# Cybersecurity challenges for educational institutions

## Understanding threats and implementing strategies to mitigate risks

July 2017

Cybersecurity threats are rising across all industries, as hackers attempt to access sensitive data for nefarious reasons, including financial gain, identity theft and political motivations. For example, the 2017 SonicWall Annual Threat Report[1] found that instances of ransomware attacks are soaring, increasing from 3.8 million attacks in 2015 to 648 million in 2016. Unfortunately, educational institutions are generally vulnerable to cyberattacks, mainly due to the open nature of many schools' technology infrastructures and funding concerns emphasizing keeping systems running rather than protecting environments.

A cyberattack can have damaging effects on an institution, from financial losses related to repairing the infrastructure following a breach and potential litigation, to severe reputational damage. Therefore, the focus for administrators and technology resources must shift from being reactive, and addressing cybersecurity incidents after they occur, to implementing a proactive strategy and framework to identify and address cyberthreats before they can harm the institution.

While schools can encounter several different types of cyberattacks, RSM risk advisory professionals have worked to remediate hundreds of cybersecurity concerns within educational institutions in recent years, and have noticed a significant increase in three specific types of attacks: phishing, ransomware, and insider threats or malicious users. For each of these emerging threats, we provide an overview of the risk, a specific case study about a situation that an institution faced and an explanation of how to help prevent a similar attack.

### Case 1: Phishing attacks

#### Overview

Phishing is not necessarily a new threat, but the frequency of attacks and the amount of information that hackers can

1 "2017 SonicWall Annual Threat Report," accessed June 26, 2017, https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810.

leverage to launch an attack have caused this risk to escalate even further. Contact information for employees at all levels is readily available from a variety of sources, including institution websites and social media profiles. Perusing such sites can give attackers insight into employee emotional status, physical location (e.g., on vacation or out of the office) and other factors that can be leveraged to mount a credible phishing attack. This information is embedded within carefully targeted emails that look completely legitimate.

Unfortunately, phishing emails like these include links that are used by attackers to collect email, application, network and system passwords, or are designed to exploit other vulnerabilities.

### Case study

RSM recently worked with two universities that suffered similar phishing attacks after migrating to a new payments and payroll solution. Both had the same organization implement the system and were very public about utilizing the new platform, with information on both projects readily available on the internet.

Unfortunately, many users at both universities were not familiar with how the new system worked, which is fairly typical with new implementations. Unauthorized users and attackers were aware of the new system implementation, however, and sent out phishing emails in an attempt to exploit the vulnerability of unsuspecting new users. They built a distribution list from information available online.

The phishing email directed users to a website that mirrored an email logon screen and collected user names and passwords, and, in some instances, recovery emails, phone numbers and security questions. All of that information was then sent back to the attackers, providing all of the information necessary to access a user's email.

The attackers accessed email accounts and set up rules to delete emails from the new financial application that would indicate changes in the system. They then used the stolen user name and password to log into the financial platform, and changed direct deposit information for many payroll accounts to prepaid debit cards.

While that breach caused significant damage to both institutions, it also affected many end users, exposing their information from the payroll system. Compromised bank account information, routing numbers, addresses, names, phone numbers and Social Security numbers all have the potential to lead to identity theft.

### Investigation

A mitigating factor that could have kept hackers out of the payroll system is two-factor authentication on the email system or payroll application, or both. In these instances, neither university had particularly sensitive information in its email, but that could have been a serious concern as well. In other areas of the university, sensitive human resources, medical or research information could have been exposed.

To help solve the issue, the RSM team performed digital forensic analysis of log data to determine what happened, when it happened and how it happened. We advised the clients to help ensure they provided relevant and complete logs. Both organizations performed independent log review, but in both cases, RSM viewed the data through a slightly different lens, and ultimately discovered more actionable information. Based on our findings and our understanding of the rules and regulations that attorneys follow and what information they look for, appropriate law enforcement steps were taken.

Fortunately, one university had forensic data from the time of the incident. The other did not. In that scenario, we relied on the new financial system's logs to identify both legitimate and unauthorized access. The payroll vendor kept more detailed logs, and helped to ascertain additional details, including what pages were viewed in the payroll application. The institution did not know that those logs existed, or how to ask for them. Our experience in digital forensic analysis allowed us to provide insights our clients couldn't have developed based on their limited experience with such situations.

### Lessons learned

One of the takeaways from these cases is that institutions should limit the amount of information that is made public about new system implementations. While it is an exciting endeavor, hackers specifically target new implementations because of vulnerabilities that can arise while transitioning to a new platform, including users going through the learning curve of becoming comfortable with new features and functionality.

## Case 2: Ransomware

### Overview

With ransomware situations, an individual will fall for a phishing email and download malware, which then encrypts system files and subsequently prevents users from accessing them. The main goal of ransomware is to get the person that is affected to pay a ransom to regain access to systems and networks, rather than stealing data or remotely accessing and controlling information.

For example, a common malware application named SamSam (sometimes referred to as Samas) utilizes an automated script that crawls the internet, looking for systems with a specific server vulnerability. Once it finds one that is vulnerable to an attack, the script exploits that vulnerability to gain access to the system and then crawls through the internal network.

Once attackers gain access to the network, they can access accounts, harvest credentials and change privileges. Attackers can use several different methods to gain a stronghold on the environment. However, when they are in the network, they can attack sensitive databases, find sensitive data and install malware to be more persistent on the network. There is no limit to a potential breach once privileged access is gained.

### Case study

RSM worked with a college that was affected by SamSam in an information security incident that ultimately contained many unknowns. When attackers compromised the institution's

network and deployed SamSam, it infected nearly 800 computer systems—almost every computer system on the school's network.

However, before RSM's involvement, the school attempted to begin remediating the problem by wiping and rebuilding many of the affected systems.

### Investigation

When the RSM team arrived on site, 85 to 90 percent of the systems had already been wiped and rebuilt, which eliminated significant evidence that would have helped determine the nature and extent of the incident.

The institution also had very limited logging that occurred during the infection, limiting the amount of information available that would show activity during that critical time frame. While there were few computers and systems that the RSM team could analyze, we determined that the ransomware was pushed into the system by an automated scripting function, and the attacker did not manually go to each system and deploy it.

The RSM team also determined that the system that was "patient zero," or the one that the attacker used to gain access to the network and initiate the ransomware attack from, was likely wiped or rebuilt as part of the institution's remediation efforts. RSM consulted with the institution's attorneys to discuss the size of the incident, how data was stored on the network, and what could be learned from additional logs and rules for data storage.

Because of the limited evidence, RSM needed to coordinate its investigation with the attorneys representing the institution to determine the appropriate rules, regulations and notification obligations for the institution.

### Lessons learned

Given the remediation efforts adopted and the lack of advance planning, it was almost impossible to understand when the infection occurred and how the network was compromised. The lack of forensic data and the small sample set to analyze greatly increased the difficulty for the client to remediate the incident.

The moral of this story is to have a robust incident response plan, and implement preplanning, monitoring, networking and logging to enable effective triage, analysis and response.

## Scenario 3: Insider threat or malicious user

### Overview

Threats don't always come from outside an institution's environment. In many cases, employees can hack into networks to change permissions, or access sensitive information from human resources or sensitive financial data. In addition, students often attempt to hack into school networks to alter grades or disciplinary and financial information, or simply to access internet resources that are blocked by the school.

Many institutions attempt to stay up to date on external threats, but lose sight of the potential vulnerabilities that can come from within. Internal parties already have a certain level of access to the technology infrastructure, and can cause just as much damage as criminals that attempt to initiate a breach from outside the network.

### Case study

RSM worked with a boarding school where a student (hacker) had gained access to systems that belonged to teachers within the organization. The school performed an internal investigation to determine how the unauthorized access occurred and what was accessed.

The school identified the hacker, and determined that a password recovery tool was used to recover the username and password to a teacher's account within the school's learning management system. The hacker then accessed the grading system to alter grades. Ultimately, the school knew the impact of the incident, but did not know what other systems were affected and what credentials may have been harvested from other networks.

### Investigation

RSM analyzed one system that the school knew the student pulled credentials from. The team looked at the forensic artifacts that were generated by the tools the student used, and generated an automated script to search for similar artifacts on every system within the network.

That script was deployed for a month, reporting that a system was clean if no artifacts were found, or performing additional analysis on systems that contained artifacts or any other hallmarks of suspicious access. Ultimately, the script scanned about 85 percent of the school's network and identified other systems that were accessed, with the remaining systems rebuilt or replaced over the summer.

Running the script across the school's network gave the school a high level of confidence that the hacker did not attempt to run the identified password recovery tools on any other systems in the school's environment, and ultimately did not compromise any additional user account credentials.

### Lessons learned

Institutions don't always know where a threat may come from, and as a result, they can't prevent every incident from occurring. In this scenario, the institution had a very technical and strong IT and incident response team, which allowed it to efficiently identify the threat actor as well as the attack vector. RSM's help with the investigation to analyze, scan and pinpoint affected servers was crucial as well. As a result, the institution was able to quickly identify the potential impact as well as mitigate any risk associated with that threat.

## Conclusion

The cybersecurity threats to educational institutions are constantly evolving. New risks emerge on a consistent basis, and existing threats change shape and can attack an institution with different methods. Educational entities will always be acutely vulnerable to attacks because of their open infrastructure, designed to foster learning and research. However, that does not mean that threats cannot be discouraged or quickly mitigated before they result in significant damage.

Institutions generally must increase their overall awareness to understand potential threats, and leverage the necessary resources to implement a proactive cybersecurity strategy. That strategy should include periodic vulnerability assessments, detailed logging procedures, thorough incident response plans and scalability to address new threats. This comprehensive plan can provide an effective foundation to help protect key technology systems, sensitive data and an institution's reputation.

**+1 800 274 3978**
**rsmus.com**



wp-ne-ras-ge-0317

RSM