Ransomware Guide

DWT's Ransomware Guide is intended to provide general information and considerations when preparing for and responding to a ransomware attack. It is not legal advice and should only be used for informational and reference purposes.

Our Information Security & Data Breach Response Team can help you develop a ransomware playbook tailored to your organization and business, either as part of our Ransomware Response Workshop or as a standalone project.

Preparation and Prevention

Effective ransomware response begins well before any attack. Below are several steps organizations can take to reduce the likelihood of a ransomware attack and better prepare their response and recovery should such an event occur. These steps are based on various regulatory guidance and best practices, including those referenced at the end of this guide.

Tune Up Your Incident Response Plan (IRP)
Ransomware preparations are a good opportunity to revisit (or create) your IRP and refresh it as needed. Consider drafting ransomware-specific processes and tactics into your IRP or developing an accompanying playbook or runbook focused on ransomware response. You can use the "Response and Recovery" section of this guide as your starting point for your own ransomware guide.

Hold a Tabletop or Other Incident Response Exercises
Practice responding to a simulated ransomware incident with your incident response team and your executive leadership. These exercises can educate stakeholders about the risks and challenges of ransomware and can help identify where your response processes need improvement.

Establish Provider Relationships and External Contacts
Identify outside counsel, digital forensics and incident response (DFIR) firms, public relations firms, and other outside support you might need to engage following a ransomware attack. Know how to contact and engage these firms quickly. Consider establishing good points of contact with the Federal Bureau of Investigation (FBI) and other law enforcement agencies.

Develop a Business Continuity and Recovery Plan
Imagine that ransomware has taken down your entire network and that full recovery will take weeks. Then develop a detailed plan for maintaining a minimum level of operations and prioritizing systems for a phased restoration.

Assess and Implement Detection and Hardening Measures
The U.S. Cybersecurity & Infrastructure Security Agency (CISA), the National Institute for Standards & Technology (NIST) and others have published numerous recommendations on technical defenses and mitigations against ransomware. These include:

- Network segmentation;
- Vulnerability scanning;
- Third-party penetration testing and security audits;
- Regular software patching, particularly of Internet-facing systems;
- Multifactor authentication;
- Deletion of unused user/service accounts and restricting account permissions according to the principle of least privilege;
- Disabling or hardening protocols frequently exploited by attackers, such as Remote Desktop Protocol (RDP) and Server Message Block (SMB);
- Email filtering and email spoofing protections;
- Deployment and monitoring of endpoint detection and response (EDR) tools and intrusion detection and prevention systems (IDS/IPS);
- Application allowlisting; and
- Built-in security and hardening measures for cloud-based systems.

Evaluate and Test Your Backups
Robust and secure backups are a game-changer for effective ransomware recovery. Best practices for backups include taking steps to:

- Develop and implement a backup strategy: In an ideal world, you could back up all your data on a continual basis. In the real world, with storage and bandwidth limits and other practical hurdles, an organization needs to identify its high-priority systems and data and establish a manageable schedule for backing them up. A good backup strategy incorporates legal, business, and IT security considerations.
- Maintain offline or segmented copies of backups: Backups are a prime target for ransomware attackers looking to assert leverage over their victims. Maintaining backup copies offline or in a segmented network helps keep critical data accessible for restoration. When restoring backups, proceed with caution: backups can be infected if they are reconnected to an infected network.
- Test backup procedures and solutions regularly: The middle of a ransomware attack is a terrible time to discover that your backups are corrupt or otherwise nonviable. Regularly test backups to make sure they work as you expect.

Emphasize Employee Training and Awareness
Ransomware attackers often gain a foothold into victim networks through phishing and other social engineering attacks. Train employees to identify phishing emails and other suspicious activity, including through organization-wide phishing tests. Make sure that your employees know how to report potential security incidents quickly, including when they are outside the office.

Scrutinize Your Service Providers
Third-party service providers can be a significant vector for ransomware attacks. Evaluate your service providers' contractual commitments on cybersecurity and, where feasible, require your service providers to undergo third-party auditing and certification.

Maintain Network Diagrams, Asset Inventories and Data Flow Maps
Good documentation of your computing environment is a powerful tool for responding to a ransomware attack. If you engage a DFIR firm, this documentation can help your provider get up to speed quickly and focus its efforts. It can also help you identify the best ways to isolate infected portions of your network, minimize business impact, and track the computers that must be cleaned and restored.

Response and Recovery

If ransomware is detected within your network, time is of the essence. Activate your IRP and review the following considerations as soon as possible.

Isolation and Containment of Impacted Systems
Your first priority must be to find and isolate infected systems to prevent further spread of the ransomware or other malware infection. Your ransomware playbook or runbook could include various options for isolating systems and network segments, depending on your network topography, physical availability of systems, and other factors. If possible, infected systems should be isolated but not powered down. Powering down a system will cause loss of key evidence stored in the computer's volatile memory.

Internal Communications Protocols
It is generally recommended that organizations use out-of-band communications methods during a ransomware attack. Your standard communications tools (email, chat applications, etc.) may be unavailable because of the attack, or attackers may be monitoring them to anticipate your response tactics.

Outside Counsel and Incident Response Firms
Consider engaging outside legal counsel and an external digital forensics and incident response (DFIR) firm to assist with your response. Your outside law firm typically will engage the DFIR firm—preferably one you do not use for routine matters—on your behalf to strengthen assertions of the attorney-client privilege and attorney work product protection.

Reporting and Notification
An organization may be required to notify government entities or affected third parties of the attack within a matter of hours or days, particularly if there may be significant operational disruptions or if sensitive data is compromised. Review the relevant legal and contractual requirements and determine your obligations as soon as possible. Consider whether you should notify certain external parties even if you are not required to do so.

Law Enforcement Engagement
You may decide to proactively notify law enforcement of the attack. Law enforcement may be able to provide actionable intelligence about the attackers and may ask you to share key evidence that you have gathered.

Threat Actor Engagement
Attackers typically will provide contact instructions in the ransom notes accompanying encrypted files. You should decide early in the response process whether you need or intend to engage with the attackers. Your DFIR firm or a specialized ransomware negotiation firm can assist you with attacker engagement.

Decision to Pay a Ransom
Perhaps the hardest decision you will face following a ransomware attack is whether you should pay a ransom. Important considerations include:

- Ability to restore: Determine your ability to restore your operations without paying the ransom. Examine the state of your backups and your ability to rebuild affected systems and services.
- Restoration timeframe: Keep in mind that restoration of your network and operations may take a considerable amount of time even if you pay a ransom. Consult your technical team to determine how much downtime and disruption you realistically are likely to save by paying the ransom.

- "Double extortion": Numerous ransomware groups engage in "double extortion"—encrypting files and threatening to publicly release data stolen from the victim network. Consult your legal and technical teams to determine if sensitive data was exfiltrated from your network and to evaluate the importance of preventing further disclosure.
- Legal risks: In some cases, such as where an attacker is on a U.S. sanctions list, paying a ransom can have serious legal consequences. Work with your legal counsel to identify and navigate this potential liability.

Investigation and Remediation
It is critical that you conduct a thorough investigation of the attack and remediate threats before substantially restoring your operations. Key goals for this process include:

- Identify IOCs and TTPs: Search for indicators of compromise (IOCs)—such as bad IP addresses, file names and hashes of malicious software, and compromised accounts—and evidence of other attacker tactics, techniques and procedures (TTPs). Leverage intelligence from law enforcement and your DFIR firm.
- Eradicate backdoors and other threats: Ransomware attackers typically seek numerous ways to access your network, including by deploying software "backdoors." Find and securely remove malware, block bad IP addresses, rotate compromised passwords, and take other necessary actions to secure your network.
- Data exfiltration: Determine whether the attackers accessed or exfiltrated sensitive data, such as sensitive personal information or business confidential materials. As noted, the attackers may attempt "double extortion" by threating to release such data if you do not pay the ransom. Access to or exfiltration of personal data may also trigger breach notification obligations.

Secure Restoration
Reconnecting an infected computer to an otherwise clean network can be a costly error. Develop and follow a clear protocol for securely reconnecting your network. Before reconnecting a computer to the network, consider:

- Scanning for and remediating any IOCs or other bad activity;
- Installing additional threat detection and response tools;
- Adopting additional device and network hardening measures (for example, closing unnecessary ports and limiting user admin permissions); and
- Wiping and rebuilding computers from clean images as necessary.

SEC Disclosure
Publicly traded companies must determine whether to disclose the attack in required securities filings and other public statements. Ransomware attacks may be material events for the purposes of SEC regulations, both because of the significant operational disruptions they cause and the potential exposure of sensitive data. If you are required to disclose the attack (or otherwise choose to do so), work with your legal and technical teams to carefully and accurately craft your public statements.

Contacts

Michael T. Borgia
PARTNER
202.973.4282 | Washington, D.C.
michaelborgia@dwt.com

Alex Reynolds
COUNSEL
202.973.4251 | Washington, D.C.
alexreynolds@dwt.com

Kristen N. Bertch
ASSOCIATE
202.973.4249 | Washington, D.C.
kristenbertch@dwt.com

DWT Insights

Bookmark or subscribe to our Privacy & Security Law Blog for timely updates on important news and information concerning the dynamic field of data security.