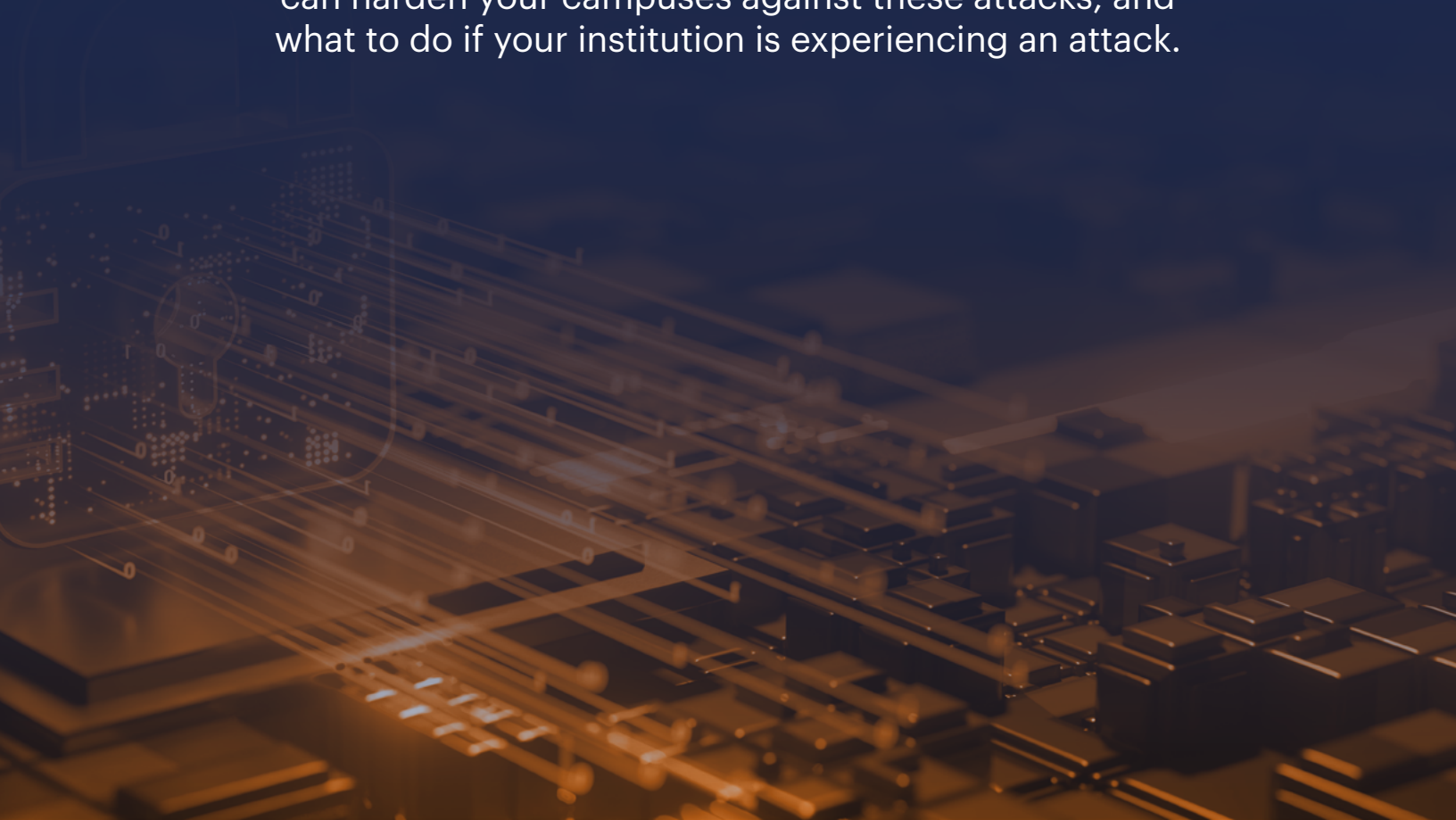
ThreatDown™
Powered by Malwarebytes

2023 HIGHER EDUCATION RANSOMWARE *EMERGENCY KIT*

Ransomware is a clear and present danger to higher education institutions. This emergency kit explains why you should be concerned about ransomware, how you can harden your campuses against these attacks, and what to do if your institution is experiencing an attack.



CONTENTS

ThreatDown
Powered by Malwarebytes

UNDERSTANDING THE THREAT

From April 2022 to April 2023, 85% of higher ed UK institutions said they experienced a breach or attack, nearly 10% of which were ransomware related.[1] Even one successful attack can have huge consequences: ransomware attacks on UK higher ed ransomware attacks have impact costs exceeding £2m.[2]

In June 2023, University of Manchester confirmed they had suffered a ransomware attack in which attackers allegedly stole 7TB of data.[3] In July, the Rhysida ransomware gang allegedly attacked the University of the West of Scotland, publishing 363 gigabytes of data on its leak site.[4]

Apart from ransom payments, which the National Cyber Security Centre (NCSC) advises organizations not to pay, recovering attacks cost education institutions dearly. Three-quarters (75%) of UK higher education institutions say they were negatively impacted regardless of whether there was a material outcome or not. Most commonly, they report needing additional staff time to deal with the breach or attack, or to inform customers or stakeholders (70%).[5]

Higher education presents unique challenges for cybersecurity because it fosters a culture that:

- **Encourages open communications** to enhance learning and foster research
- **Stores a wealth of intellectual property** and personally identifiable information (PII)
- **Has siloed academic departments** (that inhibit implementation of campus-wide security protocols)
- **Houses a dangerous mix of tech savvy and tech illiterate** as well as users with multiple roles (e.g., teachers who are also students)

40%

Slowest recovery time (twice the global average)

$1.14M

Amount University of California SF paid in ransom

10M

Records impacted to date in top 10 states for higher ed data breaches

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex#chapter-2-detailed-findings
[2] https://beta.jisc.ac.uk/blog/latest-cyber-impact-report-underlines-ransomware-as-a-huge-threat-but-financial-cost-of-attacks-is-still-unclear
[3] https://www.bleepingcomputer.com/news/security/university-of-manchester-confirms-data-theft-in-recent-cyberattack/
[4] https://www.thescottishsun.co.uk/news/11087430/hackers-thousands-scottish-students-uws-dark-web/
[5] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex#chapter-2-detailed-findings

ANATOMY OF A RANSOMWARE ATTACK

Criminal hackers typically deploy ransomware as the last act in a sophisticated infiltration of your network. Every ransomware attack is different but typically follows a predictable pattern with five phases.

Breach	
Attackers gain unauthorized access to one of your computers through malware; a software vulnerability; remote access exploits; or by phishing, guessing, or finding a password. They can gain access months before the attack phase.	The best way to stop a ransomware attack is to prevent the initial breach. This requires web protection, effective vulnerability and patch management, hardening of remote access, and training users to identify and report phishing.
Infiltration	
Attackers quietly explore your network to prepare for their attack. They may steal data and try to disable security software and backups.	You cannot prevent every breach. But monitoring logs and alerts that security solutions generate may enable you to identify suspicious activity and stop intruders before the attack phase.
Attack	
Attackers run ransomware throughout your network, often at night or over the weekend.[2] You may be forced to shut down systems that are critical to teaching and learning.	Stopping attacks requires multiple layers of security defense, anomaly detection for unknown "zero-day" threats, and ransomware prevention technology.
Response	
Attackers leave notes, demanding a ransom—which could be millions of dollars—and explaining how to negotiate. They will issue deadlines and may threaten to leak sensitive data.	You need offline backups and a response plan so you can restore critical operations as quickly as possible. As you work to do so, speak with students, alumni, staff, faculty, cyber insurance provider, lawyers, law enforcement, and others.
Recovery	
Whether or not the attack is successful, attackers may still be on your network or have left malware or artifacts behind to re-enter or re-infect your network. If you pay the ransom, attackers will note your willingness.	After restoring critical operations, you must discover what happened. You will need to expel the attackers from your network, remove all traces of the breach, and harden your network against a repeat attack.

[2] **The majority (76%) of ransomware attacks** take place either on week nights (49%) or over the weekend (27%).

SHOULD YOU PAY THE RANSOM?

Most experts and government agencies do not recommend paying a ransom. Ransom payments incentivize further attacks and fund the continued development of ransomware, making everyone less secure.

Depending on your location, you may not have a choice: **North Carolina and Florida recently passed laws** that prohibit public entities, including state-funded schools, from paying ransoms.

If you are deliberating over whether to pay a ransom, weigh these factors carefully:

1. **Decryption often fails.**
   Cybercriminal organizations' decryption tools are often poor quality and may lead to partially corrupted data or simply not help. **Regis University in Colorado paid an undisclosed amount** to ransomware attackers in an attempt to restore their systems, to little avail; operations remained impaired for months.

2. **You are trusting criminals to keep their word.**
   Stolen data that's held for ransom may not be reliably deleted or properly secured. In some cases, criminals have leaked data before discussing the ransom or after the institution has already paid. In the April 30, 2023 **attack on Bluefield University, attackers posted more than two dozen student records** (with PII) on their site on the dark web to strengthen their threat: Pay up or we post it all.

3. **The cost of recovery can dwarf the ransom.**
   Even if you pay the ransom, you will need an extensive clean-up operation and upgraded protection to prevent future attacks. The cost in downtime, lost productivity, and recovery can dwarf the ransom. **Maricopa County Community College District paid an estimated $26M** after discovering that PII for more than two million past and present students, staff, and vendors had been exposed. Costs in this case were particularly high because the attack was the result of not properly repairing an earlier and less widespread hack.

4. **Paying leads to repeat attacks.**
   If you pay a ransom, attackers will note your willingness to pay and your inability to withstand an attack. Not all colleges and universities confess to having experienced a cyberattack, so it is difficult to determine which among them have been attacked multiple times. However, **80% of the companies that paid a ransom were attacked a second time** (with 40% paying again—and 70% of those paying more after round two).

RANSOMWARE PREVENTION CHECKLIST

	BREACH	INFILTRATION	ATTACK	RESTORATION	RECOVERY
Create an inventory of assets including hardware, software and data	✓	✓			
Audit your network for unknown computers and services	✓	✓			
Disable Internet-facing systems, services, and ports you don't need	✓	✓			
Perform regular vulnerability scans	✓	✓			
Patch systems regularly, prioritizing the most vulnerable and critical[3]	✓	✓			
Ensure systems are properly configured, and security features are enabled	✓	✓			
Harden remote access with MFA, password rate limits, and password lockouts	✓				
Deploy endpoint security software to all endpoints and servers	✓	✓	✓		
Provide staff with cybersecurity awareness training	✓	✓			
Implement a process for reporting and responding to suspicious activity	✓	✓	✓		
Document your network structure and data flows		✓			✓
Use network segmentation to subdivide your computer networks		✓			
Use least-privilege access for all systems and services	✓	✓			
Use allow listing to ensure that only authorized software can run		✓	✓		
Restrict the use of legitimate tools commonly used by attackers[4]		✓			
Harden domain controllers according to the latest best practice[5]		✓			
Monitor your network and endpoints using IDS, EDR and SIEM		✓	✓		✓
Make regular, comprehensive backups, keeping at least one copy offline				✓	
Have a process for restoring computers from clean system images				✓	
Practice restoring systems from backups, so you know they work				✓	
Create an incident response plan[6] that aligns with regulations			✓	✓	
Create a critical asset list so you know what you need to restore first • Consider how you will communicate internally and externally • Make contingency plans so critical functions can continue • Understand your legal and regulatory obligations				✓	

[3] As many as **60% of breaches could be avoided if available patches were applied**. A February 2023 ransomware attack against **Georgia Institute of Technology exploited a software vulnerability** for which a patch had been available since February 2021.
[4] This is known as "living off the land." The Living Off The Land Binaries and Scrip (LOLBAS) project maintains a list of legitimate software used by attackers at **https://lolbas-project.github.io/**
[5] Domain controllers are a prime target for attackers. Microsoft maintains a guide to securing domain controllers against attack at **https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack**
[6] You can find a response plan template at **https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md**

10-STEP RANSOMWARE RECOVERY PLAN

If you are dealing with a ransomware incident, you may be working under extreme pressure. Ransomware may still be encrypting files, attackers may have issued ultimatums, and you will be anxious to get all critical systems nup and running again to restore operations campus wide. Ask for help, prioritize your actions, communicate clearly, and take care of each other.

We recommend you take the following actions, in order:

1. **Contain the attack.**
   Isolate infected systems or networks to limit the impact of the attack. Your priority should be containing the attack, but if you can do so while preserving evidence by leaving affected systems turned on, do so.

2. **Establish the scope of the attack.**
   Determine which systems and what kind of data have been affected and prioritize critical systems for recovery.

3. **Communicate with stakeholders.**
   Stakeholders may include the President and governing board, department deans, faculty senate, lawyers, cyber insurance provider, and law enforcement, among others.

4. **Seek assistance.**
   Consider seeking expert assistance from local and national law enforcement, vendors, and other third parties familiar with ransomware recovery.

5. **Preserve evidence.**
   With the help of law enforcement and third parties, try to preserve evidence from the attack if you can.

6. **Identify the ransomware being used.**
   Identifying the ransomware being used will help you determine whether a public decryptor is available and will dictate the direction of containment and clean up.

7. **Contain the breach.**
   Try to identify the systems and accounts exploited for the initial breach as well as any precursor malware or persistence mechanisms the attackers might have left.

8. **Rebuild systems.**
   Use known good system images and backups to restore critical systems. Take care to segregate clean systems from affected systems.

9. **Reset, patch, upgrade.**
   Reset passwords, patch and upgrade software, and instigate any additional security checks necessary to prevent a recurrence of the attack.

10. **Document lessons learned.**
    Ransomware is constantly evolving. Use what you have learned from this attack to better prepare for the next one.

CONSIDER MANAGED DETECTION AND RESPONSE (MDR)

If you're feeling overwhelmed with the amount of information we just hurled at you, then you're a human being. Continually detecting and triaging ransomware threats is tough work—it's also not a one-person job.

To keep up with the volume of alerts and detect potential ransomware activity, you need (at least) the following:

- An Endpoint Detection and Response (**EDR**) solution
- A security information and event management (**SIEM**) solution
- A dedicated **24x7 Security Operations Center (SOC)** staffed with professionals to monitor the alerts and logs those solutions generate)

That said, the technology required for a SOC is generally complex, and the human expertise and staff hours required to monitor that technology can be prohibitively expensive.

Consider an MDR service. With MDR, you can outsource your anti-ransomware efforts to a team of top-tier professionals. MDR may be more cost-effective than building and staffing your own SOC—and is certainly less expensive than recovering from a cyberattack.

Get a quote for ThreatDown MDR >

24x7 security monitoring and threat hunting for your organization.