FS-ISAC Akamai

# Ransomware Essentials: A Guide for Financial Services Firm Defense

October 2024

## Introduction

Ransomware is one of the few threats that can truly disable a financial services institution. Increasingly innovative, aggressive, and frequent, ransomware attacks can disrupt customer services, halt business operations, and damage the institution's standing with customers and regulators.

This document aims to help the sector address ransomware threats. Using operational insight from FS-ISAC and its members, it's particularly useful to information technology (IT) professionals, those who develop cyber incident response policies and procedures, and those who coordinate incident responses. The paper focuses on:

- Ransomware mitigation best practices
- Incident response/crisis management
- Considerations on paying ransoms
- Resources for further study

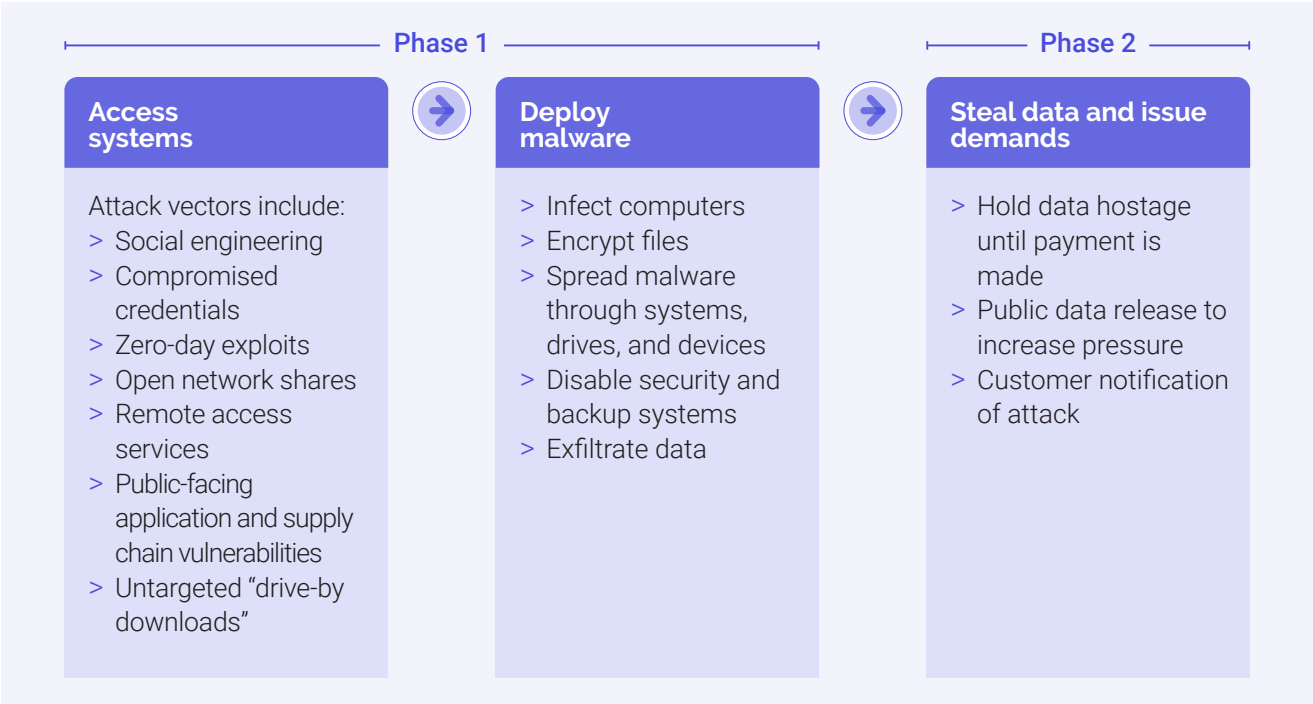
**Ransomware is on the Rise**

| | |
|---|---|
| ⬆ 70% | Increase in observed events[1] |
| ⬆ 64% | Ransomware attacks on the financial services sector[2] |
| ⬆ 4,374 | New victims over the last 12 months[3] |

## Phases of a Ransomware Attack: Infect and Encrypt, Exfiltrate and Harass

Ransomware is a form of extortion that has developed into a two-phase attack – first encryption and data exfiltration, then demands for payment and harassment to speed the ransom payment.

Threat actors execute the first phase by gaining access to the victim's computer systems and deploying malicious software (malware) to infect the victim's computers and encrypt their files.



### Ransomware-as-a-Service

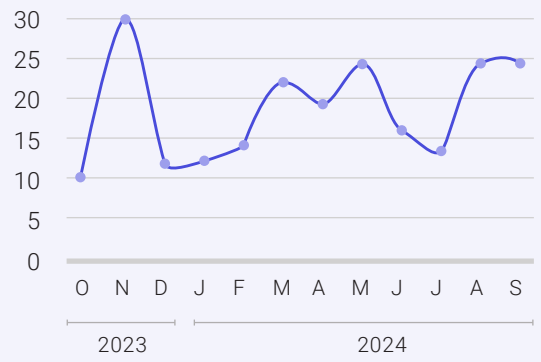
Some criminal groups build and sell malware to other threat actors, enabling successful attacks by low-skill criminals. Other ransomware groups – like REvil, LockBit, and CL0P – employ advanced techniques to infiltrate financial institutions, steal sensitive data, and demand ransoms.

Usually, threat actors attempt to spread the malware across the financial firm's connected systems, including shared storage drives and other accessible devices – ransomware is often deployed as a secondary payload after a device has been compromised by other malware. Such malware can be so destructive that it renders the victim's systems inoperable.

The top ransomware threats are human-operated attacks, often facilitated by criminal organizations that sell initial access or bots as a service. Once threat actors access the network, they move laterally to disable security tools and backup systems. These attackers often have extensive knowledge of systems administration and common network security misconfigurations (GenAI makes them easier to find), enabling them to perform thorough reconnaissance and adapt to what they discover in a compromised network.

The second phase is the exfiltration of data, followed by a 'hostage' demand (also known as Leakware or Doxware) in exchange for the encryption key to the data. In a triple extortion attempt, threat actors also launch a DDoS attack so the financial firm can't operate the business. In a quadruple extortion attempt, cybercriminals leak data and contact customers, employees, business partners, media, and even regulators to inform them of the data compromise and accelerate the payment.

**Events** | Last 12 Months




*Ransomware events in the financial sector over the last 12 months. Source: eCrime Threat and Risk Intelligence Services*[4]

Despite law enforcement crackdowns, these groups rapidly adapt, using new infrastructure and evolving tactics and an irregular cadence of attacks.

Many ransomware attacks intertwine financial motives with geopolitical agendas. Hacktivist groups like Anonymous Sudan and KillNet, driven by geopolitical conflicts like the Russia-Ukraine war, have increasingly targeted critical banking infrastructure.

## Proactive Ransomware Defense: Cyber Fundamentals, Crisis Management Plans, and Best Practices Protect Your Firm

One of the most frustrating – and dangerous – aspects of a ransomware attack is the loss of access to necessary tools. A compromised firm may not have access to its SOC or forensics tools. Systems like email and communications infrastructure may also be offline or untrustworthy. Therefore, ransomware incident response plans should include workarounds and the ability to rapidly restore or replace a minimal set of critical capabilities to maintain operations.

## Build Cyber Hygiene Fundamentals into Your Technical Controls

As a contribution to the sector's defense, FS-ISAC recently released Cyber Fundamentals, a risk-based approach using Defense-in-Depth principles appropriate to any financial services institution at any level of cyber maturity. Of the Cyber Fundamentals' 16 recommendations, the following six are the most relevant to ransomware defense.

### Cyber Fundamentals Checklist:

1. Isolate, test, and exercise backups
2. Update software, automate patching
3. Require MFAs and strong passwords
4. Train employees
5. Write and exercise incident response plan
6. Use EDRs, DLPs, and firewalls

### 1 Use non-erasable and non-modifiable backup systems to duplicate data and system configurations

> Regularly back up critical data and system configurations to isolated environments. If segmentation is in place and backups are preserved, the impact of an attack may be manageable.

> Test backups at least annually in real-world technical exercises to ensure backups can be restored quickly and completely in the event of an attack. Cloud computing makes testing and restoration easier, but some firms may only be able to test restoration of certain critical functions. A robust restoration plan, likely on a separate new infrastructure, will take a great deal of effort, especially in large firms.

### 2 Regularly update and patch software

> Updates and patches reduce initial infection potential from both technical and social engineering attacks.

> Where the risk is acceptable, automate patch management to ensure consistent application of updates across all systems, reducing human error and delays.

> If patching is delayed, develop standard processes to implement mitigation strategies like virtual patching utilizing a web application firewall (WAF).

### 3 Use a zero-trust and least privilege policy with multi-factor authentication, and require strong passwords for every employee, device, and account

> Implement a zero-trust approach where all users and devices, inside or outside the network, are authenticated, authorized, and continuously validated before gaining access to applications and data.

> Leverage resources like NIST 800-207 Zero Trust Architecture to develop your strategy.

### 4 Train employees on their role in cybersecurity

> Conduct regular training sessions to educate employees on the latest cybersecurity threats, including phishing, social engineering, and the dangers of clicking on unknown links or downloading unverified attachments. People who understand the potential impact of clicking on external links or reusing passwords will generally take more care about their activities.

### 5 Develop an incident response plan specific to ransomware attacks

> Detail the steps to be taken immediately upon detection, including isolation, communication, and recovery procedures.

> Conduct regular tabletop exercises and full-scale drills to ensure that all team members are familiar with the response plan and can act quickly and effectively under pressure. Exercises allow you to review and update plans to adapt to evolving threats and changes in your organization.

### 6 Implement EDR, DLP, and firewall solutions

- Implement Endpoint Detection and Response (EDR) solutions. EDR solutions monitor endpoints (computers, servers, mobile devices) for suspicious activity, and respond to threats in real-time to disrupt ransomware before it can spread.
- Implement Data Loss Prevention (DLP) solutions. DLP solutions monitor and control the movement of sensitive data, helping to prevent exfiltration attempts by cybercriminals.
- Use firewalls, configured closed by default, with active blocking. When deploying firewalls, look at internal segmentation as well. One example is agent-based microsegmentation augmentation of traditional firewalls, which minimizes the potential impact of encryption malware. Another key control for exfiltration monitoring is a SWG/DNS firewall that can detect data being stolen and prevent users from going to malicious websites.

## How to Develop and Implement a Crisis Management Plan

**Crisis Management Plan Checklist:**

- Policy on paying ransoms
- Crisis management framework
- Roles and responsibilities

Ransomware presents a unique challenge in that the time between detection and impact – the flash to bang – is essentially zero. Unlike cyber incidents that unfold over weeks, ransomware requires immediate execution of crisis management plans in real-time, without some of the normal phases of mitigation.

While the technical controls mentioned above are critical to defending against and responding to a ransomware attack, process-based capabilities are equally important. A crisis management plan must involve the entire leadership team and include a clear policy on whether to pay the ransom. If your legal team approves paying, you'll need to have a contract with a payment negotiator and be prepared to purchase cryptocurrency – most criminals require ransom payment in crypto.

Next, consider how to respond effectively if an attack is successful. You will need both a strategic crisis management plan and a tactical response plan. The ISO 2700 is a great framework, as is the NIST 2.0 crisis management framework (and it's the baseline for all FFIEC guidance). That framework helps you plan the essential factors of strategic and tactical responses.

As you build out the plan, identify the Incident Response (IR) team. It should include functions from across the organization. All their actions should be driven by the Responsible, Accountable, Consulted, Informed (RACI) model.

**Strategic Response Framework**

- Mission statement
- Strategies and goals
- Senior management approval (signed off/on)
- Organizational approach to incident response
- IR team's communication with the firm
- Metrics for incident response capability and effectiveness
- Roadmap for maturing the incident response capability
- IR program's role in the overall organization

| Crisis Management Team | |
|---|---|
| **Senior Leadership** | > Chief Executive Officer<br>> Chief Financial Officer<br>> Board of Directors |
| **General Counsel and Legal/ Risk Management Consultants** | > General Counsel<br>> External cyber SME advisor<br>> Ransomware consultants/payment experts<br>> Law enforcement agency (LEA) liaison<br>> Cyber insurance liaison |
| **Communications/ Public Relations** | > External cyber incident SME |
| **Operations** | > IT leadership<br>> Call centers, customer service, and related functions<br>> Business continuity planning team |
| **InfoSec** | > IR/SOC<br>> Threat intel<br>> Forensics teams<br>> External forensics experts |
| **Vendor Management** (lead team if ransomware impacts vendors) | > Third-party risk management |
| **Human Resources** | > Employee communications<br>> Staff support and counseling |

As you think about the team's tasks, determine:

- A plan for early detection of malware and post encryption if the malware is not discovered before it executes.
- A plan to deal with the technical aspects of encryption and the external impact of data being released.
- The process and triggers to notify insurance, regulators, law enforcement agencies, and external subject matter experts (PR, forensics, legal).
- The process and sequence for board, regulatory, employee, and public notifications.
- A process for dealing with key vendors impacted by the breach or ransomware.
- Third-party management including:
  - > Vendor breach impact assessment
  - > Third-party communication plan
  - > RACI for this process
- How to tie the business continuity/disaster recovery plan to the crisis management plan.
- The systems necessary to collect and preserve forensic evidence, maintain a chain of evidence, and track the sequence of events – remember, this is a crime.
- How to collaborate with law enforcement, and the relationships and processes needed to share intelligence.
- Testing/exercises that drive validation. A great resource to design the threat scenario and build out the master scenario events list (MSEL) is the Cybersecurity and Infrastructure Security Agency's (CISA) Tabletop Exercise Packages. In any case, testing and exercises should be:
  - > Regularly scheduled with documented improvement plans.
  - > Scenario-based, with drills for the different types of activities involved with current ransomware trends.
  - > Designed to make sure all the steps in the crisis management plan are exercised, whether tabletop or technical.

## Should You Pay the Ransom? The Risks, Regulations, and Factors to Consider

FS-ISAC does not encourage paying a ransom to criminal actors. Ransoms fund further criminal activities and perpetuate the ransomware business model. However, the decision requires the evaluation of all options to protect shareholders, employees, and customers when systems are compromised. It's a serious, individual business decision, so ransomware victims should consider the following risks:

- You may or may not regain access to the data. After paying the originally demanded ransom, some victims have been asked to pay even more to get the promised decryption key. Some individuals and institutions paid but were never given decryption keys.
- You are not protected from future attacks. Some victims who paid the demand were targeted again.
- You may be out of compliance. Laws and regulations vary across jurisdictions, but many apply specifically to financial services institutions. In her book, Digital Empires: The Global Battle to Regulate Technology,[5] Anu Bradford covers three overarching approaches to governing the digital landscape: market-driven, state-driven, and rights-driven. Examples of state-driven governance of ransomware responses include:
  - **In the US:** The US Department of the Treasury's Office of Foreign Assets Control (OFAC) has imposed sanctions on a number of cybercriminal threat actors and groups – by paying a ransom you may be violating those sanctions. Victims who pay ransoms might also be subject to criminal or civil penalties, such as those who knowingly pay an entity either designated as a foreign terrorist organization or that is subject to sanctions by the Department of the Treasury.

    Moreover, federal cybersecurity preparedness laws require federal agencies to secure their networks and authorize CISA and the Office of Personnel Management (OPM) to establish federal network security requirements. The US states of Florida, Indiana, Louisiana, North Carolina, and North Dakota require public entities to report ransomware incidents. The Computer Fraud and Abuse Act (CFAA) can be used to prosecute those who perpetrate ransomware attacks.
  - **In the UK:** The UK has enforced financial sanctions under the cyber sanctions regime since May 2019, introduced when the UK was part of the European Union (EU). Following the UK's exit from the EU, the Cyber (Sanctions) (EU Exit) Regulations 2020 (the Regulations) were introduced under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA).[6]

    Facilitating a ransomware payment may breach UK sectoral sanctions or the law of other jurisdictions. The Foreign, Commonwealth and Development Office (FCDO) has produced guidance on each sanctions regime that gives details of sectoral sanctions.
  - **In Australia:** Making or facilitating a ransomware payment may breach Australian sanctions laws and result in criminal penalties where such payments are made to persons or entities subject to Australian autonomous sanctions laws.

## References and Further Reading

FS-ISAC Cyber Fundamentals

MS-ISAC #StopRansomware Guide

CSBS Ransomware Self-Assessment Tool

IC3 reporting and annual security trends

UK National Cyber Security Centre Guidance

Europol tips to prevent ransomware

### Original report references


Cybersecurity and Infrastructure Security Agency (CISA): "Reduce the Risk of Ransomware" Awareness Campaign

Cybersecurity and Infrastructure Security Agency (CISA): Ransomware Guide

Cybersecurity and Infrastructure Security Agency (CISA): Stop Ransomware Webinars

Cybersecurity and Infrastructure Security Agency (CISA): Stop Ransomware Fact Sheet

Cybersecurity and Infrastructure Security Agency (CISA): Protect your Center from Ransomware

Federal Bureau of Investigation (FBI): Common Scams and Crimes – Ransomware

Federal Bureau of Investigation (FBI): Ransomware Prevention and Response for CISOs

Europol: "NoMoreRansom" International Initiative

National Cyber Security Centre (NL): Ransomware

National Cyber Security Centre (UK): Phishing Attacks: Defending your Organisation

National Cyber Security Centre (UK): Ransomware: What Board Members Should Know About Ransomware

National Cyber Security Centre (UK): Mitigating Malware and Ransomware


## Endnotes

1 Increase in observed ransomware events: Ransomware and Data Leak Site Report, March 2023 - eCrime.ch

2 Ransomware attack increase on the financial services sector: ABA's Banking Journal

3 New victims over the last 12 months: Orange Cyberdefense

4 Ransomware attacks in the last 12 months https://ecrime.ch/

5 Anu Bradford: https://scholarship.law.columbia.edu/books/367/

6 UK cyber sanctions regime: https://www.gov.uk/government/publications/financial-sanctions-cyber-attacks#:~:text=The%20Cyber%20(Sanctions)%20(EU%20Exit)%20Regulations%202020%20put,country%20other%20than%20the%20UK