ISACA®

Quick Reference

Ransomware Incident Management

Ransomware is an especially egregious form of malware that restricts access to a system and can, at best, temporarily impact revenue generation or, at worst, cause a massive financial loss event that triggers bankruptcy or liquidation. Complicating this is the public sector's growing reliance on private sector entities to defend against ransomware, which has significantly increased the criticality of supply chain risk management.

Variables Influencing Ability to Prepare and Recover from Ransomware

There are a number of variables that influence one's ability to prepare for and recover from a ransomware attack.

ENTERPRISE SIZE

INDUSTRY SECTOR

REGULATORY LANDSCAPE

Ransomware Preparedness Checklist

Preparedness is critical in a global digital ecosystem that demands enterprises of all sizes be better at the basics. Ideally, an enterprise would have sufficient in-house staff, but that is often not the case. This quick reference guide covers key activities for improving ransomware readiness and serves as a useful resource for identifying external needs, such as consultants, service providers, etc., based on criticality, funding, staffing and risk tolerance.

PLANNING AND PREPARATION

○ **Establish roles and responsibilities:**

a. A ransomware incident response (IR) team typically includes an IR manager, forensic analysts, ransomware negotiator, risk manager, threat intelligence manager, vulnerability manager and security operations manager.

b. Organizational members should include an executive lead, response support (e.g., HR, crisis communications, PR, legal counsel) and business unit and technical leads for IT, OT, application, middleware, networking, endpoint and architecture.

○ **Document escalation procedures,** including internal and external reporting requirements. Enterprises are wise to establish relationships with—and document contact information for—applicable law enforcement, regulatory authorities and information-sharing entities (e.g., Computer Emergency Response Teams (CERTs), Information Sharing and Analysis Centers, InfraGuard, etc.).

○ **Ensure backup strategies are operationalized**, including an offline backup strategy that supports disaster recovery needs (e.g., hot/cold).

○ **Establish policies, procedures and corporate artifacts** to aid ransomware IR in developing corporate policy on ransomware payment; regulatory requirements for ransomware incident and data leakage reporting; IT architecture (e.g., network, infrastructure, application and security architecture diagrams); and documentation on connectivity with third parties and relevant contracts (e.g., breach notification).

DID YOU KNOW
You are able to use this guide and check off the items as they are completed, simply click the circle to the left of the task.

IDENTIFICATION AND DETECTION

Six steps to identify and detect a ransomware incident:

○ **1. Define indicators of compromise (IOCs):**

- Boot time of services and applications
- Unknown/unexpected services and applications
- Presence of unauthorized remote access/VPN software
- System performance (CPU/RAM utilization)
- Host security instrumentation performance is degraded/disabled
- Unknown/unexpected FQDN/IP address connections
- Protocol mismatches
- File hashes
- Inbound and outward traffic

○ **2. Define tactics, techniques and procedures (TTPs). The MITRE ATT&CK® framework is a useful aid.**

○ **3. Identify the indicators of exposure (IoEs), such as exploited vulnerabilities.**

○ **4. Identify and define relevant risk factors, including:**

- Extortion level (i.e., Single/Double/Triple/Quadruple extortion)
- Assets (e.g., systems, applications, subsystems, etc.)
- Toxic data (e.g., protected health information, credit card numbers) that were exposed
- Sensitive data (i.e., intellectual property) that were exposed
- Service outage (i.e., impact to operations)
- Number of staff impacted
- Number of customers impacted
- Public impact (e.g., utility services, critical infrastructure)
- Business impact (e.g., productivity, brand/reputation, fines/penalties)
- Third party risks
- Data encryption

○ **5. Request network captures:**

- NetFlow (network metadata)
- Full packet capture (network record)
- Purpose of capture
- Traffic volume

IDENTIFICATION AND DETECTION

○ 6. **Search for evidence of IOCs. Artifacts may be categorized as host or network level. Examples of each include:**

○ HOST LEVEL

- Logs
- File hashes
- Registry entries (Windows only)
- Presence of unauthorized software
- Recently created compressed files
- Memory dump
- List of active/running network services
- Scheduled processes
- Scheduled job list
- Prefetch lists
- Firewall rules and logs (host level as applicable)
- IDP/IPS rules and logs (host level as applicable)
- Antivirus/antimalware rules and logs (host level as applicable)
- List of logged-on users (historic and current)
- Available network shares
- Mounted network shares
- User accounts
- Session data

○ NETWORK LEVEL

- File extracts from full packet captures
- SSL/TLS certificates
- Active network connections (firewall/screening router)
- ARP cache
- DNS cache
- Running processes (network infrastructure)
- Firewall rules and logs
- IDS/IPS rules and logs
- EDR/XDR rules and logs
- DHCP logs
- Directory services logs
- Network time protocol
- Proxy server logs
- User agent strings
- Nonstandard application callouts/phone homes/updates
- Data loss prevention logs

ANALYSIS

Steps to analyze a ransomware incident

○ 1. **Business Analysis:**

- Customer impact
- Toxic data exposure
- Sensitive data exposure
- Public safety impact
- Business impact (brand/reputation, impaired market growth, organizational changes)
- Compliance impact (regulatory censures, fines and penalties)
- Operational impact (productivity loss, response costs)

○ 2. **Technical Analysis:**

- Systems impacted
- IOCs discovered
- TTPs identified
- IOEs identified
- System(s) isolation
- Forensic image acquisition
- Conduct forensic analysis of ransomware to determine ransomware type and capabilities
- Execute/detonate in a controlled/sandboxed environment
- Develop containment, eradication and recovery strategies
- Identify and verify eradication techniques (e.g., patch/mitigation) are successful
- Document FQDN/IP addresses
- Identify affected services to be disabled, when approved
- Document modifications and updates to network infrastructure, when approved (including firewall, router and IDS/IPS rules and configurations)
- Document modifications and updates to endpoints, when approved (including antivirus/antimalware and EDR/XDR rules and configurations)
- Update SIEM rules and alerts as appropriate to increase visibility

CONTAINMENT

Steps to contain a ransomware incident:

○ **Number of systems impacted**

○ **Amount of data exposed (toxic and sensitive)**

○ **Total services (business and IT) impacted**

○ **Attack vector identification**

○ **Vulnerability identification**

○ **Identify instrumentation available to determine full scope of incident:**

- Antivirus/antimalware System
- Data loss prevention system
- Directory services
- Domain name services
- Firewall
- Routers
- Switches
- IDS/IPS
- Network monitoring system
- Network scanner
- SIEM
- Vulnerability scanner

ERADICATION

Steps to eradicate a ransomware incident:

○ 1. **Coordinate efforts with the appropriate team members through:**

- Direct phone calls/conference calls
- Out-of-band communications
- In-person meetings

○ 2. **Prevent further propagation through the network (approval should be granted for all activities):**

- Block FQDN/IP addresses
  - > Disable identified services
- Remove affected system(s) from network
  - > Update firewall rules and configurations
  - > Update router rules and configurations
  - > Update IDS/IPS rules and configurations
- Revoke and reset credentials for affected accounts, including user and service
- Disable unnecessary services and protocols

○ 3. **Eradicate ends by closing off the initial attack vector and mitigating the vulnerability:**

- Remove/reduce attack vector
- Increase logging and monitoring
- Remove system(s) from production
- Mitigate the vulnerability (patch/virtual patch)
- Migrate data from impacted system(s) to staging area
- Scan/analyze data, searching for trojan files
- Update golden image to prevent future introduction of same vulnerability
- Disconnect from third party in the supply chain if the third party was the source of the breach

RECOVERY

Steps to recover from a ransomware incident:

○ 1. **Systems: Reimage the system using the updated golden image.**

○ 2. **Data: Document business impact of any data not fully recovered/restored. Determine if recovery point objectives were met or missed. This refers to negotiated recovery (decryption key purchased from attacker) or recovery from data backups.**

○ 3. **Incident remediation: Proactively prevent the incident from reoccurring:**

- Update instrumentation baseline configurations and golden image
- Verify and validate business recovery status
- Monitor for network IOCs
- Scan for host IOCs
- Mitigate exploited vulnerabilities (patch/virtual patching)
- Increase logging and monitoring
- Coordinate and update stakeholders and business partners (as appropriate)

POSTMORTEM, LESSONS LEARNED AND AFTER ACTION

The following are steps to review, reflect and implement improvements after a ransomware incident.

Use the Kipling Method (5W1H)[1] or an alternative to identify the root cause required for the postmortem, lessons learned and continuous improvement reviews. Minimally, the following must be addressed at a high level:

Who was involved?

Where did it happen?

What happened?

Why did it happen?

When did it happen?

How did it happen?

[1] Datamyte.com, "The Comprehensive Guide to 5W1H Method: Learn What, Where, When, Why, And How to Use It," 29 August 2022, https://datamyte.com/5w1h-method-comprehensive-guide/#:~:text=The%205W1H%20is%20a%20questioning,letter%20H%20stands%20for%20How.

○ INCIDENT POSTMORTEM AND REVIEW

- Which stakeholders were impacted?
- Who were the threat actors involved?
- Where did things go wrong in our response approach (close gaps/ corrective actions)?
- Where did things go right in our response approach (reinforce the positives)?
- When did we detect this?
- Why didn't we detect it sooner?
- Why did our controls fail to prevent it?
- What could have been in place to limit the impact?
- What prevented an even faster response time?
- What accelerated response efforts?
- What systems were compromised?
- What data was exposed (toxic/sensitive)?
- What needs to be adjusted within business operations to prevent future incidents?
- What was impacted?
- What does it mean to the business?
- What does it mean for IT operations?
- How did the incident occur?
- How can this be avoided in the future?

○ LESSONS LEARNED

- Facilitate meeting with affected senior management, business unit leadership, IT, audit and security to determine the root cause of the incident.
- Update relevant policies, processes, procedures, configurations and audit needs accordingly.

○ AFTER ACTION

- Implement and operationalize the relevant policies, processes, procedures, configurations and audit updates.
- Audit and assess effectiveness and efficacy of implemented and operationalized policies, processes, procedures and configurations.
- Review ransomware IR workflows to identify any potential gaps that caused issues or delayed response and recovery efforts.
- Review controls to identify any gaps that caused issues or delayed response and recovery efforts.
- Draft mitigation efforts and corresponding project plans with supporting business cases to close any gaps identified that exceed the organization's risk appetite

Mitigation Strategies

Solid cybersecurity practices are the most obvious mitigation tactic available to enterprises to combat potential ransomware attacks, but security alone cannot guarantee that an organization will not be attacked.

To help with mitigation, organizations should consider obtaining cyberinsurance that covers ransomware, as most practitioners agree it is important (**figure 1**). In fact, over half of the respondents in a recent ISACA survey[2] indicated their organization had cyberinsurance (**figure 2**). However, insurance does not mitigate poor or nonexistent security practices, and carriers increasingly require minimum readiness levels to qualify.

FIGURE 1: Importance of Cyberinsurance

How important is cyberinsurance to an organization?

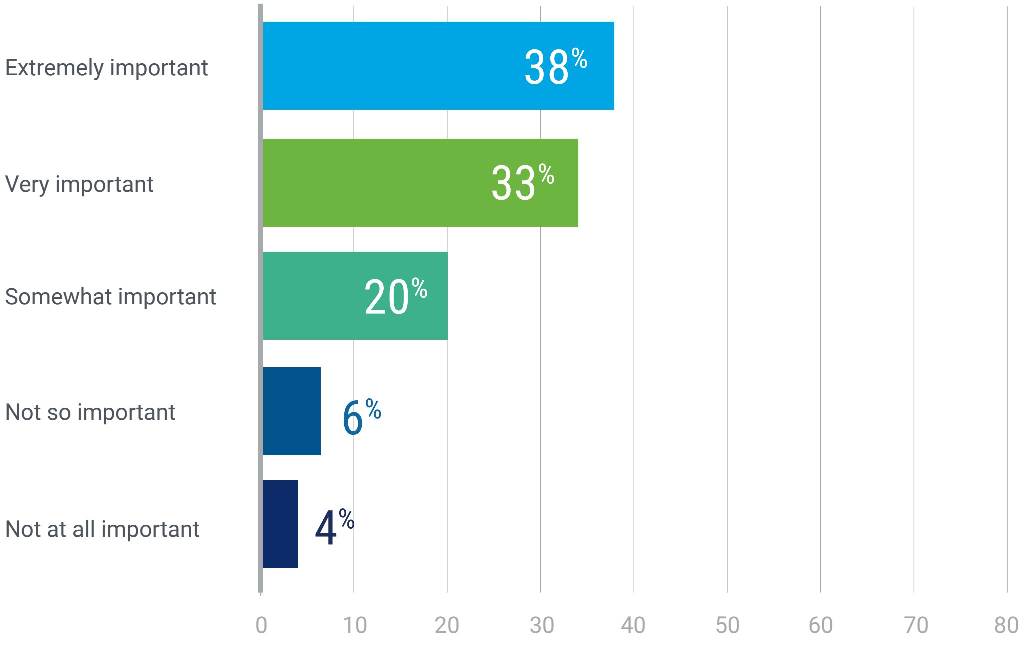
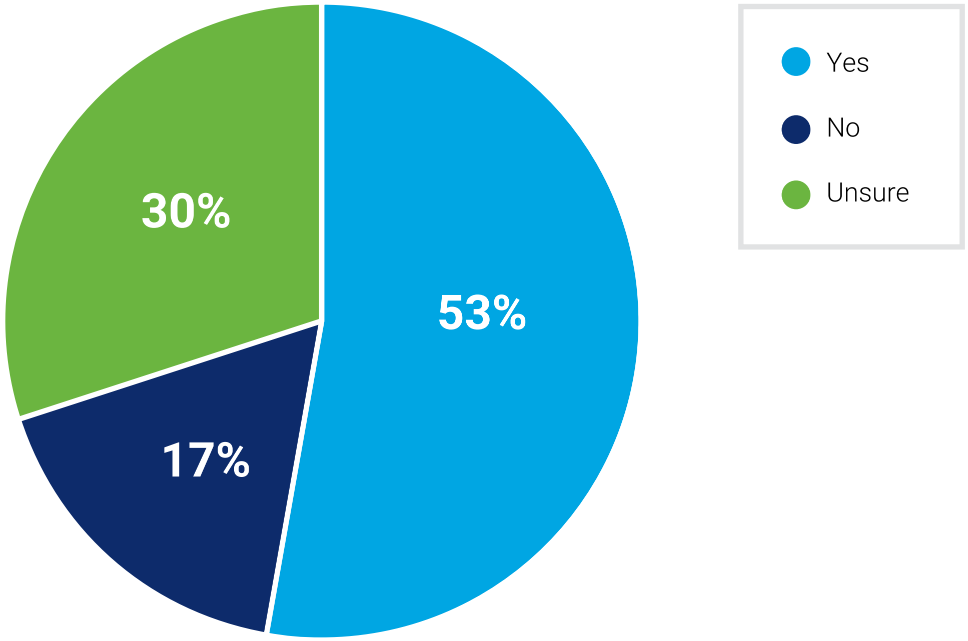


FIGURE 2: Percentage With Cyberinsurance

Does your organization have a cyberinsurance policy?



[2] In Q1 2023, ISACA surveyed constituents that work in IT risk or have detailed knowledge of the IT risk function in their enterprise. The respondent base included 1,859 completed surveys.

According to the survey results, reasons vary for why organizations purchase a cyberinsurance policy (**figure 3**). In addition, the type of cyberinsurance coverage differs by enterprise (**figure 4**).

FIGURE 3: Why Cyberinsurance was Purchased

Why did your organization purchase a cyberinsurance policy? Select all that apply.

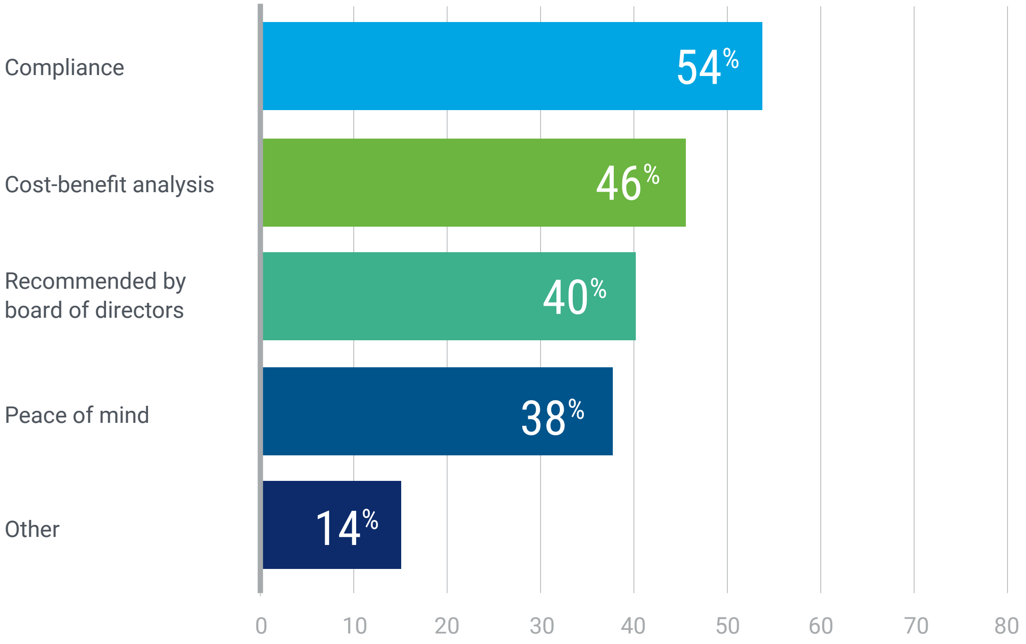
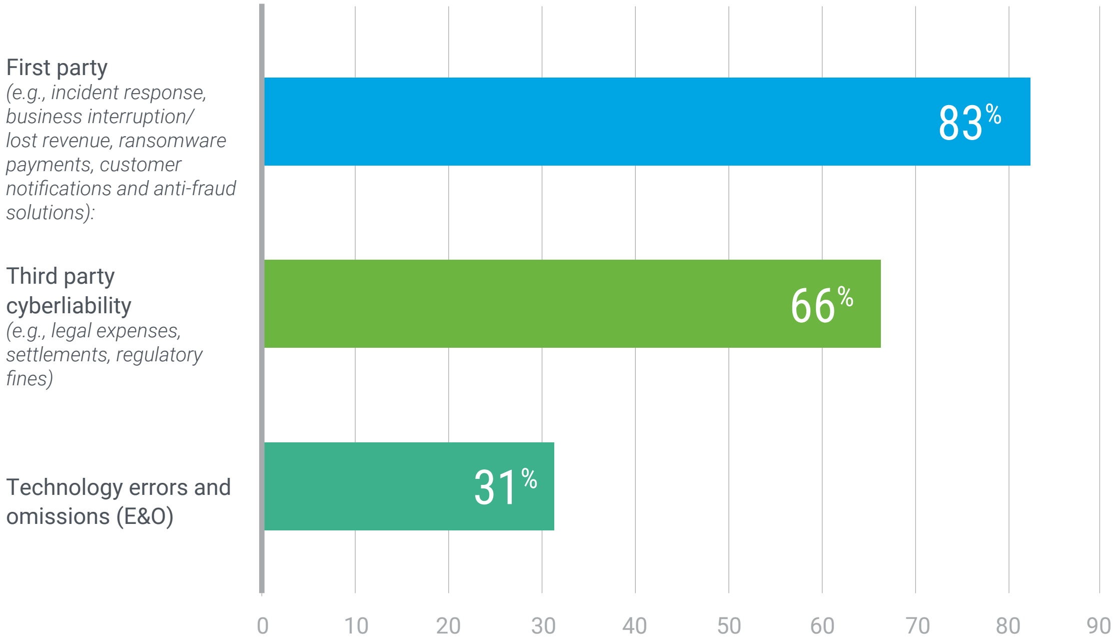


FIGURE 4: Type of Cyberinsurance Coverage

What type of cyberinsurance coverage does your organization have? Select all that apply.



TO LEARN MORE, VISIT:
www.isaca.org/resources/cybersecurity.