THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

Iona

One of the
RSM team

Incident Response Guide

Table of contents

Incident response hotline
+1 855 810 0615
DFIR.Team@rsmus.com

If you believe your organization has experienced a breach and needs immediate assistance, please contact RSM's incident response team.

Cyber incident checklists

The following outlines high-level questions to determine whether you have suffered an information security incident. If one or more of these apply to your business, unauthorized access may have occurred within your network. If your answers lead to concerns about any of these common incidents, consider the following containment processes and next steps to address your issues and protect your network and systems.

Malware and ransomware attacks

Malicious software can enter your network in a number of ways, such as by email attachments or infected websites. The malware can spread quickly through your system, exploiting vulnerabilities, causing disruptions and allowing access to sensitive data. Malware is often used as a precursor to launching a ransomware attack. After attackers have scoped out your environment, they can then launch a ransomware attack that is exceptionally well targeted to inflict the most harm to pressure you into paying the ransom.

Example:

An employee may receive an email that has an attachment that contains malicious code. When the file is accessed by the user, malware is downloaded and executed on the system, which allows the attacker to gain access to the environment. Another frequent attack mechanism is for the attacker to locate a vulnerable system that is exposed on the internet and then compromise that system to get into the environment.

Assessing your situation:

- Have you been notified of sending suspicious emails without your knowledge?
- Have you been unable to visit certain websites?
- Are you experiencing poor system performance?
- Is your computer behaving erratically after visiting an unknown website or opening an email attachment?
- Are you using the same logins and passwords for multiple platforms and accounts?
- Are you receiving high or severe level notifications from your anti-virus solution concerning malware infections?
- Are your users reporting that they are unable to access files or applications within the network?
- Do the potentially infected systems or users have access to manage sensitive company information, such as accounting, financial or human resources information?
- What steps were taken prior to and immediately after the suspicious behavior was observed?

Containment processes:

- Disconnect the infected computer from the company network (both wired and wireless).
- Put controls in place to prevent users from accessing known malicious emails, websites or links.
- Cut off user access to shared resources and network applications.
- Educate employees about potential activities that can exploit network vulnerabilities with malware.
- Prevent any additional incoming or outgoing emails from the source of the original malicious message and related sites.

Potential evidence sources:

- Forensic image of infected systems, including memory (RAM) from the infected system
- Application logs
- Firewall and intrusion detection systems (IDS) logs
- Network traffic logs
- Physical storage
- System event logs
- Cloud and on-premises email logs

Potential next steps:

- Assess the nature, scale and scope of the incident; determine if it is possible that sensitive information, including personally identifiable information (PII), payment card industry (PCI) data, protected health information (PHI), financial account information or protected privacy data, was at risk of exposure.
- Determine if third-party assistance is needed in order to respond to the incident:
  - Have you contacted your cyber insurance company to discuss whether coverages are in place to offset fees related to the response?
  - Is there a need to engage a third-party incident response partner?
  - Is there a need to engage cyber breach or privacy counsel?
  - Is there a need to engage a public relations or crisis management firm?

Business email compromise

Business email accounts can be compromised in several ways. However, the most common is when attackers direct users to fraudulent websites where users are enticed to enter their credentials. A business email compromise attack is frequently associated with some type of financial fraud. These events can often lead to significant financial loss, as well as the potential theft of confidential or protected information.

Example:

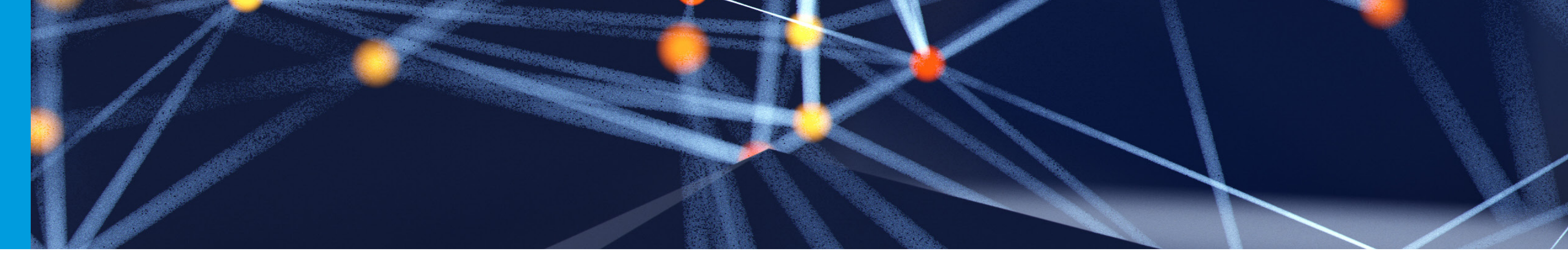
An employee may receive a phishing email to access an online resource (e.g., a document in cloud storage, a voicemail message). The email is designed to appear legitimate; however, when the link is clicked, it directs the user to a fraudulent website where they are instructed to enter their credentials. The attacker then takes over control of the user's business email account and attempts to have payments sent to a bank account the attacker controls.

Assessing your situation:

- Have you been notified of sending suspicious emails without your knowledge?
- Do you have vendors, suppliers or other people asking where their payment is, but you have already sent the payment?
- Have your vendors, suppliers or others recently asked you to update their payment or billing information without secondary confirmation, such as a phone call?
- Are you not receiving email messages that you know should be there?
- Did you follow a link to a website that asked you to enter your username and password, but you were not able to successfullylog in?
- Are you using the same logins and passwords for multiple platforms and accounts?
- Do you manage sensitive company information, such as accounting, financial or human resources information?
- Do you utilize web-based banking or electronic payments?
- What steps were taken prior to and immediately after the suspicious behavior was observed?

Containment processes:

- Reset the affected user's password and force a session disconnect.
- Remove all copies of the malicious email from the environment to prevent other users from accessing it.
- Check for unauthorized rules, and then document and remove any that are located.
- Put controls in place to prevent users from accessing known malicious emails, websites or links.
- Prevent any additional incoming or outgoing emails from the source of the original malicious message and related sites.
- Educate employees about potential activities that can exploit network vulnerabilities with malware.



Potential evidence sources:

- Cloud and on-premises email logs
- Application logs
- Firewall and IDS logs
- Network traffic logs
- System event logs
- Forensic image of infected systems and system memory, as appropriate

Potential next steps:

- Assess the nature, scale and scope of the incident; determine if sensitive information, including PII, PCI, PHI, financial account information and protected privacy data information, was at risk of exposure.
- Determine whether third-party assistance is needed in order to respond to the incident:
  - Have you contacted your cyber insurance company to discuss if coverages are in place to offset fees related to the response?
  - Is there a need to engage a third-party incident response partner?
  - Is there a need to engage cyber breach or privacy counsel?
  - Is there a need to engage a public relations or crisis management firm?
  - Do you need to start working with any vendors to assist with response efforts?

Social engineering attacks

Social engineering is a targeted threat to businesses, with outsiders or internal personnel manipulating employees to gain access to sensitive or confidential data. An incident can occur in several different ways, such as via phone or with person-to-person contact, for various reasons, such as capturing bank account or health care information and various passwords, or installing potentially malicious software.

Example:

An employee receives a phone call from an unknown person, posing as a member of your IT staff. The caller requests account information or credentials to access systems in order to make changes or improvements. In reality, that caller is a criminal, seeking access to your network and files for nefarious purposes.

Assessing your situation:

- Does a nonemployee seem to have intimate knowledge of company matters?
- Has anyone outside your company asked for personal or proprietary information?
- Has an employee asked about sensitive information that is not necessary for their job function?
- Has anyone, internally or externally, asked you questions about sensitive or proprietary data that made you suspect wrongdoing? Why do you think you may be the victim of a social engineering attack?
- What information did the attacker seek, and what was provided?
- To what systems and information was the attacker given access?
- What information can you access? Can you access sensitive financial, accounting or human resources data?

Containment processes:

- Immediately disable any accounts accessed by the criminal. If the criminal accessed a cloud-based system, such as Microsoft Office 365, do not disable the account as this can affect the availability of information to perform an investigation. Instead, restrict access to the account by changing the password and force a session disconnect.
- Segregate the computer the attacker accessed.
- Seize any RAM, leaving the computer running but disconnected from company networks.
- Take a forensic image of the affected computer(s).
- Capture traffic from the machine if the intrusive connection remains active.
- Notify all employees about the attack and potential social engineering methods to limit future damage.
- Further emphasize the importance of not sharing logins, passwords and any sensitive information to potentially unauthorized people via phone and email conversations and even face-to-face communication.

Potential evidence sources:

- Forensic image of infected systems, including RAM
- Application logs
- Firewall and IDS logs
- Network traffic logs
- Physical storage
- System event logs
- Cloud and on-premises email logs

Potential next steps:

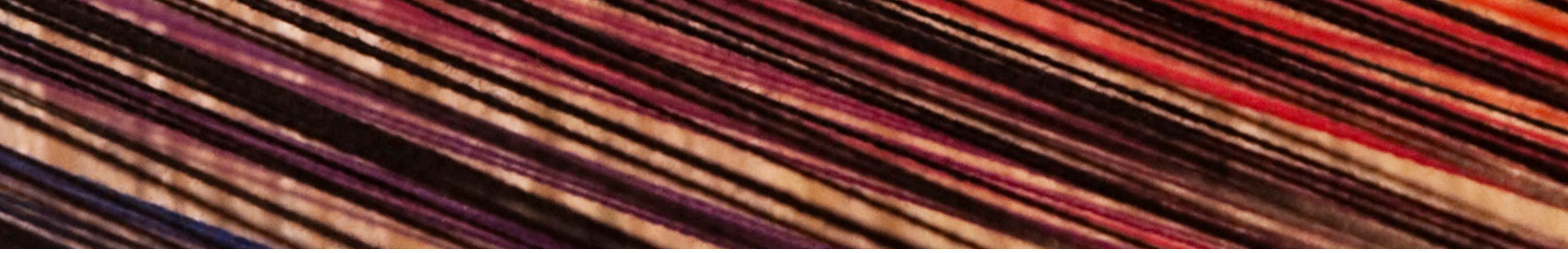
- Assess the nature, scale and scope of the incident; determine if sensitive information, including PII, PCI, PHI, financial account information and protected privacy data, was at risk of exposure.
- Determine whether third-party assistance is needed in order to respond to the incident:
  - Have you contacted your cyber insurance company to discuss if coverages are in place to offset fees related to the response?
  - Is there a need to engage a third-party incident response partner?
  - Is there a need to engage cyber breach or privacy counsel?
  - Is there a need to engage a public relations or crisis management firm?
  - Do you need to start working with any vendors in order to assist with response efforts?

Lost or stolen computers, devices or media

With increased technology capabilities and utilization, sensitive information is typically stored on a host of devices, and occasionally those devices are lost or stolen. Unfortunately, employees sometimes lose computers or devices that contain company information. Computers or devices are also frequently stolen from residences, vehicles or even the office. Information is now more portable than ever, but it can easily fall into the wrong hands, and your data can be exposed.

Example:

An employee mistakenly leaves a mobile device at an airport before boarding a plane, or a laptop is stolen from a vehicle.



Assessing your situation:

- What type of information resided on the lost or stolen computer or device?
- Do you utilize encryption for computers and devices that access sensitive data?
- Are devices equipped with remote tracking or wiping tools?
- Do you utilize rolling backups for employee computers and devices?
- Did the device potentially contain sensitive information, such as financial or accounting data, PII or PHI?
- Was only a single device lost or stolen, or were multiple devices or additional documents taken or misplaced?

Containment processes:

- Immediately change account passwords after notification of a lost or stolen device.
- If the computer or device is stolen, contact the police to file a report.
- Assess whether full or partial backups of data stored on the device exist elsewhere.
- Continually remind employees of best practices to secure devices and documents and discourage loss or theft.
- Make use of remote wiping or tracking capabilities, if available.

Potential evidence sources:

- Backups
- Server emails and archives
- User network shares

Potential next steps:

- Assess the nature, scale and scope of the incident; determine if sensitive information, including PII, PCI, PHI, financial account information and protected privacy data, was at risk of exposure.
- Determine whether third-party assistance is needed in order to respond to the incident:
    - Have you contacted your cyber insurance company to discuss if coverages are in place to offset fees related to the response?
    - Is there a need to engage a third-party incident response partner?
    - Is there a need to engage cyber breach or privacy counsel?
    - Is there a need to engage a public relations or crisis management firm?
    - Do you need to start working with any vendors to assist with response efforts?

Incident response methodology

The following outlines key steps to take to respond to information security incidents. This information is summarized from the National Institute of Standards and Technology's *Computer Security Incident Handling Guide*.

Preparation—Having a plan in place can be the differentiator between failure and success. It is imperative today that organizations develop and maintain an incident response plan (IRP). That way, your organization has a plan and playbook in place should the need arise to respond to an incident. This plan should be tested regularly to ensure that key stakeholders know their roles and the organization can vet the plan in order to implement improvements.

Identification—Knowing the threat and its origin helps your organization determine the proper response to evaluate the security of systems and data. Any individual within your organization can identify a threat. All staff and users should be trained on the growing number of threats, best practices to avoid them and how to report potential incidents.

Validation and assessment—Incidents typically begin when an employee reports irregular behavior from the network, on a device, or loss of access to data or systems. If issues are not originally noticed by IT staff, they are typically reported to them by end users. IT personnel must be prepared to validate and assess potential incidents by using proper methods and tools.

Communication—An incident can cause unwanted communication to outside individuals, including the perpetrator. For example, communication using a compromised email account could notify intruders that they have been detected, potentially leading to destroyed evidence or further damage. This can be avoided by using another form of communication, such as voicemail, cell phones or text messages.

Containment—After identifying a threat or intruder, containing the situation is of critical importance. Take steps to contain or segregate potentially infected systems from infecting or damaging other data or systems in the environment. This could mean restricting access to specific systems or entire physical locations. Depending on the severity and type of incident you suffer, you may need to shut down devices, route network traffic to a separate virtual local area network (VLAN) or leave them operational to allow additional investigation.

Preservation and evidence collection—Effectively collecting evidence helps preserve potentially important information that will be needed to assess the origin and extent of the incident. In some cases, you may also need to collect evidence for legal purposes. Utilize chain of custody forms to document the transfer of evidence between parties.

Recovery of systems—To recover from an incident, your organization must take actions which could include patching vulnerable systems, locating and eradicating potentially malicious data or processes, restoring to a previous known good backup, rebuilding a system from scratch, or a combination of all the above. It is also beneficial if you have undertaken some proactive steps prior to suffering a cyber incident. The proactive actions can include preparing and securing backups for critical systems and data in advance, and having updated and tested disaster recovery and IRPs.

Notification—If a potential or confirmed incident occurs within your organization, designated individuals must be informed as quickly as possible. Your IRP should outline a notification group including information security personnel, system owners, public affairs, human resources, legal and any other necessary individuals. The notification should include key information, such as who identified the incident, the date and time the incident was discovered, the symptoms, which systems or data were affected, who was notified and when, and the steps taken to address the situation.

Common security assessment areas

The following list details processes that organizations may fail to fully address when developing an overall data security platform. Evaluating each of these areas can help your organization implement a comprehensive strategy to protect your sensitive information.

Policy

Information security—Your company should develop and implement an information security platform that aligns with the organization's vision and goals. Audit, compliance and operational managers should have input to encourage network and data confidentiality, integrity and availability.

IRP—Your IRP should outline all processes and contacts for a potential cybersecurity incident. Regularly test your IRP after implementation; be sure to include key groups such as legal and human resources in your testing.

Business impact analysis—Perform an analysis to detail key information and systems and the organization's risk tolerance in a potential incident. Several areas should be considered in the assessment, including human resources, finance and any proprietary systems or data.

Policy and procedure review—All IT governance policies and procedures should be periodically reviewed and updated to account for emerging risks and changes within the company. Policies and procedures should include version information along with the author, the date implemented and specific objectives.

Security awareness training—Employees should receive regular education and training on identifying and reporting potential incidents that could affect information security. Training should include education on common cyber incident types, such as phishing and social engineering attacks.

Building access policy and procedures—Develop clear policies and procedures that govern building access for employees, maintaining records for vendors and visitors who access your facility, as well as the removal of any physical property.

Internet use policy—Implement a policy that details how employee internet use is monitored and what information is collected. Also describe acceptable use guidelines and how network resources can be utilized for personal use.

Network

Segregating networks by department and data classification—Your network topology could benefit from network segregation with subnetworks or VLANs. Separating departments, such as human resources, finance and legal, can improve your security posture and reduce the risk of compromised data.

File-level auditing—Your organization should consider applying a file-level auditing platform to increase tracking capabilities. Audit logs should include several details, such as the date and time data was accessed, who accessed the data and what actions were taken.

Guest wireless network—Your guest wireless network should include Wi-Fi Protected Access 2 security with password protection. That password should periodically change to increase network protection. The guest network should be separated from the employee network, and should include a legal statement detailing proper use that must be accepted prior to use.

Internal vulnerability scans—Following any change in network structure or design, your organization should perform internal scans of the network to ensure the platform is secure.

Security information and event management (SIEM)—Your organization should implement a SIEM strategy to gather alerts and information about your virtual private network (VPN), network and applications. Your IT team should develop and use a notification system to communicate alerts and regularly review logs to evaluate any errors and concerns.

Cloud-based email—Detailed logging should be enabled for any cloud-based email, and the logs should be retained for as long as the platform allows. In addition, multifactor authentication (MFA) should be enabled to minimize the threat of an attackers seizing control of a user's email account.

Security

Full disk encryption—All laptop and desktop computers should include full disk encryption to protect local and network files and company systems.

Secure email transmission—If you distribute critical information via email, you should consider implementing an application to help ensure secure transmission. Several platforms can reduce the risk of sensitive data disclosure and protect information from being compromised.

Password complexity—All network and application accounts should have an appropriate level of complexity. Passwords should also be changed on a regular basis, and the same password should not be used across multiple platforms or accounts.

MFA—All accounts that are accessible from outside your organizations network should have MFA in place to protect against exposed credentials, password cramming and brute-force password guessing attacks.

Standard desktop and laptop deployment—Your IT function should implement a standard for desktop and laptop distribution. Implementing a standard process helps to create uniform processes for help desk, application and program support.

Removal of physical equipment policy and procedures—Develop a system of controls to allow removal of equipment or property from facilities only with proper documentation.

Mobile device wiping—With the proliferation of mobile device usage on your network, you should implement secure password and remote wiping capabilities to protect your data and systems.

Potential evidence sources

The following list defines several evidence sources and how they can help your organization identify and investigate a potential incident. Proper electronic evidence collection should be a focal point of the IRP.

Application logs—Application logs track local and third-party network applications, detailing when programs were executed, any errors, and information on access and modifications to accounts and data. These logs may not directly capture evidence of malicious activity, but can offer a glimpse into network issues or changes as a result of malicious code. IT must maintain an inventory of installed applications to monitor potential evidence sources and fully understand the logging abilities of important applications.

Backups—If you have viable backups for systems and data, they can provide a point-in-time snapshot of specific systems that can be used for analysis. They can also help you recover from a cyber incident.

Email logs (cloud-based and on-premises servers)—This information can document communication and authentication records between hosts, servers and email clients. These logs include several key sources of information, including host and user activity, files, IP addresses, URLs accessed, browser and system activity, and any errors recorded. You can utilize these logs to monitor incidents, including how an infection originated, and illicit access to accounts and File Transfer Protocol, web and webmail servers.

Firewall and IDS logs—Firewall and IDS logs are critical tools that collect information on internet traffic, both to and from your network. These logs include information on the volume of data your network experiences, as well as connection attempts and data's origin and destination. The records can identify IP addresses of computers that communicate via network connections and the port number used by the service or application. The logs identify and can help target any abnormal or malicious events, unauthorized network access or failed attempts at access.

Computer and server forensic image—Often, computers and servers hold critical information that will need to be analyzed as part of an incident response effort, such as system event logs, file access history and other artifacts of value. The data from these systems is typically captured in forensic images, which are written to a special file to ensure that the contents are not altered after the image has been created. The data from these systems can then be examined in a secure manner without the concern of altering the data. In addition, the captured data can typically be used as evidence in court when preserved in this manner.

Network traffic logs—Network traffic logs track IP addresses, data loss prevention and VPN activity. These logs can produce evidence regarding the origination of an infection and any removal of sensitive data from your environment. Network logs can be used on a constant basis, or designed only to capture a certain type of activity or activity during a defined time period. Network logs can be useful even following an incident, logging traffic and collecting evidence of malicious activity after the fact.

RAM—RAM temporarily stores code, data and settings for your system. This memory can often include critical evidence of the execution and activity of malicious code. Appropriate tools must be used to collect evidence from volatile memory while the system is in use. This contradicts typical first-responder actions of disconnecting infected computers to limit further exposure. The goal is to preserve evidence in volatile memory while also isolating any malicious code.

System event logs—Event logs track hardware, operating system, and internal and third-party application activity. These logs record key information about system and service usage, changes to settings and access privileges, as well as access to the network and accounts. Typically, event logs are utilized for auditing purposes, and they must be contained quickly before potential evidence is deleted.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

+1 800 274 3978
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.