their data, few retrieved all of it, according to the Sophos report—even after paying the ransom. Higher education institutions only recovered 61% of data on average. Only 2% reported recovering all their data.

Higher education is also among the slowest of all sectors to recover from a ransomware attack. Forty percent of the colleges and universities hit by a ransomware attack in 2021 took more than a month to recover fully, which was double the global average of 20%. Nearly one in 10 colleges took at least three months to recover.

In addition, the average remediation cost of $1.42 million in higher education was more than the global average for all sectors.

Organizations Must Be Prepared

Colleges and universities can purchase **cyber insurance** to help cover some of the costs associated with a ransomware attack. Yet, as the higher education technology association **Educause observes**, the market for cyber insurance is still evolving and maturing. What's more, insurers are requiring institutions to take increasingly comprehensive steps to protect their data from an attack, including having an air-gapped or isolated copy of their data stored with a cloud provider such as Amazon Web Services.

This requirement is driving better cyber defenses: According to the Sophos report, 96% of higher education organizations with cyber insurance have upgraded their data security and management solutions to improve their cyber insurance posture.

Although the risks of a ransomware attack are growing, colleges and universities can take measures to protect themselves effectively. With the right combination of policies and technologies, higher education organizations can decrease the likelihood of a successful attack—and respond and recover quickly if an event should occur.

“Colleges and universities need to take the threat of ransomware very seriously,” Nixon concludes. “They need to retain a clean copy of their data that can be used to prevent paying a ransom and bring their systems back online quickly and confidently.”