



HOW EDUCATION  
INSTITUTIONS CAN AVOID  
BECOMING THE NEXT  
RANSOMWARE VICTIM

**SECURITY EXPERTS** are now calling it the “epidemic of our time.” Ransomware — a family of malware that hijacks an organization’s data so hackers can extort a payment — is increasingly the go-to method of attack for cybercriminals. During the first few months of 2017, ransomware attacks rose by more than 250 percent.<sup>1</sup> Most alarming is that education is the No. 1 target of ransomware, according to a 2016 ransomware study which noted that at least one in 10 education institutions have experienced a ransomware attack.<sup>2</sup>

One such institution was Michigan State University. The college was breached with a ransomware attack in November 2016. Although the demand was for 400,000 records, quick action by the university limited the breach to fewer than 500 records and university officials opted to not pay the ransom.<sup>3</sup> However, other higher education institutions have not fared as well, and have been forced to pay tens of thousands of dollars via Bitcoin.<sup>4</sup>

The overall threat to higher education is significant. For example, if hackers capture data from a university research project and destroy or release it publicly, a multi-year grant worth millions of dollars would be in jeopardy. Unfortunately, that’s not an implausible scenario. “Despite our best efforts to convince people to follow sound data protection practices, we often find important information gets stored on a laptop inside a lab somewhere,” says Bob Turner, chief information security officer (CISO) at the University of Wisconsin, Madison (UW-Madison).

Higher education isn’t the only vulnerable area. School districts are also a target. For example, in April 2017, cybercriminals demanded \$37,000 from Pekin Community High School in Illinois after they used encryption to deny

## UNDERSTANDING YOUR ENEMY

Ransomware is random, agnostic and increasingly sophisticated. Here are the six steps an attacker must take to succeed.



administrators access to their data (the high school did not pay the ransom).<sup>5</sup>

Scenarios like these demonstrate why it is important to incorporate an anti-ransomware strategy into your institution’s overall cybersecurity plan. Where to start?

## RANSOMWARE: A SERIOUS THREAT TO HIGHER EDUCATION

Education is the  
**#1 TARGET**  
of ransomware.



**1 IN 10**  
education  
institutions have  
experienced a  
ransomware  
attack.



Education  
institutions are  
**4X MORE**  
likely to be hit  
with ransomware  
than health care  
organizations.





**Thieves broadcast emails with infected attachments — often disguised as compressed files that contain malicious JavaScripts — and hope unsuspecting recipients will open them and infect internal networks.**

This paper presents a step-by-step approach for understanding today's ransomware threats, along with best practices for preventing them.

## RANSOMWARE EVOLVES

A number of factors are driving cyber thieves to focus resources on ransomware-driven profits. First, other go-to methods for making money are losing their punch. For example, selling personal information and credit card numbers isn't as lucrative as it used to be, as the prices paid for stolen records declines.<sup>6</sup> This is prompting thieves to search for new revenue opportunities.

Digital innovations are also providing criminals with new tools for extortion. Topping the list is Bitcoin, the virtual monetary system that operates without the oversight of a central bank to uncover and intervene against illegal activities. It's the preferred method for accepting ransoms, giving victims and authorities zero options to trace transactions back to perpetrators. After seeing the rise of Bitcoin-enabled extortions, an unidentified university chief security officer told the *Wall Street Journal* he purchased two machines to mine Bitcoins "in case he needs to quickly recover a critical computer."<sup>7</sup>

Asymmetric cryptography is another technology enabler for data thieves. The encryption method uses two keys — one public, the other private — allowing hackers to make important files inaccessible to the rightful owners. Victims are promised they will receive a private key to unlock their data when they pay a ransom. Although dozens of malware families fall under the ransomware umbrella, some of the most common programs delivering asymmetric cryptography today include: Cerber, WannaCry and Locky.

Hackers exploit a variety of IT vulnerabilities to get malware onto

## TO PAY OR NOT TO PAY?

Victims of ransomware attacks face a difficult decision — whether or not to pay to regain access to their data, with no guarantee the extortionist will abide by the deal.

According to experts, paying a ransom should be the last resort for retrieving information. Noting that the U.S. government doesn't encourage ransom payments, the FBI acknowledges that whether or not to pay a ransom is a serious decision "requiring the evaluation of all options to protect shareholders, employees and customers."<sup>8</sup> It advises victims to evaluate the technical feasibility, timeliness and cost of restarting systems from backup.

The FBI also points out that some individuals and organizations never receive the decryption keys to unlock their data, even after making a payment. Others make the initial payment and then must make subsequent payments before they actually receive the decryption key. In many cases, extortionists will eventually comply once they receive money — that's part of the business model. If victims get stiffed, there's little incentive for others to pay. But giving money to cyber criminals has far-reaching ramifications. Part of the profits will likely go to further research on their part to develop new and more difficult-to-block malware.

The best approach is to have a response plan in place before problems arise so you don't have to make important decisions under pressure.

**Paying a ransom should be the last resort for retrieving stolen information.**





## CONSIDER CREATING A NEW POSITION - THE CHIEF DATA OFFICER

Two years ago, UW-Madison hired its first chief data officer (CDO), one of only a handful known to be working in higher education today. After an initial period of speaking with faculty and staff, the CDO developed a data classification methodology that is helping CISO Bob Turner implement a university-wide security strategy.

Now data and security officials are formalizing rules for granting access to the various classifications of data. "It's all about making sure research data or administrative data stays where it's supposed to be while being available to the right people," Turner says. "Also, if somebody is doing any operation that involves university data, we have a clear understanding of what they're doing."

**Prevention is the Cure:  
As education institutions  
formulate anti-ransomware  
efforts, officials must focus  
on preventing rather than  
defending against attacks.**

school networks and seize control of data. Betting on human error is one common strategy. Thieves broadcast emails with infected attachments — often disguised as compressed files that contain malicious JavaScripts — and hope unsuspecting recipients will open them and infect internal networks. Unlike phishing or other targeted cyber attacks, ransomware emails are often random rather than direct messages to specific individuals.


Another strategy is to deliver an exploit kit via spam or a compromised website. Once on a computer, these kits run in the background as they search for system vulnerabilities, such as missing security patches for Microsoft Office applications, web browsers, Adobe Flash Players or Java software. Hackers then exploit any openings to install ransomware and begin the extortion process.

Web-based file sharing platforms are another vulnerability because they make it easy for students and staff to share files without the security oversight of the IT department. For example, researchers may not consult with IT managers before creating a cloud-based account for sharing data. "Often, that's urgency driven, so I don't fault them at all for that," UW-Madison's Turner says. "We just need to check in regularly to make sure that our approach to this area matches their approach."

Education institutions are particularly vulnerable to this list of exploits because their environments are designed for collaboration and openness. Students, faculty and staff routinely sign on to school networks from a variety of locations and many different types of devices to freely share information. This diversity is a challenge to school cybersecurity officials who are responsible for protecting many access points. Turner says estimates that more than 500 campus networks connect to the university's backbone.

But the challenge reaches beyond just locking down large campuses. Research grants for higher education often require collaboration with other institutions, so even an organization with state-of-the-art security controls becomes vulnerable to infections contracted by peers.

Similarly, the decentralized nature of data governance policies challenges education institutions. While many schools develop an overarching security strategy, it may be up to individual colleges or departments to implement it. Yet these smaller organizations may not have a full-time IT security staff to manage policies and keep them updated. "We'd like to think that we're all playing from the same sheet of music, but the simple fact is we're not," Turner says.



He adds that the university is working toward more common strategies and technologies with the help of an internal group known as the Madison Information Security Team. It's composed of representatives from each of the major colleges and departments and meets regularly to identify common security approaches that would work for everyone, and thus may be incorporated into the university-wide strategy.

## HOW TO SAFEGUARD

As schools formulate anti-ransomware efforts, one overriding reality quickly becomes clear — officials must focus on preventing rather than defending against attacks. After all, by the time an organization realizes WannaCry is on the network, criminals have already had an opportunity to seize valuable data. But with constantly evolving ransomware, how can institutions fully block known and unknown threats? The answer comes with a multi-pronged campaign that focuses on policies, technology and people.

Data governance standards are the first step in formulating effective anti-ransomware policies. Schools need to classify and rank the criticality of data as well as determine who has access to specific applications and files. “Everything begins and ends with assessing your data,” Turner says. “If you just try to protect all data at the same level, it becomes a very expensive proposition because you may be overspending to protect unessential information. Or, it becomes a cheap proposition because none of your data is being adequately protected. By understanding the different types of data you have, you’ll be in a better position to understand how each should be appropriately managed.”

To help make those calls, Turner taps into various governance bodies on campus. He and members of the Madison Information Security Team report to the Madison Technical Advisory Group — the main IT governance body — which is composed of the university’s chief information officer and department CIOs. “They offer us guidance on IT goals and provide an ear for listening to our security initiatives,” Turner says.

In addition, the school’s Information Technology Committee is a faculty-run governance body that works with IT and security staff on ways to enhance teaching and learning resources. Finally, Turner says the university is a pioneer in organizing a data governance executive council, which manages the classification, prioritization and stewardship of data.

With data classifications in place, the FBI advises organizations to pay particular attention to privileged accounts, such as those that grant administrative rights

**“If you just try to protect all data at the same level, it becomes a very expensive proposition because you may be overspending to protect unessential information. ... By understanding the different types of data you have, you’ll be in a better position to understand how each should be appropriately managed.”**

Bob Turner, CISO, University of Wisconsin, Madison

to systems and managing data. For example, only people whose roles require it should have this special status, and policies should be in place to ensure these staff members use the power only when necessary.<sup>9</sup>

Schools should also update policies to address the rise of cloud storage and the reality of on-premises and off-premises data centers. One approach is to determine which option is best for highly sensitive information, or data associated with federally funded research projects that fall under the Federal Information Security Management Act (FISMA). “We are looking at whether to deploy more systems to cloud environments that offer services for data loss prevention,” Turner says.

Enhanced backup and disaster recovery plans are another focal point for policy modernizations in the age of ransomware. When prevention fails, reliable and comprehensive data backup strategies are vital for foiling extortionists. If criminals strike, IT managers can shut down the infected systems, restore purloined data onto clean machines and avoid paying a ransom. The caveat, however, is that thieves still have the option of publicly disseminating personal information or proprietary research data, which explains why prevention should be the primary goal.

Nevertheless, given the importance of backups as part of an overall strategy, IT and security managers should work with administrators and department heads to update recovery plans. Start by classifying individual files according to their criticality. Systems managing the most valuable information may need to be backed up regularly throughout the day to reduce the possibility of important information being lost. While this is the safest option, it is also the most expensive and may not be appropriate for less vital data that can safely be backed up nightly or even weekly.

Finally, having modern policies in place is just the start. Schools must also regularly validate their recovery and

# WHAT TO LOOK FOR IN NEXT-GENERATION FIREWALLS

Next-generation firewalls, or NGFWs, monitor data traveling across physical and cloud-based resources and can help mitigate zero-day threats. Look for the following capabilities when vetting potential NGFWs.

1

**TOOLS FOR  
MONITORING DATA  
AS IT TRAVELS  
ACROSS PHYSICAL  
AND VIRTUAL  
RESOURCES**

2

**SANDBOXES FOR  
QUARANTINING  
AND TESTING  
SUSPICIOUS  
CODE THAT MAY  
BE ZERO-DAY  
MALWARE**

3

**THE ABILITY  
TO ASSESS  
DATA FLOWING  
THROUGH EVERY  
COMMUNICATIONS  
PORT**

4

**THE ABILITY TO  
ANALYZE THE  
VALIDITY OF  
ENCRYPTED DATA**

5

**SENSORS FOR  
MONITORING  
NETWORK TRAFFIC**

**Next-Generation Security:**  
**Unlike traditional firewalls,**  
**NGFWs can assess data no**  
**matter what communications**  
**port it's traveling through,**  
**and regardless of whether it's**  
**encrypted or accessing physical**  
**or virtual IT resources.**

business continuity tactics. Related to this, they should have a process for quickly incorporating the results of validation exercises into overall policies to keep them up to date.

UW-Madison's ultimate goal is continuous testing and improvement planning. "We're moving to a process where testing feeds directly into a periodic or continuous monitoring strategy," Turner says. "The challenge is getting everybody to understand that continuous monitoring requires a lot of effort, especially when you have the diversity of technology and networking that we have here on campus."

Testing must also be coordinated with other institutions linked by research projects and other activities. Further challenges arise when making sure the feedback from the testing is relayed across institutions.

## TECHNOLOGY UNDERPINNINGS

To stop extortionists from exploiting security holes in applications, schools should bolster their software patching efforts. One option is to invest in automated patch management programs that relieve IT departments from manually installing vendor updates. Note, however, that patches may sometimes prove incompatible with existing installations, possibly leading to system and application downtime. Thus, planners may need special testing and implementation procedures for critical resources requiring high availability. While practical from an economic and capabilities perspective, cloud-based applications and infrastructures also offer relief from patching responsibilities by resting the burden of testing and installing patches on the cloud provider.

Basic cybersecurity requires automatic updating and monitoring of anti-virus software as well. However, while this protects institutions from known malware, newly created threats can slip through these basic defenses. Next-generation firewalls (NGFWs) implemented within the overall security platform can mitigate zero-day threats and other vulnerabilities. These technologies monitor data traveling across physical and cloud-based resources and can stop known and unknown threats from accessing networks. NGFWs address zero-day malware by quarantining unrecognized or suspicious code and running tests to validate its authenticity. When tests uncover problem software, organizations can destroy it before it infects school networks.

Unlike traditional firewalls, NGFWs can assess data no matter what communications port it's traveling through, and regardless of whether it's encrypted or accessing physical



**“Fear, uncertainty and doubt are never part of a good security strategy. So I try to make sure I totally understand what their issues are. That way, we can come up with the best techniques and methodologies for researchers, faculty and campus administrators. At the end of the day, you can design the best security possible, but if nobody uses it, what’s the point?”**

Bob Turner, CISO, University of Wisconsin, Madison

or virtual IT resources. Leading NGFWs can also perform network security monitoring to flag suspicious traffic on the network. While this may identify malware that has already breached the network, it still gives officials an opportunity to limit the damage before it reaches other systems and end users.

To further limit ransomware from spreading to the most valuable data, schools should consider segmenting it inside a virtual LAN with virtual firewalls. Encrypting the information and requiring multi-factor authentication to access it also heightens security.

Schools should also look into joining industry organizations — such as the Cyber Threat Alliance — that share data about cyber attacks worldwide, including ransomware incidents. Thus, if a new cryptography mutation appears, security officials can update their defenses to stop the threat before it slips onto networks.

Finally, because security threats evolve so rapidly and in such high numbers, schools should consider contracting with third-party services that automatically update their security frameworks based on trending information.

## ADDRESSING HUMAN FACTORS

Even the best security policies and technologies aren’t enough to fully protect colleges and universities from becoming ransomware victims. Mistakes by end users, whether that is opening an untrusted attachment or browsing an infected website, remain a hacker’s easiest entry into internal networks. Thus, the cornerstone of any security program should be ongoing training of faculty, staff and students to reinforce best practices. These discussions should also detail proper data management techniques, including the dangers of storing proprietary research data on a laptop rather than in a secure central location.

These discussions shouldn’t be one-way conversations; CIOs and CISOs should also listen to end user concerns about staying productive and doing their jobs. “Fear, uncertainty and doubt are never part of a good security strategy,” Turner says. “So I try to make sure I totally understand what their issues are. That way, we can come up with the best techniques and methodologies for researchers, faculty and campus administrators. At the end of the day, you can design the best security possible, but if nobody uses it, what’s the point?”

Regular conversations with senior leaders are also vital, not only to reassure them that security measures are in place to address cybersecurity threats, but also to help them understand why additional investments will be needed to stay ahead of hackers.

## PREVENTION IS THE BEST

Ransomware is insidious, destructive and on the rise. Its victims include higher education institutions and K-12 districts, as hackers prey on human error, gaps in software patching procedures and other common security vulnerabilities. But with the right anti-ransomware strategy and modern technology for blocking known and zero-day threats, CIOs and CISOs can wield the most powerful weapon of all — preventive measures that keep the malware from ever taking hold in their organizations.

*This piece was developed and written by the Center for Digital Education custom media division, with information and input from Palo Alto Networks.*

### ENDNOTES

1. <http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034>
2. <https://www.csoonline.com/article/320811/security/who-is-a-target-for-ransomware-attacks.html>
3. <http://statenews.com/article/2016/12/msu-to-spend-nearly-3-million-after-data-breach>
4. <http://beta.latimes.com/local/lanow/la-me-in-los-angeles-valley-college-hacking-bitcoin-ransom-20170111-story.html>
5. <https://www.databreaches.net/il-pek-in-high-school-hit-by-ransomware-and-37000-demand/>
6. <http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632>
7. <http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/>
8. <https://www.justice.gov/criminal-ccips/file/872771/download>
9. Ibid.

Produced by:

CENTER FOR  
**DIGITAL**  
EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21<sup>st</sup> century.

[www.centerdigitaled.com](http://www.centerdigitaled.com)

For:



Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for government agencies and educational institutions worldwide. Built with an innovative approach and highly differentiated cyber-threat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables everyday operations, and protects an organization's most valuable assets.

Find out more at [www.paloaltonetworks.com](http://www.paloaltonetworks.com).