Board Briefing: Protection Against Cyberextortion and Ransomware

Briefing and action steps for boards and the C-suite
Context for This Report

Methodology
• Board briefing topics are selected based on client interest and frequency of topic coverage in legal, compliance, privacy and security media sources.

Goal of this report
• Provide context, expert opinions and recommended actions to facilitate effective board discussions on news topics with legal, compliance, privacy and security implications.

How to use this report
• Review the slides to gain critical context.
• Customize and use the slides to facilitate a discussion with your board.
Ransomware Attacks: Examples From the Headlines
Victims of Ransomware Attacks

Colonial Pipeline Company

- In May 2021, Colonial Pipeline, which transports 2.5 million barrels of fuel a day and provides 45% of the East Coast’s fuel supply, was victim to the Darkside ransomware attack.\(^1\)

- The hackers stole, copied and encrypted nearly 100 gigabytes of sensitive data, holding the data hostage and threatening to leak it.

- The cyberattack forced the company to freeze its IT systems and shut down its operations for six days.

- The CEO of Colonial Pipeline authorized a $4.4 million payment of bitcoin to the hackers.

- The shutdown of the pipeline, although temporary, pushed the national average price of a gallon of gas past $3 for the first time in seven years.

Source: Gartner

JBS Foods

- In May 2021, a ransomware attack forced JBS Foods, the world’s largest meat processor, to shut down nine beef plants and disrupted production at poultry and pork plants.\(^2\)

- The attack affected systems in North America and Australia but did not impact its backup servers or expose any customer, supplier or employee data.

- While the origin of the attack is still under investigation by the FBI, JBS Foods reported that the ransom demand had come from “a criminal organization likely based in Russia.”

- Although the attack only significantly impacted JBS Foods’ operations for about one day, experts predict that the disruption could still significantly impact wholesale beef prices.

Source: Gartner
Victims of Ransomware Attacks

ISS World

- In February 2020, ISS World, a global facilities management company, was the target of a crippling ransomware attack.3

- The attack forced the company to switch off its networks, leaving its hundreds of thousands of employees without access to their systems or emails.

- ISS World spent between $45 to $75 million on remediating the IT incident, implementing workarounds to continue service delivery and managing the cost-of-service underperformance because of system downtime.

- ISS World expects to spend an additional $22.5 to $40 million on rebuilding its IT infrastructure due to damage to some of the company’s IT assets.

Source: Gartner

University of California, San Francisco

- In June 2020, after a month-long standoff with criminal hackers, UCSF reportedly paid $1.14 million, converted into bitcoin, to free its systems.4

- The university was able to successfully negotiate down the ransom payment by over half the original amount through external counsel.

City of Atlanta

- In 2018, the city of Atlanta was hit by the SamSam ransomware attack, costing city taxpayers more than $9 million.5

- The attack shut down the city’s online system and affected police systems.

- The attack exposed the city’s poor IT infrastructure and the need to fix its security vulnerabilities.
What Is Ransomware?
What Is Ransomware and How Does It Work?

Cyberextortion and Ransomware

- **Cyberextortion**: A hacker threatens to seize, damage or release electronic data owned by the victim.
- **Ransomware**: A type of cyberextortion where a form of malicious software infiltrates computer systems or networks and encrypts data, holding it “hostage,” until the victim pays a ransom.

Source: Gartner

Process

Ransomware usually enters an organization’s system through:

- a) **Email phishing campaigns**, prompting a user to click on a link, downloading the ransomware automatically, or
- b) Exploiting vulnerabilities in an organization’s security and IT systems.

The ransomware then spreads across all accessible IT systems, **encrypting the data** and making it **inaccessible to users**.

The cybercriminals then demand payment from the owners in return for access to the data or systems, in some form of **cryptocurrency**, usually bitcoin.

Payment must then be made within a few hours or days, after which the data will be permanently lost or erased.

Source: Gartner
Rate of Infection Requires Urgent Action

While ransomware can occur within seconds, it can cause an organization to lose access to its systems for multiple days or weeks, leaving companies unable to provide services to its clients, which can cost millions of dollars in damages. Some more insidious variants are slower-moving, gaining access to critical systems and accounts over time while destroying backups.

Infection to Encryption in 3 Seconds

User clicks on phishing email
User unknowingly downloads ransomware
Ransomware unpacks and executes
Ransomware downloads encryption keys
Ransomware scans computer to identify all attached drives
File encryption begins
User gets ransom notification

Source: Artic Wolf
A Growing Threat

Due to vulnerabilities exposed by the global pandemic and record highs in the prices of cryptocurrency (which has enabled anonymous and untraceable monetary exchanges) ransomware attacks have almost tripled since the beginning of 2019. Over 100 million ransomware attacks occurred in 4Q20.

246
County, city or state government organizations have been attacked since 2018.

$1,900,000
Demanded in bitcoin by hackers from a single organization in more serious cases.

34,000
Identified ransomware variants for sale on over 12,000 “dark web” marketplaces, causing companies millions of dollars in losses when combined.
Costs of Attack

Ransomware has an annual global cost of over $1 billion. As ransomware becomes a sustainable business option for cybercriminals and attack methods become more sophisticated, the costs associated with attacks will only continue to grow.

Source: GroupIB

Direct costs

Average cost of attack for a small business paying the ransom is $713,000.

Source: Gartner

Indirect costs

Cost of business that is lost during the hours/days that systems are locked and the costs of repairing or restoring systems.

Source: Gartner

Reputational harm

Bad reputation will cost organizations, their clients and customers.

Source: Gartner
How Do I Protect Against Ransomware?
Stakeholders Involved in Ransomware Protection

While several functions should be represented in a company’s ransomware protection group, the most critical stakeholders are assurance and IT and security.

Core stakeholder responsibilities

**IT and Security**: Ensure proper governance of IT systems and software applications across the organization.

**Communications**: Develop a crisis communications plan that accounts for third-party vendors, suppliers and other key stakeholders.

**Assurance**: Assess organization’s (and IT’s) preparedness to respond to an attack and manage potential systems failure.

**HR**: Ensure employees are appropriately educated on computer security and the threat of a ransomware attack.
Treat Ransomware Protection as an Investment

Businesses face a choice between investing to create better protection and saving money upfront while leaving themselves exposed to much higher costs down the line. Although protection can be expensive (e.g., restore testing), investments in ransomware controls are best understood in a business context that considers risk, value and cost.

This figure demonstrates how understanding ransomware protection in a strategic business context enables organizations to optimize ransomware risk and make targeted investments.

- **Business Unit A** is very business-critical but has a poor ransomware protection score. The organization should treat this business unit as a priority from an investment perspective.

- **Business Unit B** has lower business criticality and commensurately less sensitivity to unscheduled outages. It may be defensible to accept higher ransomware risks and lower investment in protection.

- **Business Unit F** has low business criticality but high levels of investment. This business unit may have overinvested in costs to have such a high ransomware risk score.
Summary of Ransomware Controls

Broadly speaking, there are three types of controls that determine an organization’s readiness to address a potential ransomware attack.

- **Backup and restore**: Primary capabilities get back data and resume normal operations.
- **Business continuity**: Allows the business to continue operating during recovery.
- **Phishing training**: Directly reduces the risk of a ransomware incident.
Gartner research shows that over 90% of ransomware attacks are preventable. Work with IT and security to ensure your organization has a robust security infrastructure with controls and processes to identify and fix vulnerabilities.

### Basic operational security best practices

1. **Test and reinforce restore capabilities:** Prioritize critical business processes to test annually with a full restore (a test to ensure that encrypted files can be successfully recovered). Assess restore readiness and determine where controls need to be strengthened (e.g., improve recovery speed by leveraging features of recovery solutions, such as automated alerts).

2. **Prepare to manage business continuity without technology:** Define manual continuity strategies for business processes that are unable to function in the event of an attack.

3. **Improve endpoint security:** Endpoint security refers to securing endpoints, also known as end-user devices (i.e., desktops, laptops and mobile devices). Endpoints usually serve as points of access to a company’s network, which make them vulnerable to cyberattacks. Consider the use of advanced endpoint protection that can identify new malware variants and detect malicious traffic by upgrading to the latest version of your endpoint protection platform (EPP) software.

4. **Implement network segmentation:** Put critical data on separate network segments and consider internal firewalls or physical separation. (Many organizations already make use of network segmentation with demilitarized zones [DMZs] used to separate internet-facing devices and internal infrastructure.)

5. **Update application patches:** Patches are updates to computer programs that include fixing security vulnerabilities. Ensure application patches, which use a central patch management system for the operating system, software and firmware, are up to date.

Source: FBI & Gartner
Gartner research shows that over 90% of ransomware attacks are preventable. Work with IT and security to ensure your organization has a robust security infrastructure with controls and processes to identify and fix vulnerabilities.

### Action Steps for IT and Security Partners

Gartner research shows that over 90% of ransomware attacks are preventable. Work with IT and security to ensure your organization has a robust security infrastructure with controls and processes to identify and fix vulnerabilities.

### Basic operational security best practices

6. **Run penetration/vulnerability testing:** Evaluate the state of your security resilience and preparedness in terms of tools, processes and skills to defend against attacks.

   - A vulnerability assessment is the process of identifying and quantifying security vulnerabilities by conducting an in-depth evaluation of your information security posture.
   - A penetration test simulates the actions of an external cyberattack to identify weaknesses in the company’s security controls (e.g., a company may send emails to the employee population that imitate a ransomware attack and provide employees with educational resources following the simulation).

7. **Strengthen firewalls:** Configure firewall rules to only permit the minimum ingress and egress traffic necessary to perform the organization’s business or to meet application and support needs.

8. **Restrict (write) access to shared documents and file servers:**

   Manage the use of privileged accounts by implementing the principle of least privilege.

   - Users should not be assigned administrative access unless absolutely needed. Those who require access should only use it when necessary, and they should operate with standard user accounts at all other times.
   - Examples of common ransomware locations include temporary folders supporting popular internet browsers or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Source: FBI & Gartner
Action Steps for IT and Security Partners

Gartner research shows that over 90% of ransomware attacks are preventable. Work with IT and security to ensure your organization has a robust security infrastructure with controls and processes to identify and fix vulnerabilities.

**Basic operational security best practices**

9. **Disable macro scripts**: Macros automate frequently used tasks but can pose a potential security risk as hackers often introduce a destructive macro in a file that can spread a virus into your organization’s network. Disable macro scripts from files transmitted via email and consider using Microsoft Office viewer software to open Office files transmitted via email instead of full Office suite applications.

10. **Use application approved list**: Application approved list is allowing systems known and permitted by the company’s security policy to be used.

11. **Scan all incoming and outgoing emails to detect threats, and filter executable files from reaching end users.**

12. **Enable strong spam filters to prevent phishing emails from reaching the end users.**

13. **Periodically secure separate copies of backups (outside of the usual process) to guard against the backups themselves becoming encrypted or destroyed by ransomware.**

Source: FBI & Gartner
After creating a cyber incident response plan and disaster recovery (DR) procedure, test them to understand the productivity impact and the time to restore systems for your organization.

**Action Steps for Assurance Partners**

- **Response plan:** Describes how an organization will respond to potentially catastrophic, computer-related incidents, such as viruses or hacker attacks.
  
  The plan should include steps to determine whether the incident originated from a malicious source — and, if so, to contain the threat and isolate the enterprise from the attacker.

- **Response team:** There is a team responsible for responding to security breaches, ransomware attacks and other potentially catastrophic incidents in organizations.
  
  The team should include technical specialists, as well as leaders from legal, risk, HR or the public relations team who can guide relevant stakeholders on appropriate communication in the wake of such incidents.

**Cyber incident/breach response plan**

**IT/DR plan**

- It is critical for technical professionals to develop a DR strategy that outlines a process to recover critical business applications, within a desired recovery time.

- A DR plan helps prevent organizational risk errors in process, long-term strategic misdirection and longer outages.

- Review the U.S. National Institute of Standards and Technology (NIST) *Guide for Cybersecurity Event Recovery*, which is used by federal agencies.

Source: FBI and Gartner
Action Steps for Assurance Partners

Implement a cyber education awareness and training program for employees, who are common targets in cyberattacks.

Cybersecurity education

Train and educate users about computer security

- Organizations should regularly educate and train all employees, particularly those dealing with sensitive data, on the threat of ransomware and its effect on an organization.
- Frontline employees are often targets to ransomware attacks and therefore should be educated on the following:
  - What is ransomware and how is it delivered.
  - How employees can identify and report threats to IT if they receive a suspicious pop-up.
  - Employee security best practices regarding the use of email, internet and social media, which are common points of access for ransomware, and which pose the most threat to an organization.

Leverage public resources on cybersecurity preparedness

- Review free ransomware simulation tools and other training collateral from KnowBe4. These can simulate 15 ransomware infection scenarios and one cryptomining infection scenario and show you if a workstation is vulnerable.
- Infosec IQ and many other vendors have a free trial of over 1,000 interactive modules, phishing templates and education reinforcement materials that can be used in conjunction with paid solutions.
- The U.S. government launched a new campaign called Know the Risk, Raise Your Shield. The effort includes videos and fact sheets.

Source: FBI, Gartner and Symantec
Action Steps for Assurance Partners

Consider getting cybersecurity insurance with cyberextortion coverage, which can cover some costs caused by ransomware.

Cybersecurity insurance

To mitigate the consequences against ransomware, consider cybersecurity insurance plans that offer cyberextortion/cyber-ransom coverage as part of the cybersecurity insurance, or are included as an added premium. Many cyber liability policies will cover the following types of costs caused by ransomware:

- **Ransom money**: Money paid to a cybercriminal in response to a ransomware attack. Some policies may also cover the property you give up because of a threat.

- **Extortion-related expenses**: Expenses incurred as a result of dealing with the threat, e.g., cost of hiring a consultant to help with negotiations with the cybercriminal.

- **Repair costs**: As paying the ransom doesn’t guarantee your files and systems will be recovered and left undamaged, cyber liability may cover losses you incurred as a result of any damage, theft or misuse of the data or systems caused by the attack. Other costs covered may include the cost to restore, replace or reconstruct programs, software or data.

Gartner recommends contacting your insurer before paying ransom, as reimbursement for the ransom paid may not always be guaranteed by your insurer.

Source: Gartner
How Do We Respond to an Attack?
Responding Early to Mitigate Damage

When faced with a ransomware attack, the first step is to report to law enforcement immediately and contain the malware.

Responding to ransomware

- **Initiate incident response and DR procedures**, as it may take IT time to isolate and remove the ransomware and restore data and normal operations. Then, assess the strengths and weaknesses of the incident response plan.
- **Contact law enforcement immediately**. Contact local FBI or a U.S. Secret Service (USSS) field office immediately to report a ransomware attack and request assistance.
- **Consult experienced legal counsel** to navigate the legal, financial and cybersecurity risks that must be carefully navigated.

Actions for IT and security

- **Isolate the infected computer immediately** and remove infected systems from the network to prevent the ransomware from spreading to other network or share drives.
- **Isolate or power off affected devices that have not been completely corrupted**.
- **Secure backup data or systems** by taking them offline, ensuring backups are free of malware.
- **Collect and secure partial portions of the ransomed data** that might exist, if available.
- **Change all online account passwords and network passwords** after removing the system from the network, if possible, and change all system passwords once the malware is removed from the system.

Source: Gartner and FBI
Considerations for Paying the Ransom

Organizations are encouraged not to pay the ransom, as they are not guaranteed access to their files and systems after making the payment. Investing in ransomware protection capabilities is also likely to be cheaper than paying the ransom.

To pay or not to pay?

The FBI does not support paying the ransom. However, it recognizes that businesses may be faced with the inability to function, requiring executives to consider all options to protect their shareholders, employees and customers. So, before paying ransom consider the following:

- ~30% of the time organizations were not able to recover their files because hackers did not provide the decryption keys needed to retrieve access to files after organizations made the payment.
- Some victims who have paid ransom have reported being targeted again by cybercriminals.
- Victims who paid ransom have been asked to pay additional ransom to get the decryption keys.
- Paying ransom could encourage further cyberattacks.

Gartner also does not support paying ransom. While the number of ransomware incidents resulting in payouts is unclear, approximately 80% of organizations that pay ransom demands end up being exposed to another attack. Moreover, investing in ransomware protection measures (e.g., recovery solutions) generally costs less than paying the ransom.
Complying with Cybersecurity Regulation

Given the severe consequences of a ransomware attack, paying ransom may be a violation under the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission (FTC) or the Office of Foreign Assets Control (OFAC).

Considerations for ransomware payments

**HIPAA:**
- Companies in the healthcare industry may be subject to cybersecurity obligations, which include provisions for ransomware, under HIPAA, as interpreted by the U.S. Department of Health and Human Services (HHS). This may include security measures to prevent ransomware.
- The HIPAA “Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.” This may include security measures to prevent ransomware.

**FTC:**
- Under Section 5 of the FTC, companies are required to implement reasonable measures to detect and prevent unauthorized access to its authority, which may include ransomware under this obligation.

**IRS:**
- Over the past few years, cyberhackers made demands in the form of cryptocurrency, such as bitcoin. In 2014, the IRS declared that bitcoin is considered property, not currency, and therefore can be taxed.
- The use of bitcoin may then leave a taxpayer with a taxable gain or loss, depending on the net outcome.

**OFAC:**
- Under OFAC, paying ransom to entities or governments under OFAC’s sanctions list are illegal under U.S. law. As of October 2020, organizations may be subject to financial penalties if they do make ransom payments to these entities.
- Many states have enacted laws that require businesses to implement security measures to protect personal information used by businesses from cyberattacks.

Source: Gartner
Endnotes

1 Colonial Pipeline blames ransomware for network shutdown, NBC News.


3 ISS World Hit with Malware Attack that Shuts Down Global Computer Network, Threatpost.

4 How hackers extorted $1.14m from University of California, San Francisco, BBC News.

5 The Ransomware That Hobbled Atlanta Will Strike Again, Wired.

6 The Security Rule, HHS.gov.
For Further Reading


More targeted, sophisticated and costly: Why ransomware might be your biggest threat, CSO Online.


What businesses need to know about cybersecurity challenges, Washington Post.

What we know about the pipeline ransomware attack, CNN.