INFORMATION SECURITY INCIDENT RESPONSE GUIDE

beazley

NAVIGANT

NAVIGANT

INFORMATION SECURITY INCIDENT RESPONSE GUIDE

OVERVIEW

Navigant, in partnership with Beazley, developed this response guide to provide information on good practices during common data security incidents, sample documentation, and general information technology risk areas. The information provided is derived from experience and industry standards and is intended to be informational as each incident is unique across varying organizations resulting in unique response requirements that cannot be defined in a general document such as this document.

CONTENTS

SECTION I – GENERAL INCIDENT RESPONSE GUIDELINES

Outlined below are key steps to handle a response to many types of information security incidents. These guidelines are summarized according to the National Institute of Standards and Technology (NIST) – Computer Security Incident Guidelines manual.

Identification

Identifying the threat and the nature of the threat is important not only to determine the proper course of action to take in order to respond to an incident but to also assess the security of data and systems. Identification of a threat is possible by any individual within a network or organization. Proper training should be implemented to teach staff and users about the vast number of types of threats along with best practices to avoid them.

Validation/Assessment

Incidents may begin with an employee reporting odd or inappropriate behavior from a device or loss of access to data, software, hardware, or networking resources. If the behavior is not first encountered by IT staff, it will likely be reported to them. IT staff should be prepared to validate the incident and determine the nature of the incident by using the proper tools as discussed below.

Communication

The incident may result in undesirable communication within the company to outside entities, including the intruder. For example, if intruders have gained access to an employee's email account, further communication using that account could notify the intruders they have been detected and cause them to destroy evidence or cause further harm. Be prepared to use a separate method of communication such as cellphones, voicemail, text messages, etc.

Containment

Once a threat or intruder has been identified, containing the threat is the next highest priority. Steps should be taken to ensure that evidence is not tampered with, which may mean restricting access to hardware or physical locations. Depending on the nature of the intrusion, devices may need to be shut down, segregated to a local VLAN or left running in order to facilitate further investigation.

Preservation & Evidence Collection

A primary reason for gathering evidence during an incident is determine the extent of the incident. There may also be a need to preserve and collect evidence for legal proceedings. It is imperative to clearly document how all evidence has been collected. Evidence need be accounted for throughout the whole process. Chain of custody forms should be used to detail the transfer of each piece of evidence each time that piece of evidence is transferred to a different party.

Recovery of Systems

Recovering from an incident includes both reactive and proactive responses. Reactive responses include applying any necessary patches and updates to systems found to be vulnerable. Proactive responses include the advance preparation of backups of critical systems, databases and data as well as images which preserve desired installation and settings of operating systems and applications. Users should be aware of backup systems and how they function, so that they do not accidently lose data by storing it in the wrong place, or leaving their system off when backups occur.

Identification of Exposed Protected Health Information ("PHI") and Personally Identifiable Information ("PII")

When PHI and PII have likely been exposed, identifying the exact set of impacted individuals and specifically what information was exposed about each individual is critical. Specific identification allows companies to avoid over-notifying individuals and allows the legal department to meet specific requirements for notice by state and exposure type. This is possible through programmatic data mining performed at the file level to pinpoint specific files and emails containing PHI and PII. Programmatic tools can also be used to de-duplicate individuals exposed with varying level of information across multiple files and to prepare a unique list of individuals to be notified for ultimate circulation to a notification vendor.

Notification

When a confirmed or potential incident is discovered it is important to notify appropriate individuals of the incident. This may include internal stakeholders such as information security officers, system owners, human resources, public affairs, and the legal department, as deemed necessary and appropriate as indicated by company guidelines. During the course of the investigation, if PHI or PII is identified and compromised the institution may have the obligation to notify the individuals, including clients, patients and business partners, whose data was compromised and may need to report the breach publicly. Proper documentation will aid in the notification process. Documentation should include facts such as who first identified the incident, what was the date and time that the incident was detected, what symptoms were encountered, who was notified of the incident and when were they notified, and what steps were taken to handle the incident.

SECTION II – COMMON DATA PRIVACY INCIDENTS & BEST PRACTICES

MALWARE

Description

A malware incident can originate from various sources, including phishing email, externally attached storage devices, and email attachments. Malware can also infect and expand from an end user's computer when the end user clicks on a link to a malicious website.

Situation Example

A user receives an email requesting that the user reset a password by clicking on a website link. The email was spoofed to appear that it originated from the employee's internal IT department, and the link caused the user to download and execute a malicious code that exploited system vulnerabilities.

Sample Investigative Questions

- Has anyone you communicated with via email claimed to have received suspicious emails from you?
- Have you been unable to visit certain websites, especially those related to anti-virus or system updates?
- Have you been recently experiencing unusually poor system performance?
- Has your computer been displaying unexpected behavior after accessing an unknown website or opening an email attachment?
- Do you use the same login and passwords for multiple systems or accounts?
- Do you handle sensitive information such as human resources, accounting, or financial records?
- Do you use online banking or electronic payment systems?
- What was done immediately before and after the suspicious behavior was noted?

Common Containment Tasks/Best Practices

- Segregate the affected computer from the wired and wireless network, but leave the machine running so that volatile memory can be captured.
- Inform all employees not to open the malicious email, attachment, or website.
- Disable user's access to network shares and other network applications.
- Capture volatile random access memory (RAM).
- Capture a live forensic image of the affected system.
- Advise employees to scan/wipe removable media.
- Advise user and employees of unsafe activities that can result in the systems being infected by malware.
- Block incoming and outgoing email from the source of the malicious email or site.

RANSOMWARE

Description

Ransomware is a type of malware that encrypts files on a user's computer and requests a ransom payment to decrypt the files. A ransomware incident can have traits like a malware incident, where the initial infection originates on an endpoint computer or from a compromised server and then cripples the rest of an organization's network by encrypting files on more servers and endpoints.

Situation Example

A network share drive is found to have unreadable documents. An HTML file appears on the share drive that contains information declaring the files have been encrypted, with instructions to pay a ransom to obtain the decryption keys to recover the encrypted files.

Sample Investigative Questions

- Which folder or folders on the network share have been encrypted?
- Have other files on the server hosting the file share been encrypted?
- Has a user or users reported to the IT help desk that they received suspicious emails?
- Have you traced the owner of the encrypted files to determine which computer has been infected with ransomware?

Common Containment Tasks/Best Practices

- Inform all employees not to open the malicious email, attachment, or website.
- Temporarily disable all file shares on your network until the computer from which the ransomware infection originated is identified and disconnected from the network.
- Upon identification of the infected computer, segregate it from the wired and wireless network.
- Disable user's access to network shares and other network applications.
- Advise employees to scan/wipe removable media.
- Advise users and employees of unsafe activities that can result in systems being infected by malware.

UNAUTHORIZED NETWORK ACCESS – INTERNAL/EXTERNAL

Description

Unauthorized access by hackers, current employees, or former employees.

Situation Example

A former employee with detailed knowledge of the infrastructure uses his active credentials to access files on the organization's systems.

Sample Investigative Questions

- Why do you think there was unauthorized access?
- Do you suspect that malware was installed on the accessed system?
- How did you determine if this was internal or external unauthorized access?
- Is the accessed computer behaving unexpectedly?
- Did anyone witness unusual behavior from this employee, such as staying late or coming in early, or any behavior outside of his or her normal course of work?
- Does the employee have access to remote login tools?
- Do the server logs show unusual network activity or a large number of failed login attempts?
- Does it appear that files have been accessed, deleted, modified, or moved?

Common Containment Tasks/Best Practices

- If external, disable the account that was used for the access.
- Segregate the affected computer from the wired and wireless network, but leave the machine running so that volatile memory can be captured.
- Capture volatile random access memory RAM.
- Capture a forensic image of the machine where the potential breach is believed to originate.
- If the intrusive connection is active, capture traffic from the computer.
- Determine if documents have been changed, deleted, or tampered with by reviewing backups.
- Assess what level of access to each system and network storage area the disgruntled employee had so you can determine how much data they could have accessed.
- Remind employees and users of the dangers of unauthorized access to company systems, and provide a list of best practices to prevent attacks that result in unauthorized access.

UNAUTHORIZED NETWORK ACCESS – THIRD PARTY

Description

Unauthorized access, disruption, or data loss that originates via shared access to a network from a contractor, vendor, or partner that results in unauthorized access to first party's data. Attacks may also be launched using data such as credentials, passwords, or Social Security numbers originating from an unrelated third-party breach. Third parties are often the weakest security link and this vulnerability is increasingly being targeted by attackers looking to penetrate otherwise secure networks. When a security incident is caused by a third party, the first party must investigate the incident to determine the scope of the unauthorized access and to identify and potentially notify the affected individuals.

Situation Example

Many recent high-profile breaches can be categorized as third-party compromises. These include the 2013 Target breach of their payment system data, which was traced back to a compromise of Target's HVAC contractor. Another example is the 2016 IRS attacks, as they were made possible using Social Security numbers that were originally obtained from previous unrelated breaches.

Sample Investigative Questions

- Which vendors, partners, or contractors have access to the corporate network infrastructure?
- What level of access do partners, vendors, or contractors have to systems that contain, or are linked to, the compromised data?
- Which individuals have access to third-party access credentials?
- What network segmentation is in place between the systems accessed by third parties and other parts of the enterprise network?
- What is the business impact of restricting access to and from the identified third party?

Common Containment Tasks/Best Practices

- Change user account passwords.
- Disable or restrict relevant third-party access.
- Inform relevant vendors, contractors, and partners of the attack to ensure proper preservation and containment protocols are implemented throughout the supply chain.
- Enable two-factor authentication for remote network access originating from outside the network by personnel and all third parties.
- Develop strict policies and approvals for the issuance, levels, and revocation of credentials and access issued to all third parties.
- Conduct periodic audits of credentials and access levels provided to vendors, contractors, and other third parties.
- Require cybersecurity assessments for new third parties as part of the contracting/onboarding process to ensure compliance with the internal enterprise information security program.

NATION-STATE

Description

The nation-state cyber adversary is a foreign government with both the capability and the intent to persistently target a specific group, such as a governmental entity, educational or research

facility, or corporation. The main nation-state cyber actors are China, Russia, Iran, and North Korea. The goal can be economic gain or political advantage. These nation-states use internet-enabled espionage for a variety of intelligence-gathering techniques to access sensitive or proprietary information. Other attack vectors include infected media, supply chain compromise, and social engineering. The attacks aim to install custom malicious malware code on one or more computers and to remain undetected.

The People's Republic of China (PRC) is one of the world's largest economies and has one of the world's largest defense budgets. The PRC is unique in that the PRC's information and operations intelligence apparatus, along with its warfare doctrine, includes the concept of "network warfare" or cyber warfare and acquisition of secrets. Many countries have long accused the PRC of aggressively pursuing economic espionage, traditional espionage, and cyber hacking to gain trade-secret advantage from other states. The United States, along with its allies, have traced attacks from the PRC to private and government agencies.

Russia is one of the premier cyber forces in the world. Russian intelligence services have been accused of cyber warfare and cyber attacks that include allegations of distributed denial-of-service (DDoS) attacks against banks and the oil industry. They also have been linked to numerous cases of stealing proprietary trade secrets from the U.S. defense industry, both by traditional hacker attacks and complex malware attacks. Most recently, they have been accused of meddling in the U.S. presidential elections.

Iran in recent years has been linked to numerous DDoS attacks across the U.S. banking industry and oil industry. Although not as capable as the PRC or Russia, Iran has become a cyber force mainly due to the ability of buying capability on the "dark web." The ability to rent people, processes, and computer power to perform the hacking has changed the modern-day landscape of cyber threats.

North Korea is relatively new as a nation-state player and less is known about its cyber warfare agency. North Korea was blamed for the 2014 destructive cyber attack on Sony Pictures Entertainment, as well as major cyber attacks on South Korea in 2009, 2011, and 2013.

Situation Example

An internet service provider (ISP) is the victim of a large-scale DDoS attack that disrupts its customers' service in the United States. As a part of the attack, the ISP discovers the traffic is emanating from international IP addresses that are not typically seen.

Sample Investigative Questions

- Is international web traffic typical for the business?
- Is the time of the suspected attack or anomalous behavior abnormal for the business?
- Are there critical systems that could have been accessed via external actors?

Common Containment Tasks/Best Practices

- Implement an awareness and training program.
- Patch operating systems, software, and firmware.
- Use effective anti-virus and anti-malware solutions that update and scan regularly.
- Manage the use of privileged accounts.
- Configure access controls to grant the least amount of privilege needed by each user.
- Employ both network-based and endpoint monitoring.

SOCIAL ENGINEERING

Description

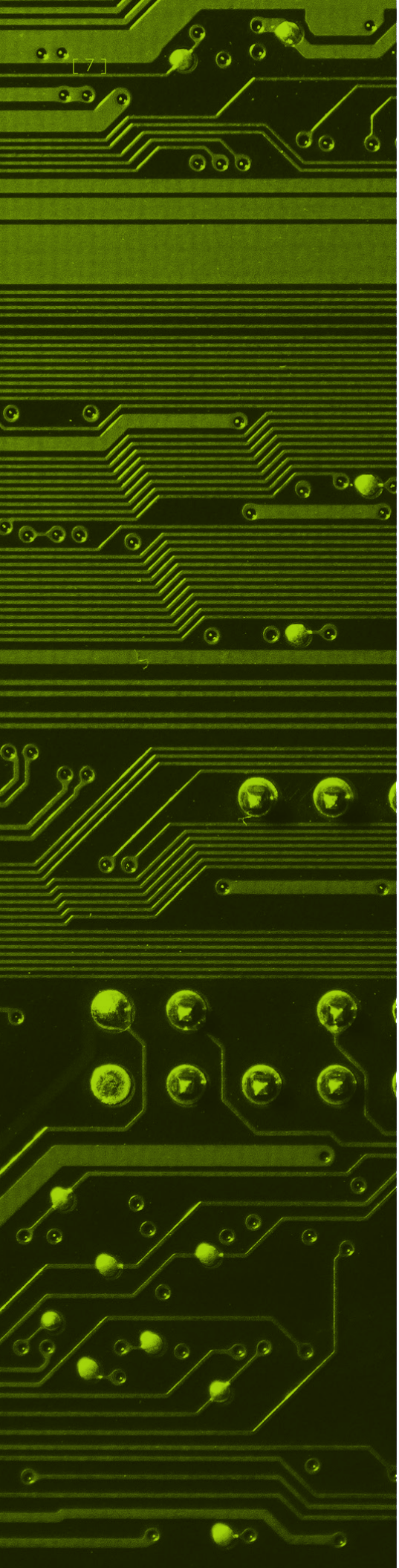
Social engineering is the art of manipulating people so they give up confidential information. Criminals may seek passwords, credentials for email, banking, or other applications, or other information that will assist in a compromise, or they attempt to gain access to your computer to install malicious software.

Situation Example

An employee receives a phone call from an unknown individual asking for account information to obtain passwords or claiming to be from the company's IT staff looking for access to the employee computer to "fix bugs."

Sample Investigative Questions

- Why do you suspect there was a social-engineering attack?
- What information did the attacker ask for and what did he receive?
- What systems or information did the attacker access?
- Did a nonemployee seem to be highly aware of company matters?
- Have you recently been asked to provide personal or proprietary information to anyone inside or outside the company? If so, who asked?
- Has another employee recently asked you to provide information that is not necessary to their job function?
- Has a person — employee or non-employee — asked you questions about the company or proprietary information that you were uncomfortable answering?
- What information do you have access to, and does it include sensitive information such as human resources, accounting, or financial records?



[7]

Common Containment Tasks/Best Practices

- Disable the accounts accessed by the attacker.
- Segregate the affected computer from the wired and wireless network, but leave the machine running so that volatile memory can be captured.
- Inform all employees about this attack so they are not susceptible to it.
- Capture volatile random access memory RAM.
- Capture a forensic image of the machine or machines the attacker may have accessed.
- If the intrusive connection is active, capture traffic from the computer.
- Remind employees to be wary about providing logins, passwords, and proprietary information to unauthorized sources through emails, phone, and face-to-face conversations.
- Inform all employees about this attack so they will be aware of the potential methods used by the attackers.

BUSINESS EMAIL COMPROMISE

Description

Business email compromise, also referred to as executive or CEO fraud, usually involves the identities of senior executives. It often begins as a phishing scam targeting companies that work with foreign suppliers, partners, or customers who routinely require payment via wire transfer. Legitimate business email accounts are compromised through social engineering, a brute-force intrusion attack, or a remote desktop protocol (RDP) attack. Posing as the executive, the attacker instructs finance employees to issue a wire transfer. The attackers often create forwarding rules for the email account to hide legitimate emails that would cause the employee to question a wire transfer or other instructions.

Situation Example

An accounts payable employee who routinely facilitates wire transfers to foreign business partners receives what appears to be a legitimate email from a senior executive requesting a wire transfer to a legitimate foreign supplier but at a new bank account. The link points to a website that looks legitimate but turns out to be fraudulent. The executive is on vacation, so the employee replies to them in an attempt to confirm the request. The senior executive tries to respond to notify the employee that the wire transfer request is fraudulent, but the attacker has created a rule sending all emails from that senior executive to the trash folder. The employee sends the wire transfer to the new bank account controlled by the attackers.

Sample Investigative Questions

- What are the roles and responsibilities of the person whose email was compromised?
- What systems did the attacker access?
- Have you recently been asked to provide personal or proprietary information to anyone inside or outside of the organization?
- What access do you have to accounts that may be used to support wire transfers?
- Have you recently been asked to transfer money to a new or existing supplier outside of the usual business process?
- Have any colleagues reported unexpected messages requesting information that could be used to transfer money from organization accounts?
- Have any business contacts requested that communication go through their personal email accounts?

- What information do users have access to, and does it include sensitive information such as human resources, accounting, or financial records?

Common Containment Tasks/Best Practices

- Disable the accounts compromised by the attacker.
- Hold requests for international wire transfers for a brief period — e.g., two days — to verify the legitimacy of the request.
- Review all wire transfer protocols and controls.
- Immediately delete and report unsolicited email from unknown parties.
- Tighten your controls around what is posted to publicly available sources and social media sites. Pay attention to organizational hierarchy, executive job descriptions, and out-of-office details.
- Remind employees to be wary about providing logins, passwords, and proprietary information to unauthorized sources through emails, phone, and face-to-face conversations.
- Alert all employees with the authority to initiate money transfers about these types of attacks.

TAX FRAUD

Description

Perpetrators steal personally identifiable information (PII), including taxpayer identification numbers, and then file fraudulent returns to get refunds that they redirect to accounts they control.

Situation Example

An accountant logs into her computer and notices several PDF files containing client tax returns were created on her computer during her absence. Alternatively, she has several clients contact her saying fraudulent tax returns have already been filed.

Sample Investigative Questions

- Does anyone else have access to the system where the PDFs were found?
- Is the computer connected to the internet?
- What logs are available for review? Firewall? System logs?
- Does a backup of the computer from before the incident exist?
- What steps were taken after noticing the issue?
- Have you received notice that any returns were filed that you didn't submit?

Common Containment Tasks/Best Practices

- Change user account passwords.
- Preserve all network, firewall, and system logs.
- Isolate the accountant's computer from the network.
- Forensically preserve the accountant's computer.

POINT OF SALE

Description

A remote-access attack on a point-of-sale (POS) vendor to expose payment card transactions. One common characteristic of a POS security incident is that the attackers attempt to gain access to the target environment and then obtain elevated access privileges. After this is accomplished, the attacker often deploys malware to other POS systems and servers in the environment, and then starts the process of colleting credit card data. The attacker will generally set up services to have the malware executed when the systems reboot.

The area that many malware variants attack in POS systems is the memory of the computer because it is the one area where the data is usually unencrypted for temporary processing. This process of an attacker targeting the memory is often referred to as "memory scraping." From here the data is usually written somewhere on the system or to the environment in a text file, which is typically encrypted. Then the attacker exfiltrates the collected data through file transfer protocol (FTP) or other protocols that can transfer the data to other compromised servers on the internet.

Situation Example

A restaurant chain is notified by a third party like Brian Krebs (a well-known journalist who concentrates on data breaches) or one of their merchant banks to notify the organization that there has been fraud on several credit card accounts and a common point of purchase (CPP) analysis points to the restaurant chain.

Sample Investigative Questions

- Have new user accounts with administrative privileges been created or have user accounts recently been given elevated administrative privileges?
- Have new service accounts with administrative privileges been created?
- Has there been abnormal user authentications to servers and endpoints?
- Has abnormal FTP traffic been reported?

Common Containment Tasks/Best Practices

- Conduct a root-cause analysis to determine the before-and-after values, when access occurred, and where the IT infrastructure was penetrated.
- Be prepared to take systems like computers or servers offline and direct the IT team to pivot all systems to another secure mode.
- You may need to disconnect or restrict vendor access to your systems to prevent further data leaks while the incident containment/identification period is underway. Vendors who have portal access to your organization need to be vetted.

- Block sensitive data transfers via FTP and close data ports immediately to prevent further data leakage.
- Capture all traffic and commence patching, application white-listing, and privilege/access management to help limit or block the pathways for the malware to continue obtaining sensitive data.
- Document all the findings and create disk images and detailed reports that can aid in further investigation or mitigate future risks.
- Educate employees about what happened and mandate all passwords be updated on uncompromised systems, and then on compromised systems once the system is no longer infected.
- Forward logs to a centralized logging environment to create an isolated archive.
- Monitor and review anti-virus detections from both commercial and native platforms.
- Consider Advanced Endpoint Threat Detection (AETD) tools to monitor and alert for anomalous activity on sensitive systems such as POS terminals and application servers.

ATM SKIMMING

Description

ATM skimming is the process by which criminals install a "skimmer" over the ATM's card reader to capture information on a person's debit card. The skimmer appears to be a legitimate card reader. While the skimmer captures the information on the ATM user's debit card, it doesn't capture the user's PIN number. Thus, when criminals install a skimmer they normally install a hidden camera so they can record the ATM user's PIN number as it's entered. The camera is usually very small (pinhole size) and is hidden close to the ATM. Criminals have also been known to install fake keypads over the legitimate keypads to capture PIN numbers.

Situation Example

Customers who frequented ATMs located outside of two local convenience stores noticed charges to their bank account for purchases they didn't make. The charges were for items purchased from a well-known online retailer and each charge exceeded $100.

Sample Investigative Questions

- Are there cameras that have a direct line of site to the ATM?
- Is the footage backed up and regularly reviewed?
- Are the ATMs connected to the network infrastructure?
- Did any customers report seeing anyone who looked out of place or stood unusually close to them when they were using the ATM?
- Did any customers report noticing anything unusual about the way the card reader looked or how it worked when they inserted their ATM card?

Common Containment Tasks/Best Practices

- ATMs inside a business should be placed in view of the cashiers or sales associates to discourage alteration or tampering by a criminal.
- Store personnel should be alert to persons loitering around the ATM and watch for any unusual activity.
- Store personnel should periodically examine the ATM machine for any sign of tampering or changes to the appearance of the ATM.
- A card reader or keyboard that looks out of place should be reported immediately to the owner of the ATM.

LOST/STOLEN

Description

A computer system or mobile device can be lost by an employee during travel or other activities, or unlawfully removed from a vehicle, office setting, or residence.

Situation Example

An employee's laptop gets stolen from his parked car during lunch time.

Sample Investigative Questions

- Was the stolen computer or device encrypted?
- What type of encryption was being used?
- When was the last complete backup of the computer or device performed?
- Do you keep rolling backups for all devices?
- What information was on the stolen computer or device?
- Did it potentially contain personally identifiable information (PII), personal health information (PHI), or financial or accounting records?
- Was only a single device stolen, or were other devices or hard copy documents taken?
- Are there any remote tracking or wiping tools installed on the stolen computer or device?

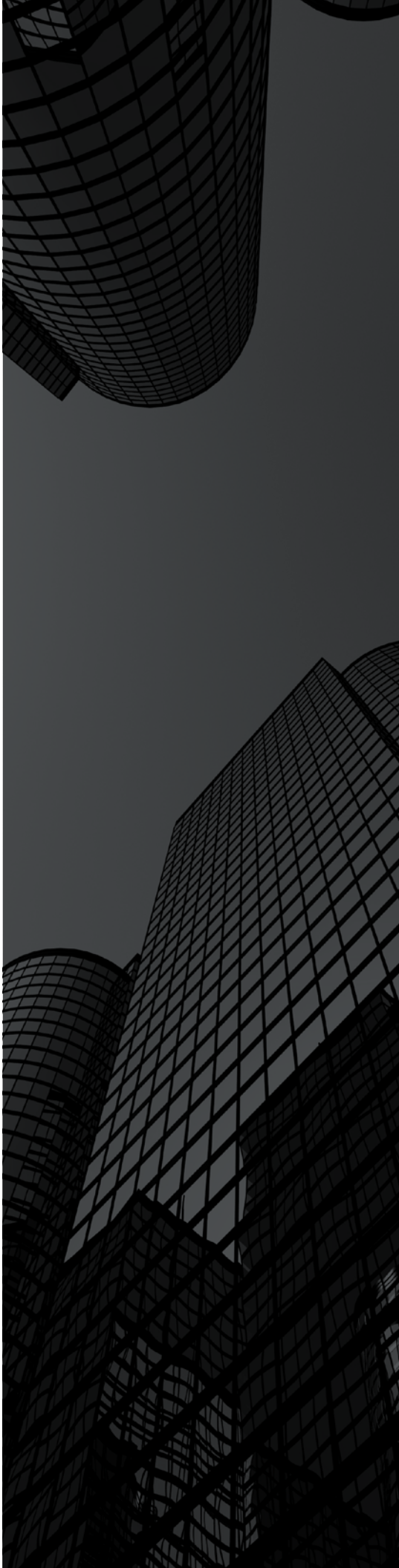
Common Containment Tasks/Best Practices

- Change user account passwords.
- File a report to the police to report the device as stolen.
- Create a companywide notification to remind employees and users of best practices to secure company-issued devices, equipment, and documents.
- If remote wiping or tracking are available, make use of them immediately.

SECTION III – COMMON EVIDENCE SOURCES/ PRESERVATION

The following is a list of common sources of evidence that should be preserved, as they are utilized to investigate the many types of intrusions addressed above. Access to these forms of evidence makes the investigation faster and less costly, while also giving the company the greatest opportunity to demonstrate that the data privacy incident was not a data breach as defined by the law. The following is a list of evidence types:

- **Email Server Transaction Logs.** Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and full transaction logs of email sent and received. The SMTP, POP and Internet Message Access Protocol (IMAP) logs are records of the communication and authentication between mail client software, hosts, and servers. They, along with transaction logs, which are records of messages being sent and retrieved, can be very valuable evidence sources. These logs can be used to track points of infection that originate with malicious emails and to monitor unauthorized activity such as machines that have become part of spamming botnets. Assuming logging was enabled at the time incidents occurred, their preservation is simple, but should be done as soon as possible to prevent automatic purging and deletion.
- **Webmail/Webserver IIS Logs.** Web server Internet Information Services (IIS) logs and webmail logs are records of communication and authentication between the web-based email client, web browsers, hosts, and servers. These records can include host and user activity, files, IP addresses, URLs that were accessed or visited, browser and OS activity, and error logging. These logs can be used to track and monitor incidences such as the origin of an infection, unauthorized access to webservers, FTP servers, and webmail servers and accounts. Assuming logging was enabled at the time incidents occurred, their preservation is simple, but should be done as soon as possible to prevent automatic purging and deletion.
- **Computer System Memory.** Volatile memory, or RAM, is the memory that is used temporarily by a system to store code, data, and settings. Critical evidence of the execution and activity of malicious code is often present in volatile memory and malicious code may leave few if any traces on hard drives and storage devices. Evidence from volatile memory must be preserved using appropriate tools while the infected system is still running. This can run counter to the immediate inclinations of first responders to an incident, which is often to shut down compromised machines to prevent further infection or damage. Preservation efforts should seek to maintain evidence in volatile memory while also containing the malicious code.
- **Physical Storage Media.** Physical storage media is any device that can store electronic data. Physical storage may include but is not limited to, hard drives, thumb drives, DVDs, CDs, mobile and tablet devices, and network storage. Physical storage is often the primary source of evidence related to an incident. When responding to an incident, it is important to determine the best method of preserving and securing physical storage. Evidence of an incident may be destroyed or overwritten by accidental or intentional system activity if proper backup, preservation, and methods to secure data are not taken. Physical storage must be accessible when the incident is being investigated. It is also important to understand what physical storage media was accessible at the time of the incident.
- **Network Traffic Logs.** Network traffic logs include information about the source and destination IP addresses of network activity, as well as logs of VPN (virtual private network) and data loss prevention utilities. Evidence from network traffic logs can include points of infection, such as access to infected or malicious websites, or the movement of sensitive material outside of the network. Network traffic logs may be



ongoing monitoring or limited periods of monitoring meant to capture specific types or periods of activity. Even if no network logs exist from the time of the incident, turning on network traffic logging may allow you to capture evidence of ongoing malicious activity.

- **System Event Logs.** Event logs include the logs created by operating systems, hardware, and some internal and third-party applications. Event logs can include a variety of activity, such as the startup and shutdown of a system and its services, modification of settings, access to network resources and accounts, and the escalation of privileges. Event logging is usually enabled to some degree on most systems for auditing purposes, and these logs should be preserved as soon as possible to prevent automatic purging and deletion.
- **Application Logs.** The logs of local and network third-party applications can include records of when programs were executed, when errors occurred and when accounts and data were accessed or modified. Application logs may not directly capture malicious activity, but they may contain evidence of errors or modifications caused by malicious code. An inventory of installed and permitted applications should be maintained by IT to track potential sources of evidence. IT should also be aware of logging capabilities of any critical applications.
- **Firewall/IDS Logs.** Firewall and intrusion detection system (IDS) logs are records of internet traffic entering and leaving a network. Firewall and IDS logs may include items such as the origin and destination of data and connection attempts, as well as the volume of data. Network connections have two basic components, a pair of IP addresses and a pair of port numbers. IP addresses identify the computers that are communicating and the port number is associated with the application or service that is being used. Firewall logs provide a record of both the IP address and port numbers from systems that are communicating. Firewall and IDS logs can be used to identify events such as abnormal or malicious network activities, unsuccessful login attempts, and unauthorized network access.
- **Computer Backups.** Backups of the user's system or data created by the user may be created on a regular schedule or at other times. Backups can be used to determine whether PII or PHI resided on the user's system and, if so, how much. Any legal obligations to notify affected individuals or report a breach to regulators will depend on the type and amount of data compromised, so backups can help determine the scope and scale and cost associated with the potential theft of data. Backups can also be used to restore the user's system and previous work.
- **Network/User Shares.** Network login credentials for the user whose laptop was stolen should be changed immediately to prevent the stolen laptop from accessing any additional network data. Department or user network shares can be used to determine the scope and scale associated with the potential theft of data based on the files the user created or had access to. Network shares can potentially be used to determine if any and how much PII/PHI resided on the user's computer. User shares can also be used to restore some if not all the user's user-created data and previous work.
- **Server Email/Archiving Solutions.** Emails on the exchange server can potentially be used to determine the scope and scale associated with the potential theft of data. Network email can be used to determine if any and how much PII/PHI resided on the user's system. Network email can also be used to restore the user's local email.

SECTION IV – INCIDENT RESPONSE CONTACT LIST

IT RESPONSE TEAM	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

IT RESPONSE TEAM	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

LEGAL	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

LEGAL	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

HUMAN CAPITAL	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

CORPORATE COMMUNICATIONS	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

VENDOR	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

VENDOR	
	<Insert Responsibilities>
OFFICE	
MOBILE	
EMAIL	

SECTION V – SAMPLE INCIDENT DOCUMENTATION

One of the most commonly overlooked items during an incident response is documentation. Outlining how an incident was handled is crucial for investigative purposes and to demonstrate the steps taken when asked during a post-incident review. The information captured in the documentation can be very beneficial and provide a "lessons learned" to help improve future incident responses. Seek legal input regarding what to document and how to document the required information.

Documentation provides an insight into "how things were" at the time of discovery and provides details on network/setting changes made to contain the incident. Information contained in an incident report should include:

- Date/time of incident
- Incident description
- Details on action items & results
  - Date/Time action performed
  - Who performed the action
  - What action was performed
  - Results of such action
- Individuals contacted/involved in incident
- Screen captures or other supplemental documentation

Pictured below is a sample segment of an information security incident report showing basic data points that should be recorded in a timely manner (See Fig 1).

Fig. 1 – Screen Capture of Sample Incident Report

INFORMATION SECURITY INCIDENT REPORT			
Incident Description			
Reporting Person:		Incident Number:	
Date/Time Reported:		Time Zone:	
Describe Initial Report of Inicident (Malware, Lost Computer, etc)			
Incident Action Items			
Date/Time of Action	Individual Performing Action	Action Description & Any Results (Notification, Remediation, Preservation Tasks, etc)	

SECTION VI – CHAIN OF CUSTODY FORM DESCRIPTIONS (EXAMPLE)

Field name and definitions below provide guidance on the sample chain of custody form attached as Appendix 1.

FIELD NAME	FIELD DEFINITION	FORMAT EXAMPLE
Client/Matter Name	Common name used to identify the matter (i.e., ABC Company, XYZ Investments). This name must be unique to this project	
Matter Code	This is the unique number assigned to an incident.	######
Custodian Name	The full name of the person who uses or owns the evidence being collected. Group Name or Organizational Name can be used for evidence that is shared by many custodians (e.g. HR or LEGAL)	Last Name, First or list Group/Organizational Name
Company Name	Company evidence received from	
Manufacturer and Model / Network Path / Email Address	Manufacturer Make and Model of Computer System / Full UNC Path of Network Share Collected / Email Account Collected	
Serial Number	Manufacturer Serial Number of the evidence being collected (not all evidence will have a serial number; enter N/A for evidence without a serial number)	
Physical Size (GB)	Storage capacity of device being collected (e.g. Hard Drive Capacity)	100.0

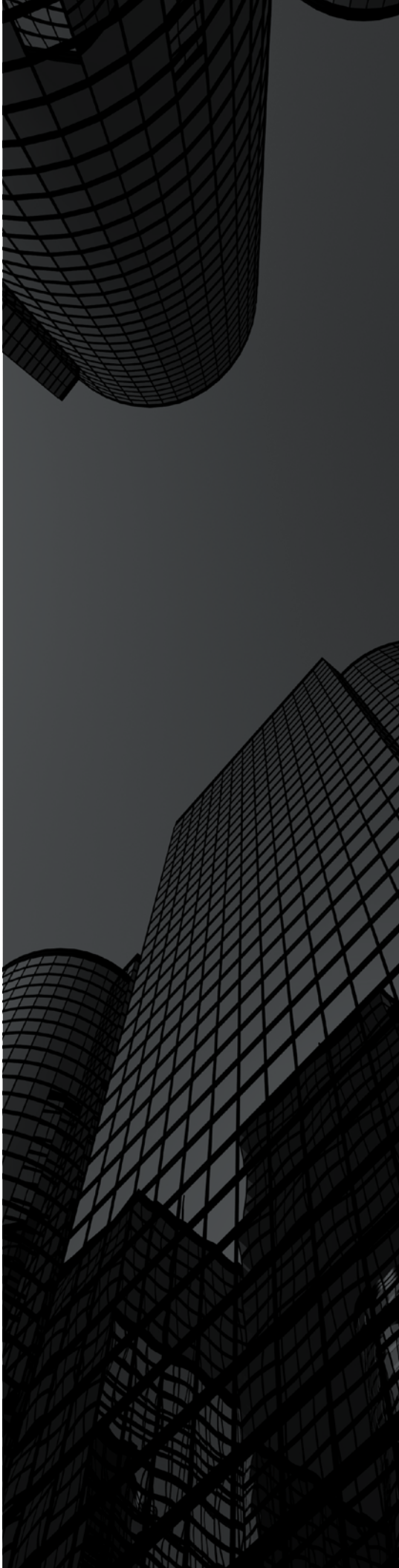
FIELD NAME	FIELD DEFINITION	FORMAT EXAMPLE
Date Collected	Date the collection was started for the listed evidence	DD/MM/YYYY
Collection Method	Active File Collection, Forensic Image (Clone, E01, DD), Backup, Logical Image, etc	First Initial and Last Name
Location of Collection	Physical location of the consultant at the time of the collection	Office Address, City, State, Country
Notes	Other identifying information, specific folder paths containing relevant data, anomalies encountered or errors, etc	123456-001-SmithJohn-D 123456-002-SmithJohn-L 123456-003-JonesSara-E
Evidence ID	Unique name given to the collected evidence. This may be the name of a forensic image file or folder name containing network share data if an active file collection. Example of the name format is the incident/project number followed by a dash then an incrementing three digit number followed by another dash then the Custodian Last Name First followed by a dash and then the data source letter. See data source table on page 12. The three digit number increments up for all evidence collected on a matter. The first item collected would be 123456-001-Name-D and the tenth item collected would be 123456-010-Name-L.	
Storage Device (Evidentiary)	Unique ID or label given to the media used to store the original data collected/imaged	
Storage Device Serial Number (Evidentiary)	Manufacturer Serial Number of the Storage Device containing the original data collected/imaged	
Storage Device (Backup)	Unique ID or label given to the media used to store the backup copy of the data collected/imaged	
Storage Device Serial Number (Backup)	Manufacturer Serial Number of the Storage Device containing the backup of data collected/imaged	
Acquisition Hash	Hash algorithm (MD5, SHA1) followed by the hash value of the imaged/collected data	
Verified? Yes/No	Verification of the Acquisition Hash value	
Unique Label/ID	Identifier that is not put on by the manufacturer, usually an “Asset Tag” or other designation.	
Received From	Representative, onsite contact, or custodian	First and Last Name
User ID	Computer Logon ID, Application Logon ID, etc.	
BIOS Date/Time	Date & Time of the Computer BIOS	
Actual Date/Time	Actual Current Date & Time	
Evidence File Name	Name of evidence image file	
CoC Date/Time	Date of action (24HR)	MM/DD/YYYY HH:MM
CoC Action	Most commonly Evidence Transfer, Evidence Received, Evidence Return	
CoC Released By	Printed and signed name of person sending evidence	First and Last Name
CoC Received By	Printed and signed name of person receiving evidence	First and Last Name

Data Sources	Description
D	Desktop Computer System
L	Laptop Computer System
E	Email Data/Server (Includes POP email accounts)
M	Mobile Phone, Tablets, iPads, iPods, eReaders
N	Network Data, Group Shares, etc.
R	Removable Media/External Devices (USB, CD/DVD)
O	Other

SECTION VII – COMMON INFORMATION TECHNOLOGY RISK ASSESSMENT AREAS

Field name and definitions below provide guidance on the sample chain of custody form attached.

1. **Incident Response Plan (IRP)** – The incident response plan should outline the procedures and contacts for the response to a data security incident. The IRP should also be tested after being developed, and include topics such as evidence preservation and include groups such as Human Capital and Legal Department.
2. **Security Awareness Training Program** – Company employees should be provided training on identifying and reporting suspected incidents that compromise the integrity of the overall information security posture of the organization. Training should include the identification of phishing email and social engineering attacks that are common attack methods encountered by organizations.
3. **Internet Acceptable Use Policy** – Acceptable Use Policy that explicitly outlines the information collected of the employees (Internet Use Monitoring) and what is deemed "acceptable use" of company issued computer systems and usage of network resources for personal reasons.
4. **Digital Evidence Collection/Preservation** – Preservation and collection of electronic evidence should be incorporated into employee training and the Incident Response Plan.
5. **Policy and Procedures Surrounding Building Access** – Written policies and procedures should be established governing the access by employees, vendors and visitors, and to address the removal of physical assets.
6. **Identification and Logging of Vendors & Visitors** – Identification and record keeping of vendors and visitors visiting the company's facilities.
7. **Policy & Procedures Surrounding Removal of Physical Equipment** – Ensure that proper controls are in place to prevent electronic equipment from being physically removed from company facilities without proper documentation.
8. **Business Impact Analysis** – A business impact analysis should be performed to properly identify confidential or valuable information and systems and determine the level of risk that is acceptable to the organization in the event of an incident. This assessment should include financial, human capital, legal, and proprietary systems/information.
9. **Disaster Recovery Drills** – Bi-Annual table top disaster recovery drills should be performed with your Internet Service Provider and relevant vendors to ensure the Incident Response Plan (IRP) is current and adequately reflects the resources needed during an incident
10. **Password Complexity** – Complex passwords should be established for all network and application accounts. Passwords should be forced to change every 90 days or as deemed acceptable by the organization.
11. **Security Information & Event Management (SIEM)** – A SIEM should be established to gather network, VPN, and sensitive application logs. Periodic reviews of the logging and the establishment of alerts should be considered.
12. **Automated Script to Remove Memory Entries and Temporary Files** – Logon batch script to remove temporary and pagefile (memory) artifacts should be considered. Remnants of sensitive information and malware related files can be commonly found in these locations.



13. **Standard Desktop/Laptop Deployment** – IT should consider a standard deployment of desktop and laptop equipment to streamline help desk support and ensure business applications and programs can be supported uniformly across the enterprise.
14. **Guest Wireless Network** – The guest wireless network should be secured with WPA2 and protected with a password that should be changed periodically. The guest wireless should be segregated from access to the standard corporate network and resources. A legal disclaimer outlining the use of the guest network should also be established and displayed to the user prior to authentication.
15. **File Level Auditing** – File level audition of servers and applications should be established.
16. **Mobile Device** – Secure password and remote wiping policy should be considered for hand held and other mobile devices (i.e. Tablets) that connect to the network.
17. **Outlook Web Access (OWA)** – Access to web based email applications such as OWA, should be secured using the HTTPS protocol. Organization should also consider restricting the printing and downloading of email and attachments unless job requirements dictate the need for such access. Logging of OWA access should be retained for a period no less than 60 days or other time frame deemed appropriate by the organization.
18. **Internal Vulnerability Scan** – Internal scans of the company network should occur annually or following a significant change in network design.
19. **Full Disk Encryption** – Full disk encryption software should be standard for all laptop and desktop systems.
20. **Secure Email Transmission** – If needed, an application to transmit secure email messages should be considered to reduce the risk of inadvertent disclosure of sensitive data and to protect information from being compromised during transmission.
21. **Segregate Networks By Department/Data Classification** – Sub-networks or VLAN's should be considered as part of your network topology. Departments such as Legal, Human Capital, Finance, and network shares, for example, should be segregated from each other. This segregation improves the overall security posture of the organization and can help reduce the risk of data being compromised during an incident.
22. **Information Security Program** – A standardized corporate information security program should be established that includes the vision and strategy of the organization. Individuals responsible for audit, compliance, and operational managers should also be integrated into the program to ensure the confidentiality, integrity, and availability of your network and information.
23. **Policy & Procedure Review** – A review and update of your overall policies and procedures relating to IT Governance (also part of the Information Security Program), should be performed. Ensure these policies and procedures also reflect information such as version, date implemented, author, and objectives.

APPENDIX I – SAMPLE CHAIN OF CUSTODY FORM

NAVIGANT

Evidence Collection – Form 200

V.09042012

Matter Information					
Client / Matter Name:		Matter Code:			
Date/Time Received:		Time Zone:			
Received From:		Company Name:			
Address 1:		Address 2:			
City:		State:		Zip:	
Custodian System					
Custodian Name:		User ID:			
Manufacturer:		BIOS Date:		Time:	
Model:		Actual Date:		Time:	
Serial Number:		NCI Evidence ID:			
Custodian Media					
Manufacturer:		Capacity:			
Model:		Unique Label/ID:			
Serial Number:		NCI Evidence ID:			
Storage Device (Evidentiary)					
Manufacturer:		Model:			
Serial Number:		NCI Label:			
Storage Device (Working Copy / Backup)					
Manufacturer:		Model:			
Serial Number:		NCI Label:			
Collection Information					
Collected By:		Collection Method:			
Evidence File Name:		Verified? (Check one)	☐ YES	☐ NO	
Acquisition Hash:	☐ SHA1	☐ MD5			
Notes					

Chain of Custody

Date/Time	Action	Released By (Sign & Print)	Received By (Sign & Print)
	Received Evidence	SIGNATURE	SIGNATURE
		PRINTED NAME	PRINTED NAME
		SIGNATURE	SIGNATURE
		PRINTED NAME	PRINTED NAME
		SIGNATURE	SIGNATURE
		PRINTED NAME	PRINTED NAME

Examiner Required To Only Complete Applicable Fields.

LEGAL DISCLAIMER

The information contained herein is for informational purposes only and is provided "as-is", with no guarantees of completeness, timeliness, accuracy or of the results obtained from the use of such information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will Navigant Consulting, Inc., or Beazley, their affiliates, or employees, representatives or agents thereof be liable to you or anyone else for any decision made or action taken in reliance on the information contained herein or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Reliance on the information in this guide does not constitute a change in the coverage under your Policy. Claims will be adjudicated in accordance with the Policy terms and conditions.

The information contained herein is provided with the understanding that the authors and publishers are not herein engaged in rendering legal, information security, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional information security, accounting, tax, legal or other competent advisers. You should consult with your attorneys, information security professionals or other qualified advisors or representatives prior to implementing any information, procedures, tests, methodologies or information security solutions in connection with your information security considerations.

Organizations that have a security incident are encouraged to get legal guidance from qualified security incident response attorneys. Beazley policy holders that have a security incident are encouraged to notify Beazley at bbr.claims@beazley.com in order that Beazley can arrange expert legal and forensics services as provided under the Beazley policy.

The design, analysis, content and other material contained herein is the intellectual property of Beazley and Navigant and is made available only for use by Beazley policy holders. This Information Security Incident Response Guide, and anything contained herein, may not be copied, reproduced, distributed or displayed without the express written consent of Beazley and Navigant.

CONTACTS

DARIN BIELBY

Managing Director, Global Cyber Insurance Channel Leader
215.832.4485
dbielby@navigant.com

ROBERT E. ANDERSON

Managing Director, Global Information Security Practice Leader
202.481.7306
bob.anderson@navigant.com

LAURA NIELSEN

Director, PHI / PII Data Mapping Practice Leader
303.383.7334
lnielsen@navigant.com

REGIONAL FORENSIC INVESTIGATION LEADS

AMERICAS

JOHN BOLES

Director
+1.703.638.0823
john.boles@navigant.com

EMEA

JANO BERMUDES

Director
+44(0)2073983840
jano.bermudes@navigant.com

APAC

FRED CHAN

Director
+852.223.32500
fchan@navigant.com

If you have a data incident, notify Beazley at bbr.claims@beazley.com (U.S. policyholders) or at bbruk@beazley.com (UK policyholders) in accordance with your BBR policy. In other jurisdictions, please notify as provided in your policy.

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

beazley

NAVIGANT