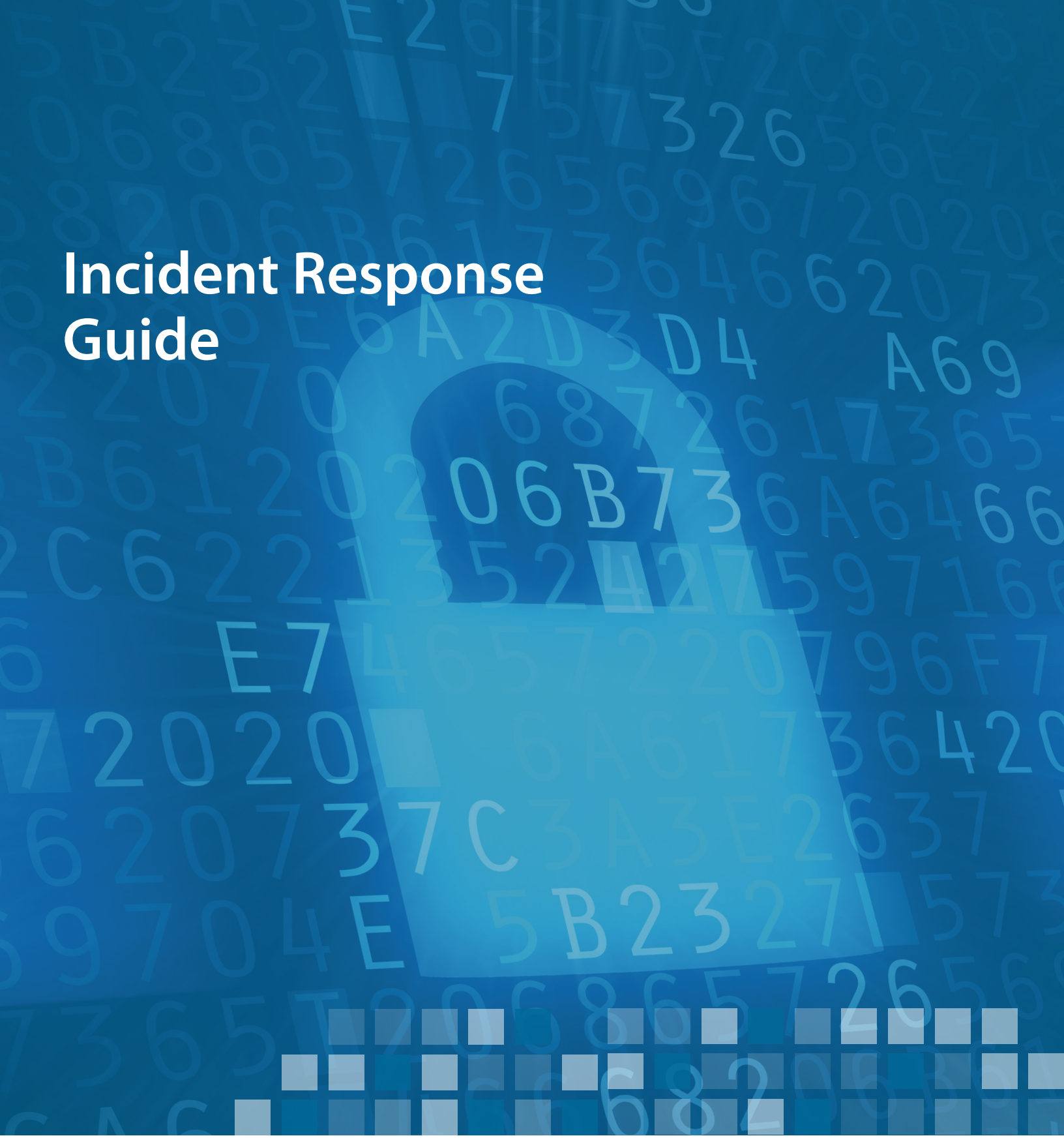
Incident Response Guide



McGladrey

Assurance ▪ Tax ▪ Consulting

Table of Contents

Incident Response Hotline
855.810.0615

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

Data privacy incident checklists

The following outlines high-level questions to ask to determine if 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, read the corresponding section in this guide to learn how to address your issues and protect your network and systems.

Malware intrusion

Malicious software can enter your network in a number of ways, for example, via email attachments or infected websites. The malware can spread quickly through your system, exploiting vulnerabilities, causing disruptions and allowing access to sensitive data.

- 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?

Internal or external unauthorized network access

Unauthorized access can wreak havoc on your systems and leave your sensitive information at risk. The potential damage can be widespread, and every part of your business is potentially vulnerable.

- Are any of your computers behaving unexpectedly?
- Do you suspect that your system has been infected with malware?
- Has any noteworthy employee behavior taken place outside of the norm such as unusual hours or conduct?
- Have any files been moved, modified, accessed or deleted?
- Do you have irregularities in server logs, such as unusual activity or an increase in failed login attempts?

Social engineering attacks

Social engineering is a growing, more directly targeted threat to businesses, with outsiders or internal personnel manipulating employees to gain sensitive data. An incident can occur in several different ways such as via phone or with person-to-person contact and can target any type of data from passwords to health and banking information.

- Does a non-employee 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 his or her job function?
- Has anyone, internally or externally, asked you questions about sensitive or proprietary data that made you suspect wrongdoing?

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, with the portability of information, it can easily fall into the wrong hands, and your data can be exposed.

- Do you allow employees to view and store network data on personal devices?
- Do you utilize encryption for computers and devices that access sensitive data?
- Are files and systems regularly backed up?
- Are devices equipped with remote tracking or wiping tools?

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 Incident Guidelines manual.

Identification – Knowing the threat and its origin helps your organization determine the proper response and 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 or a device, or loss of access to files or networks. If issues are not originally noticed by information technology (IT) staff, they are typically reported to them. 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 keep evidence safe from tampering, whether that means 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 them to a local VLAN or leave them operational to allow additional investigation.

Preservation and evidence collection – Effectively collecting and preserving evidence helps assess the extent of the damage. In many cases, you may need to collect evidence for legal purposes. You must clearly detail how evidence is gathered and account for each piece during the entire process. 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 reactive and proactive actions. Reactive actions include processes such as patching vulnerable systems and implementing any necessary platform updates. Proactive actions include preparing critical backups for systems and data in advance as well as installation instructions and settings for operating systems and applications. Users must know how backup systems operate to ensure necessary backups occur to their systems and to avoid losing key data.

Notification – If a potential or confirmed incident occurs within your organization, designated individuals must be informed as quickly as possible. Typically, your company guidelines should outline a group including information security personnel, system owners, public affairs, human resources, legal and any other necessary individuals. Proper documentation supports the notification framework, including who identified the incident, the date and time the incident was discovered, the symptoms, who was notified and when, and the steps taken to address the situation.

If personally identifiable information (PII) is identified and compromised in the incident, it must be documented. Depending on the size and scope of your incident, you may be required to publicly report the breach and inform individuals whose data may have been exposed.

Data privacy incidents and best practices

This document provides common incident examples. Additionally, it includes insights on ways to gather information about the incident, containment tasks to limit exposure and risk and evidence preservation tips.

Malware intrusion

The threat: Malware incidents can take many forms, from malicious phishing emails and attachments to infected external storage devices. Malicious websites can also infect end users' computers and spread to other employees.

Example: An employee may receive an email to reset an account password by clicking on a Web link. That email is designed to appear legitimate as if it originated from the internal IT department. However, when the link is clicked, malicious code is downloaded and executed to infect the system and exploit vulnerabilities.

Assessing your situation: Revisit the data privacy incident checklist, and ask several questions to determine if you have suffered a malware intrusion:

- 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?

In addition, asking the following questions can help you to investigate your threat:

- 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 immediately prior to and after the suspicious behavior was observed?

Containment processes:

- Disconnect the infected computer from the company network (both wired and wireless)
- Notify all employees about the situation, to keep other users from accessing the same email, attachment or website
- Cut off user access to shared resources and network applications
- Seize any volatile memory (RAM), leaving the computer running but disconnected from company networks
- Take a forensic image of the affected system
- Capture traffic from the machine if the intrusive connection remains active
- Instruct users to scan and wipe any removable storage and drives
- 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 (see the appendix for more information on these sources and how to gather critical information)**:**

- **Application logs**
- **Email server logs**
- **Firewall and intrusion detection systems (IDS) logs**
- **Network traffic logs**
- **Physical storage**
- **System event logs**
- **System memory**
- **Webmail and Web server Internet information service (IIS) logs**

Unauthorized internal or external network access

The threat: Unauthorized access can cause significant damage to your network and data assets. Threats can originate from several sources, including dissatisfied current or former employees or external hackers.

Example: An ex-employee with knowledge of your network logs in to your network via active credentials to access sensitive files.

Assessing your situation: Revisiting the data privacy incident checklist, several questions can help to determine if you have suffered internal or external unauthorized network access:

- Are any of your computers behaving unexpectedly?
- Do you suspect that your system has been infected with malware?
- Has any noteworthy employee behavior taken place outside of the norm such as unusual hours or conduct?
- Have any files been moved, modified, accessed or deleted?
- Do you have irregularities in server logs, such as unusual activity or an increase in failed login attempts?

In addition, asking the following questions can help you to investigate the threat:

- Why do you believe your network has experienced unauthorized access?
- How did you determine that your breach was initiated internally or externally?
- Do you give employees remote access to your network?

Containment processes:

- If the unauthorized access was internal, disable the associated account
- Segregate the system from your network, if possible
- Seize any RAM, leaving the computer running but disconnected from company networks
- Take a forensic image of the affected system
- Capture traffic from the machine if the intrusive connection remains active
- Review backups to evaluate whether documents have been altered, deleted or compromised in any way
- Determine the access level the user had, to ascertain the amount of data that is vulnerable
- Educate employees on the dangers of unauthorized network access and reinforce best practices to protect against attacks

Potential evidence sources (see the appendix for more information on these sources and how to gather critical information)**:**

- **Application logs**
- **Email server logs**
- **Firewall and IDS logs**
- **Network traffic logs**
- **Physical storage**
- **System event logs**
- **System memory**
- **Webmail and Web server IIS logs**

Social engineering attacks

The threat: Social engineering is an emerging threat that involves criminals manipulating your employees to access confidential information. Criminals target your network 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: Revisiting the data privacy incident checklist, several questions can help to determine if you have suffered a social engineering attack:

- Does a non-employee 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?

In addition, asking the following questions can help you to investigate the threat:

- Why do you think you may be the victim of a social engineering attack?
- What information did the attacker seek, and what was provided?
- What systems and information was the attacker given access to?
- 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
- 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 (see the appendix for more information on these sources and how to gather critical information)**:**

- **Application logs**
- **Email server logs**
- **Firewall and IDS logs**
- **Network traffic logs**
- **Physical storage**
- **System event logs**
- **System memory**
- **Webmail and Web server IIS logs**

Lost or stolen computer, mobile device or removable media

The threat: Unfortunately, employees sometimes lose computers or devices that contain company information. Computers or devices are also frequently stolen from several settings, including residences, vehicles or even the office.

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: Revisiting the data privacy incident checklist, several questions can help to determine if you have elevated risks for potential lost or stolen devices:

- Do you allow employees to view and store network data on personal devices?
- Do you utilize encryption for computers and devices that access sensitive data?
- Are files and systems regularly backed up?
- Are devices equipped with remote tracking or wiping tools?

In addition, asking the following questions can help you to investigate the threat:

- What type of encryption do you use for computers and devices?
- Do you utilize rolling backups for employee computers and devices?
- What type of information resided on the lost or stolen computer or device?
- Did the device potentially contain sensitive information such as financial or accounting data, or personally identifiable information (PII) or personal health information (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
- 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 they are available

Potential evidence sources (see the appendix for more information on these sources and how to gather critical information)**:**

- **Backups**
- **Server emails and archives**
- **User network shares**

Common security and privacy 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.

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.

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 stance and reduce the risk of compromised data.

File level auditing – Your organization should consider applying a file-level auditing platform within your organization to increase tracking capabilities. Audit logs should include several details, including the date and time systems were filed, as well as who accessed data and what actions were taken.

Incident response plan (IRP) – Your response plan should outline all processes and contacts for a potential data security incident. Regularly test your IRP after implementation, including topics such as evidence containment and including key groups such as legal and human resources.

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.

Digital evidence collection and preservation – Electronic evidence preservation and collection should be a focal point of the IRP and employee education.

Litigation hold and discovery request plan – In potential civil and criminal cases, your organization should develop a strategy to collect and preserve several data sources. Several pieces of information are typically requested in legal proceedings, including email, network shares and application data.The audit committee should provide oversight to both the internal and the external audit processes. The committee should develop communication processes that minimize duplication of effort between the internal and external audit processes and maximize audit coverage through cost-effective use of company resources.

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 must 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 impact information security. Training should include education on common breaches such as phishing attempts and social engineering attacks.

Building access policy and procedures – Develop clear policies and procedures that govern building access for employees, vendors and visitors, as well as the removal of any physical property.

Identification and logging for vendors and visitors – Implement a process to identify and keep records of vendors and guests that visit your facilities.

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.

Automated script to remove memory entries and temporary files – You should consider implementing logon batch script to remove temporary and pagefile entries. These artifacts often include sensitive information and malware-related files.

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

Full disk encryption – All laptop and desktop computers should include full disk encryption security 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.

Outlook Web Access (OWA) – Secure access to Web-based email applications using the HTTP protocol. The printing and emailing of emails and attachments should also be discouraged unless necessary. OWA access logs should be kept for a time period deemed appropriate, but no less than 60 days.

Guest wireless network – Your guest wireless network should include WPA2 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.

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.

Password complexity – All network and application accounts should have an appropriate level of complexity. Passwords should also be changed on a regular basis to discourage hacking.

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.

Disaster recovery drills – Your company should perform regularly scheduled disaster recovery drills with vendors and your Internet service provider to help ensure that your IRP takes emerging threats into consideration and is properly scoped for coverage and resources.

Fire protection for server room(s) – IT server room(s) must have protection measures in place to protect critical equipment that could be damaged in the event of a fire.

Appendix:
Potential evidence sources

The following list defines several evidence sources and how they can help your organization identify and investigate a potential incident.

- **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:** Do you have backups in place for user systems and data? If so, those backups can help determine the scope of damage related to the loss or theft. They can also help restore the user's system and any previous work. In addition, backups can help discover how much PII or PHI the computer or device contained and subsequently whether the individuals must be notified and the breach publicly reported.
- **Email server logs:** You can gather valuable information from Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and transaction logs of all sent and received emails. Key evidence sources include the SMTP, POP and Internet Message Access Protocol (IMAP) logs which record communication and authentication, and transactions logs that track sent and received messages. You can utilize these tools to determine where email infections originated and track unauthorized processes, such as computers that have been taken over by botnets to distribute spam. If logging took place when the incident took place, containment is fairly simple. However, you must act quickly before evidence is automatically deleted.
- **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.
- **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.
- **Physical storage:** Physical storage includes tools or devices that can store electronic media, including DVDs, CDs, network storage, hard drives, portable drives, tablets and mobile devices. These sources are often an incident's key source of evidence. Determining the optimal method to preserve physical storage is critical. If proper backup and preservation methods are not implemented, evidence can be destroyed or overwritten. You must understand what physical storage sources were in use when the incident occurred, and be able to access that storage during the investigation.
- **Server emails and archives:** Email servers and archives can help determine the scale of the loss or theft. They can also help restore the user's system and any previous work. In addition, the emails and archives can help discover how much PII or PHI the computer or device contained and subsequently whether the individuals must be notified and the breach publicly reported.

- **System memory:** RAM temporarily stores code, data and settings for your system. This memory can often includes critical evidence of the execution and activity of malicious code, as it typically leaves few clues on hard drives and other storage. 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 and 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.
- **User network shares:** User network shares can help determine the scale of the loss or theft, based on the user's access and files. They can also help restore the user's system and any previous work. In addition, user network shares can help discover how much PII or PHI the computer or device contained and subsequently whether the individuals must be notified and the breach publicly reported.
- **Webmail and Web server IIS logs:** These tools are communication and authentication records between hosts, servers, browsers and Web-based 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 FTP, Web and webmail servers. If logging took place when the incident took place, containment is fairly simple. However, you must act quickly before evidence is automatically deleted.

Power comes from being understood.®

When you trust the advice you're getting, you know your next move is the right move. That's what you can expect from McGladrey. That's the power of being understood.

855.810.0615 - Incident Response Hotline

800.274.3978
www.mcgladrey.com

McGladrey

IS-NT-RAS-ALL-0415