Education Edition

ThreatDown™
Powered by Malwarebytes

# 2024 Ransomware Emergency Kit

The ransomware cheat sheet and what to do when attacked

# Contents

# Understanding the threat

2023 was the worst ransomware year on record for Education: according to original ThreatDown research, the sector witnessed a staggering **105% surge** in attacks in the past year, increasing from 129 incidents in 2022 to 265 in 2023.

For Higher Education specifically, ransomware attacks increased **70% between 2022 and 2023,** with 68 attacks in 2022 and 116 total attacks in 2023.

For K-12, the story is bleaker. Ransomware attacks on K-12 increased 92% from 2022 to 2023, with 51 attacks in 2022 and 98 attacks in 2023.

Apart from ransom payments, which the FBI advises organizations not to pay, recovering from attacks costs education institutions dearly. The average data breach in the higher education and training sector cost $3.7 million in 2023, according to IBM's 2023 Cost of a Data Breach report.

Tight budgets, equipment that is often outdated, and limited IT staff, make school districts and universities an easy target for ransomware gangs compounded by cultural elements, including:

- **Fosters open communications** to enhance learning.
- **Stores a wealth of sensitive student property** and personally identifiable information (PII), and can include intellectual property and research.
- **Higher Education has siloed academic departments** (that inhibit implementation of campus-wide security protocols). IT and cybersecurity is often staffed by K-12 teachers or administrators not trained in monitoring or reacting to threat alerts.
- **Universities can house a mix of tach 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)

**$3B**

Amount University of California SF paid in ransom

**10M**

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

# Anatomy of a ransomware attack

Ransomware is typically deployed as the last act in a sophisticated infiltration of your network by criminal hackers. Every ransomware attack is different, but they often follow a predictable pattern, which can be broken down into five phases.

## Breach

Attackers gain unauthorized access to one of your computers with malware; by phishing, guessing or finding a remote password; or through a software vulnerability. This can occur 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 desktops, and users who can identify and report phishing attempts.

## Infiltration

Attackers quietly explore your network and prepare their attack. They may steal data, and may try to disable security software and backups.

You can't prevent every breach, so structure and monitor your network so you can identify suspicious activity quickly and stop intruders before the attack phase.

## Attack

Attackers run ransomware throughout your network, often at night or the weekend. Critical business operations stop. Ransom notes explain how to negotiate with attackers.

Stopping attacks requires multiple layers of security defense, anomaly detection for unknown "zero-day" threats, and ransomware prevention technology.

## Response

Attackers demand a ransom, which could be millions of dollars. They will issue deadlines and may threaten to leak sensitive data.

You must restore critical operations while talking to customers, suppliers, insurance, press, lawyers, law enforcement, and others. You will need offline backups and a plan.

## Recovery

Whether the attack is successful or not, attackers may still be on your network, and lingering malware or artifacts could cause reinfection. Your willingness to pay a ransom will have been noted.

After restoring critical operations, you must discover what happened, expel the attackers, and deny them access. Then you must harden your network against a repeat attack.

# 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. Anyway, you might not have a choice: both North Carolina and Florida recently passed laws prohibiting public entities, including local schools, from paying the ransom. If you are thinking of paying the ransom you should consider the following 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).

**FBI**

**WARNING**

The FBI does not support paying a ransom in response to a ransomware attack.
Paying a ransom doesn't guarantee you or your organization will get any data back.

# Ransomware prevention checklist

| What you should do: | 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 | ✓ | ✓ | | | |
| 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[1] | | ✓ | | | |
| Harden domain controllers according to the latest best practice[2] | | ✓ | | | |
| 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[3] that aligns with regulations | | | ✓ | ✓ | |
| Create a critical asset list so you know what you need to restore first | | | | ✓ | |

[1] 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/

[2] Domain controllers are a prime target for attackers. Microsoft maintains a guide to securing domain controllers against attack at https://docs.microsoft.com/ven-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack

[3] 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 your organization will be desperate to get up and running again. **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 also preserving evidence by leaving affected systems turned on, do so.

2. **Establish the scope of the attack.**
   Understand what systems and what kind of data are affected, and prioritize critical systems for recovery.

3. **Communicate with stakeholders.**
   Stakeholders may include senior management, PR, your legal team, cyber-insurance providers, security vendors and law enforcement.

4. **Seek assistance.**
   Consider seeking expert assistance from local and national law enforcement, vendors or 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.**
   This will help you discover if a decryptor is available, and it will inform the specifics of containment and clean up.

7. **Contain the breach.**
   Try to identify systems and accounts used in the initial breach, and any precursor malware or persistence mechanisms left by the attackers.

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 & 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.

ThreatDown™
Powered by Malwarebytes

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054 USA
sales@threatdown.com