DATAPRISE

# CIOs Ransomware Checklist:
## Before, During & After an Attack

Bonus: Incident Response Tabletop Exercise

DATAPRISE

# The Ransomware Pre-game Checklist

1. Plan, Plan, Plan. The first and potentially most critical step to effectively navigating a ransomware attack is ensuring that you are prepared for the incident.

   Having an incident response plan is foundational as it provides instructions to help your cyber team detect, respond to and recover from a security incident. It covers specific response actions based on the type of security incident – from ransomware to a breach to an account compromise – and provides a playbook for how to respond and who to notify.

2. Build a Response Team or Identify an IR Partner. As the CIO, you're the leader but it takes a team. During a security incident or ransomware attack is not the time to discover your staff isn't prepared. As part of response planning, build your emergency response team or CIRT (Cyber Incident Response Team) and define clear rules and responsibilities.

   If you do not have the internal security staff to manage a ransomware attack, consider finding an incident response (IR) partner now to keep on retainer for emergency response. The retainer approach is less expensive than ad-hoc emergency response services. If you maintain cyber insurance, your insurance provider may have a list of approved IR vendors, so ensure you select a partner that will be covered.

3. Prepare for Sound Forensics. Finally, if you operate in a heavily regulated industry, maintaining a sound cyber incident forensics chain is key to determining notification requirements. The forensics chain will allow you to follow the intruder and know what systems, records and data were impacted.

   As part of response planning, ensure you have the technology and processes to capture and maintain the digital fingerprints.

4. Conduct Tabletop Exercises. To test the plan and support a seamless response, conduct exercises at least annually on ransomware. This ensures that the first time you have an incident is not the first time you're following the plan.

   ***[Bonus: Use the Incident Response Tabletop Exercise provided in the appendix.]***

5. Maintain a Modern Backup Strategy. Backups and ransomware recovery go hand-in-hand but not all backup strategies are created equal. There is a big difference between having backups and having a backup strategy supported by modern technology that enables rapid recovery as well as prevents ransomware from encrypting the backups.

## Game Time: Ransomware Response Checklist

The steps outlined above (plan, response team, practice and backups) will enable your team to swiftly initiate the ransomware response including the following phases.

1. Isolate: Isolate and contain is the name of the game. Organizations must quickly stop the spread as ransomware is built jumping from machine to machine and spreading laterally quickly.

2. Containment: Preserving forensic evidence while containing the ransomware is essential. While instinct may say "pull the power cord," ensure your employees know not to do this. New malware is not written to disk, rather everything is in the memory. If power is turned off, the machine's memory is erased and forensic data is lost.

   Instead, pull the network cable or use your endpoint solution to isolate the machine(s) to prevent communication on the network. Remind your team that to "pull the network cable" in a virtual environment, you can disable the network interface on the hypervisor.

   Once the attacker loses access, it prevents them from executing anti-forensic actions to cover their tracks or destroy evidence. Skilled attackers will patch the vulnerabilities they used to gain access, delete their tools and erase logs to compromise a forensic investigation.

3. Eradicate and Recover: With isolation and containment executed, the next phases are eradication and recovery. The forensic investigation and business restoration are typically conducted simultaneously. The forensics team will focus on collecting data and logs as well as building a virtual copy of the impacted machines to following the chain.

   For business restoration this is where backups are critical as they allow organizations to easily recover valuable data and avoid paying the ransom.

## More from the Ransomware Pros: CISA's Checklist Summary

The Cybersecurity and Infrastructure Security Agency (CISA) published a detailed Ransomware Checklist, which goes into great depth on each step an organization should take. Following are the categories it covers to help frame your planning. **Download the full Checklist for more detail**.

### Detection and Analysis

1. Determine which systems were impacted, and immediately isolate them.
2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
3. Triage impacted systems for restoration and recovery.
4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.
5. Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.





DATAPRISE

## Containment and Eradication

**If no initial mitigation actions appear possible:**

6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected).
7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

**To continue taking steps to contain and mitigate the incident:**

8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
9. Identify the systems and accounts involved in the initial breach. This can include email accounts.
10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration.
11. Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.
12. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.
13. Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible.
14. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.
15. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.

## Recovery and Post-Incident Activity

16. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.
17. Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.
18. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community.





DATAPRISE

# Bonus: Incident Response Tabletop Exercise

This exercise is designed to spark discussion within your IT department on your organizational preparedness for a cyberattack in the highlighted scenario and provide tangible guidance on areas to improve.

### Getting Started: How to Use This Exercise

Tabletop exercises are designed to help organizations walk through potential cyber risk scenarios, evaluate cybersecurity posture, and identify potential gaps.

This exercise is meant to be a constructive and convenient tool that can be completed within 30 minutes. We recommend the below tips to provide the most value to your organization:

1. Involve all relevant IT stakeholders
2. Tailor the scenario to best match your environment
3. Determine a single facilitator for the exercise
4. Encourage discussion about how your organization would handle the scenario
5. Document your responses to the key questions
6. Develop a plan to close any gaps identified during the exercise

## Scenario Set-Up:

Your IT department has received numerous complaints from employees that their machines are running slow and are facing difficulties when trying to access the network. Your Systems Administrator takes a closer look at your network logs and discovers that there is an unauthorized intruder in your IT environment.

### Questions to Discuss

| | |
|---|---|
| 1. What do you do first? | 2. How do you determine the impact of the intruder? |
| 3. What do you have in place to contain the intruder? | 4. Can the intruder access your critical data? |
| 5. Who do you notify about the incident? | 6. What steps will you take to reduce risk in the future? |

# Dataprise Managed Cybersecurity

Dataprise Managed Cybersecurity solutions provide the real-time detection, validation, reporting, and response capabilities needed to protect an organization's IT environment from end-to-end.

We expertly combine a world-class managed detection and response with a complete cybersecurity program to increase visibility, shut down bad actors quickly, and dramatically improve your total security posture.

Beyond next-gen cyber technology, you receive an elite security team defending and protecting your organization 24x7 at a fraction of the cost of building the capability in-house. Our security professionals, analysts and hunters are always on and ready to detect, investigate and remediate any threat, any time.

### IDENTIFY

We identify your assets, the threats to those assets, and your vulnerabilities to those threats.

### PROTECT

We fortify your security layers with a focus on endpoints and users.

### DETECT

We uncover threats fast by linking data, intelligence, automation and analysts.

### RESPOND

We stop attacks in their tracks before they can impact your business.





DATAPRISE

DATAPRISE

# LET'S TALK!

1.888.519.8111
www.dataprise.com

## Why Dataprise

Founded in 1995, Dataprise is the leading strategic IT solution provider to midmarket IT leaders who believe technology should allow you to be the best at what you do.

Our broad solution portfolio is tailored to the needs of strategic CIOs and provides best-in-class managed security, network, infrastructure, collaboration, mobility, and end-user solutions.

### We Enable Strategic IT Leaders to Focus on Their Mission

At Dataprise, we handle the technology, so you can focus on your organizations mission. We leverage our in-depth knowledge of your industry, talent, and our best-in-class services to provide you with a winning formula to help your business succeed above its competitors.

### We Have a Deep Pool of Expertise

With over 300+ certified IT experts skilled in technologies across cybersecurity, infrastructure, mobility, and more, our team works with your organization to ensures your IT challenges are tackled efficiently and effectively.

### We Deliver Integrated, Resilient Solutions

We manage and support effective, resilient IT infrastructure that enables midmarket CIOs to focus on their strategic priorities to compete with unique advantages in their markets. Dataprise does this by leading with cybersecurity, the only way to protect a company and its sensitive data. While our services are comprehensive and integrated, they are also modular, so midmarket companies with some internal IT resources can get the help they need in specific areas.

DATAPRISE