

# Ransomware Attack Response: What to Expect and Next Steps



A ransomware attack can cripple business operations and put your employees at risk. Attackers often go beyond just encrypting data—they steal personal and company information, attempt to manipulate employees, and can disrupt critical communication channels.

This document outlines what to expect, how we will assist in recovery, and why certain security measures are necessary to protect both your business and your staff.



## Immediate Actions

### Contact Your Insurance Provider

- Cyber insurance (if available): Notify them immediately, as they may cover forensic investigations, legal fees, and ransom payments if applicable. They often dictate specific recovery steps, that if not followed, result in denied claims down the road.
- Commercial insurance (if no cyber policy exists): Even without cyber insurance, some policies provide coverage for business interruption or recovery assistance.

### Get Your Attorney Involved

- They understand your business needs and regulatory requirements.
- Ensures compliance with breach notification laws and other legal obligations. These can be especially important in cases where you are a supplier or contractor to the federal government, a large retailer, involved in healthcare, etc.
- Manages breach disclosures to customers, employees, and authorities to mitigate legal risks.
- They should be involved in any ransom negotiations, if not directly, at a minimum they should be listening in on negotiation calls. Most Incident Response (IR) organizations have specialists that handle the primary negotiator role.

### Secure Communication: Using Burner Accounts & Alternative Channels

- Ransomware attacks often disable email, messaging apps, and internal communication platforms.
- To maintain secure communication:
  - We will establish temporary (burner) email accounts for critical coordination between your company's designated liaison and our response team.
- Employees should avoid using their compromised business email and instead communicate via:
  - Temporary personal emails (if safe).
  - Text messages or encrypted messaging apps (e.g., Signal, WhatsApp).
  - Phone calls via a designated hotline.
- This prevents attackers from monitoring discussions and interfering with the response process.



**Insurance**



**Attorney**



**Communications**



## Employee & Account Security

### Account Assessment & Controlled Reconnection

- Attackers often steal credentials, allowing them to regain access even after the initial attack is contained.
- We methodically reconnect users (artificially slowing the reconnection process) to ensure all access points are resecured before restoring user accounts. An error during this process could result in reinfection.

### The Personal Impact on Employees

- Attackers may have stolen employee phone numbers, addresses, and personal emails from HR or other internal databases.
- We have seen cases where:
  - Employees receive threatening calls from attackers, claiming their employer “doesn’t care about them.”
  - Attackers pose as IT staff or law enforcement to manipulate employees into revealing more information.

### Credit Protection & Personal Security for Staff

- If employee data was compromised, offering credit monitoring and identity theft protection is strongly recommended.
- Employees should be advised to:
  - Ignore calls or emails from unknown sources regarding the attack.
  - Report any suspicious activity (such as phishing attempts, fraudulent credit applications, or unauthorized transactions).



**Assessment**



**Employees**



**Protection**



## Strengthening Security Post-Attack

### Cloud Security Adjustments

- We will review and reinforce cloud access controls to ensure:
- Only authorized personnel have access to sensitive data.
- Multi-Factor Authentication (MFA) is enforced.
- Access logs are monitored for unusual behavior.

### Drop Remote Connections, Enforce MFA, Mandate Password Changes

- Attackers may have installed backdoors to maintain access even after the initial attack is mitigated.
- To cut off any remaining threats, we will:
  - Terminate all remote sessions and VPN connections.
  - Require new MFA enrollments before restoring access.
  - Implement mandatory password resets (timed strategically to avoid attacker interference).

### External Accounts & Related Exposures

- You should assume that the hackers have gained access to passwords for outside accounts as well. You should immediately change all of these passwords and where supported, implement MFA. These may include:
  - Banking and investment accounts
  - Vendor supply-chain platforms
  - Shipping and receiving tools (FedEx, UPS, etc.)
  - Expense reporting and payroll sites (ADP, Workday, Paychex, etc.)
  - Remote access/VPN accounts to third parties (Citrix, AnyDesk, etc.)
  - Cloud storage and collaboration accounts (Dropbox, BOX, Sharefile, etc.)
  - CRM tools such as Salesforce, HubSpot, Zendesk, etc.)
  - Project management and development tools (Jira, Asana, Trello, GitHub, Bitbucket, etc.)
  - Social media accounts used by the business (Facebook, Instagram, LinkedIn, X, TikTok, etc.)
  - Additional email services (Gmail, Yahoo, Outlook.com, etc.)
- Many organizations have copies of documents stored in local machines such as state and federal tax returns, spreadsheets with shared online passwords, etc. Assume that all of these have been accessed and are compromised. Speak with us about deployment a password management platform to store these types of details in a secure fashion.



**Cloud**



**Enforcement**



**Exposure**



## Investigation & Long-Term Protection

### Identifying the Root Cause

- We must determine how the ransomware entered—whether through phishing, software vulnerabilities, or compromised credentials.
- A forensic investigation will trace the attack's entry point and ensure no residual threats remain. For this work, we will introduce you to an Incident Response (IR) partner who specializes in this work. If you have cyber-insurance, the IR provider will likely have been introduced to the team already.

### The Use of Incident Response (IR) Professionals

- IR teams specialize in cybercrime investigations and can uncover attack methods that standard IT teams might miss. They offers tools and techniques for collecting detailed log history from all of the devices in the environment (workstations, servers, firewalls, etc.). They also have a strong methodology that helps to minimize the possibility of reinfection.
- They will analyze:
  - Network traffic and endpoint logs to detect hidden threats.
  - Potential data exfiltration to assess if sensitive files were stolen.

### Potential to Acquire/Approve Funding for Replacement Equipment

- As part of the incident response, it's important to preserve machines and their logs for future reference. In many cases, we'll replace the hard drives with new ones (likely SSDs), but depending on the age of the machine(s) involved, it may make sense to replace them altogether. Be prepared to discuss the cost of enhancements/replacements like this.
- There is always an opportunity to improve your security practices such as:
  - Implementing updated firewalls to better protect the edge of the network
  - Breaking down the internal network into different zones, blocking lateral access and limiting the likelihood of spread during an attack.
  - Evaluating your wireless security, ensuring that you don't use simple passphrases to protect access to your private network, but instead, that you use actual domain login credentials to gain access to these resources (this prevents the ex-employee in the parking lot type of attack).
  - Improving your cloud security controls with enforced MFA, stronger conditional access policies, cloud activity monitoring for unusual travel, the creation of new administrative accounts, etc.



**Investigate**



**Respond**



**Replace**



## Moving Forward

### Key Takeaways

- **Protect Your Staff:** Employees may receive threatening calls, phishing emails, or fraudulent identity attempts—it's critical to provide security awareness and credit protection as needed.
- **Use Alternative Communications:** Email and internal tools may not be safe after an attack. We will establish burner accounts and recommend secure alternatives for essential communication.
- **Security Enhancements Are Non-Negotiable:**
  - All users will be required to use MFA.
  - Cloud access controls will be tightened.
  - Remote access will be restricted until secured.

### Conclusion

A ransomware attack is more than an IT issue—it's a business and employee security crisis. Our response strategy ensures that your operations, data, and employees remain protected throughout the recovery process.

If you or your employees experience suspicious activity, including harassing calls or unauthorized login attempts, report it immediately.

We are here to guide you through this process and strengthen your defenses for the future.

# Cybersecurity Solutions

Safeguard Your Business with Exigent Cybersecurity Solutions

## 360° Cybersecurity Protection

Cybersecurity ranks as one of the most troubling challenges for business leaders. The reasons are clear. According to the 2024 Threat Report from cybersecurity industry leader SonicWall:



Small businesses are 3x more likely to be targeted by cyber attacks



In 2024, cybersecurity experts reported a 202% rise in phishing attacks.



Intrusion attempts grew by more than 20%

Exigent approaches cybersecurity methodically, starting with the fundamental protection included in our **Assurance Managed IT Services**. Then, based on your organization's particular cybersecurity needs and challenges, we build a custom cybersecurity ecosystem to protect your valuable assets.

## Exigent Cybersecurity Solutions

### Boundary

*Firewall-as-a-Service*

Firewalls are one of your organization's first lines of defense. With Boundary Firewall-as-a-Service, Exigent's certified experts shoulder the responsibility of optimizing next-gen firewalls in a monthly subscription model. [Learn More](#)

### Fortify Complete

*MDR + SOC*

Fortify was purpose-built to address the unique challenges of protecting data and assets in today's dispersed environments. By offering advanced detection across three threat surfaces – endpoint, network and cloud – your organization gains broader protection wrapped in a live 24/7 SOC. [Learn More](#)

### Veracimail

*Email Security*

Our managed spam filtering and email security service mitigates the risks of spam and threatening content, preventing threats from reaching your inbox and eliminating the headaches, wasted time, and dangers of unsolicited email. [Learn More](#)

### Vigilant

*Security Awareness Training*

Educate your team on how to spot suspicious activity and create new, safer habits. Effective security awareness training improves your company's cybersecurity culture and reduces phishing email clicks by your employees by as much as 70%. [Learn More](#)

### Informant

*Dark Web Monitoring*

Our monitoring subscription service alerts you if our platform uncovers email addresses, passwords, or personally identifiable information related to your organization on the Dark Web. [Learn More](#)

### Ethical Hacking and Assessment Services

- Third-party risk assessments
- Penetration testing
- Vulnerability testing
- Cybersecurity consulting
- Regulatory compliance assessment and consulting