Cyber Incident Response Plan (CIRP)
Team Scenario Overview

1.1 Background

The cyber threat landscape in the financial sector is constantly changing, with new threats surfacing every day.

The best practice hardening of defences at many larger financial institutions has pushed malicious actors to adapt and modify their targets and attack vectors. As a result, smaller organizations can and have been targeted – both for immediate financial gain, and as a means of access into larger organizations' infrastructure. Any institution that has public facing (or Internet facing) operations should consider itself at risk of a cyber breach.

It is therefore critical that all organizations – regardless of size – harden their cyber defences in proportion to the sensitivity of their information assets.

1.1.1 Objectives

This guide on cyber incident management has been designed for Buduchnist Credit Union Ltd. to enhance their preparedness to deal with a cyber incident. This document is not intended to constitute a cyber risk assessment for individual institutions.

1.1.2 Context

Cybersecurity incidents or events related to IT information systems can have a significant impact on the delivery of financial services. The ability to respond to cybersecurity incidents in a consistent, coordinated, and timely manner is essential.

This guide draws on cybersecurity principles from the publications listed below:

Standard Number	Title
ISO/IEC 27035:2011	Information technology – Security techniques – Information security incident management
ISO/IEC 27035-1	*Principles of Incident Management (Draft)*
ISO/IEC 27035-2	Guidelines to Plan And Prepare For Incident Response (Draft)
ISO/IEC 27035-3	Guidelines for Incident Response Operations
NIST Special Publication 800-61 Revision 2	Computer Security Incident Handling Guide
Government of Canada	Information Technology Incident Management Plan

2.1 An Overview of Cybersecurity Incident Management

Planning and preparing for a cybersecurity incident can be challenging for many organizations. When a cybersecurity incident occurs, an organization is required to take immediate action in order to mitigate threats to the confidentiality, integrity, and availability of its information assets. This requires effective deployment of resources and established communication strategies.

Targeted organizations face an uphill battle against cyber criminals who, given enough time and money, can breach the most sophisticated system defenses. Potential threat actors include insiders who act with malicious intent, trusted insiders whose acts cause damage by mistake, and attacks from cyber criminals.

Buduchnist Credit Union Ltd. should take reasonable measures to respond appropriately in the event of a cybersecurity incident. Poorly executed incident response has the potential to cause an organization significant financial loss, ruin its reputation, and perhaps even drive it out of business altogether.

Some of the primary objectives of cybersecurity incident management include the following:

- Avoid cybersecurity incidents before they occur
- Minimize the impact of cybersecurity incidents to the confidentiality, availability, or integrity of the investment industry's services, information assets, and operations
- Mitigate threats and vulnerabilities as cybersecurity incidents are occurring
- Improve cybersecurity incident coordination and management within the investment industry
- Reduce the direct and indirect costs caused by cybersecurity incidents
- Report findings to executive management

2.2 Key Terms

The definitions below are based on the International Standard for Information Security Incident Management (ISO/IEC 27035).

CYBERSECURITY EVENT
An identified occurrence of a system, service, or network state, indicating a possible breach of information security, failure of controls, or a previously unknown situation that may be security relevant.

CYBERSECURITY INCIDENT
A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

CYBERSECURITY INCIDENT MANAGEMENT
The processes for detecting, reporting, assessing, responding to, dealing with, and learning from cybersecurity incidents.

INCIDENT RESPONSE
The actions taken to protect and restore the normal operational conditions of an information system, and the information stored in it, when a cybersecurity incident occurs.

CYBER INCIDENT RESPONSE TEAM (CIRT)
A team of appropriately skilled and trusted members of the organization that handles incidents during their lifecycle.

2.3 The Cybersecurity Incident Chain

The steps in the ISO 27035 Cybersecurity Incident Chain.

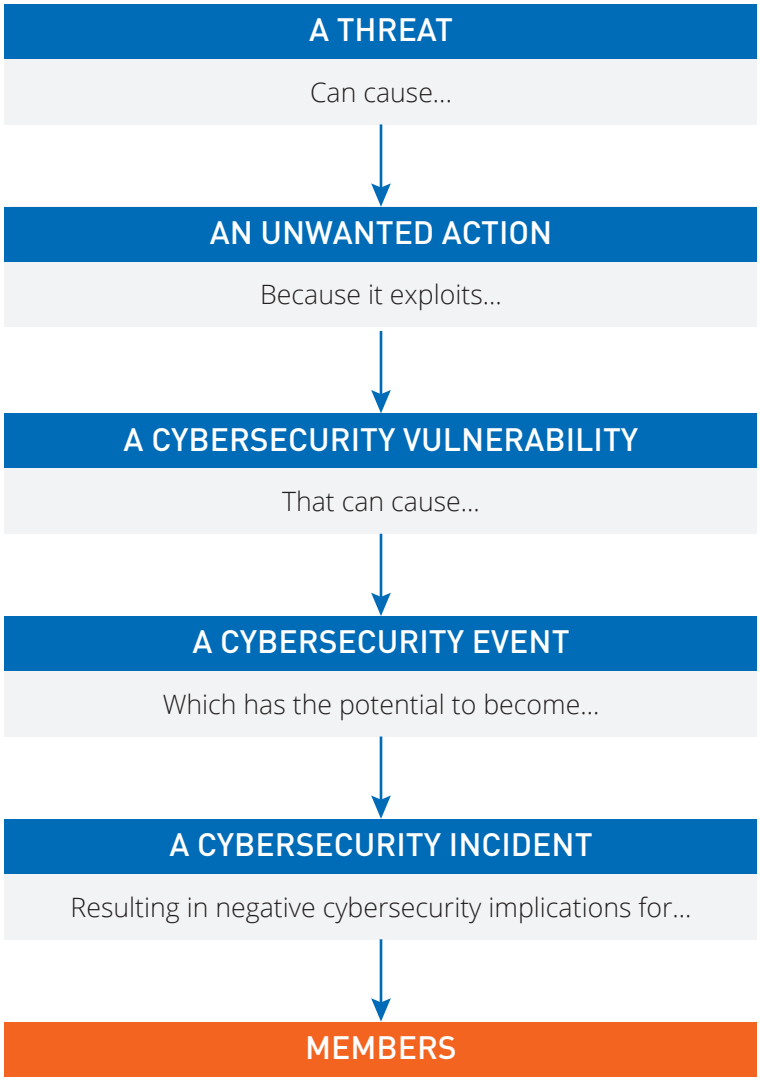
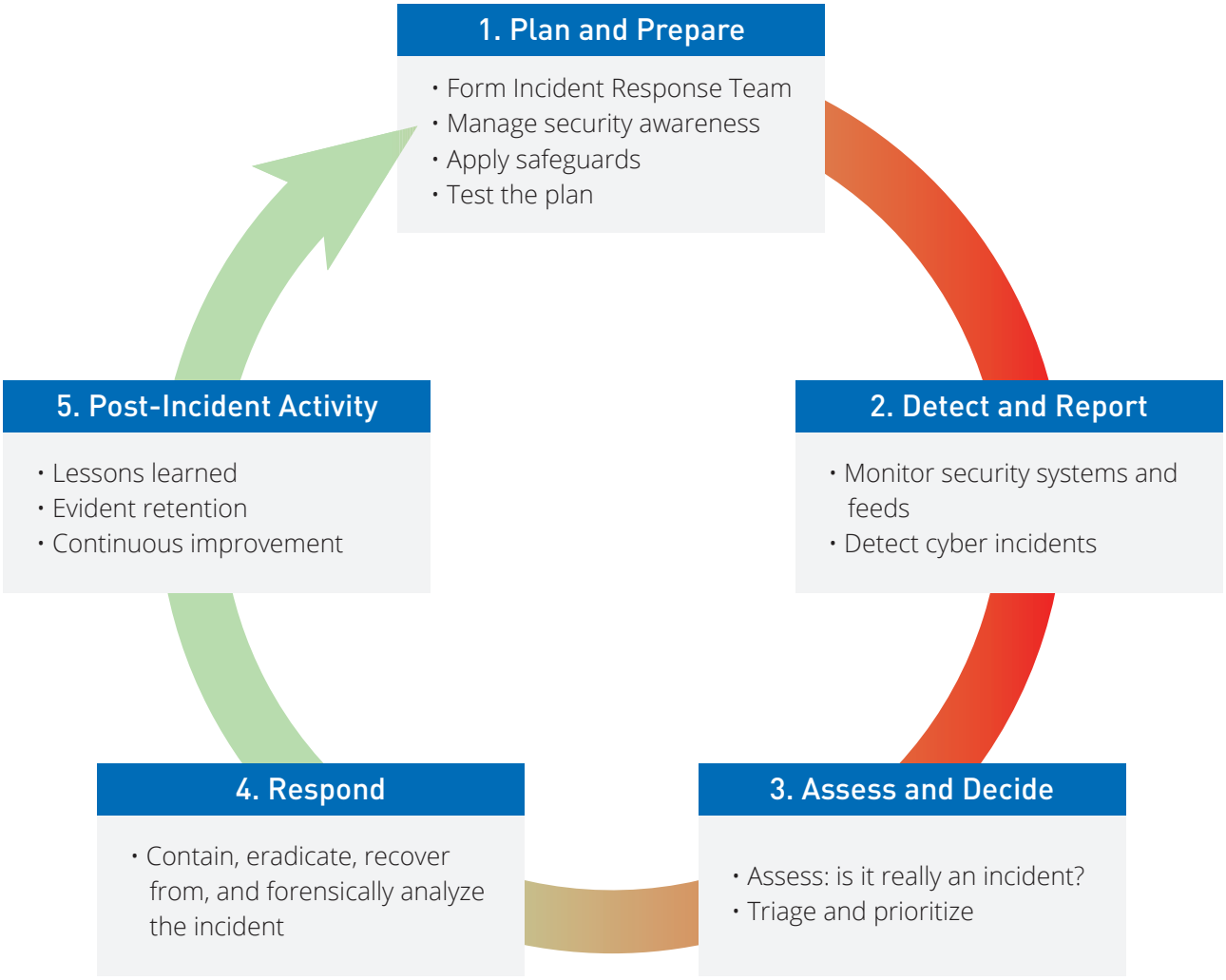


Diagram adapted from ISO/IEC 27035: Information Technology - Information Security Incident Management

2.4 Five Phases of Cybersecurity Incident Management

The five phases of cybersecurity incident management.



CIRP Team Identification

Incident Response Manager | *Taras Pitt*
Central point of all communication. Securing communication to those on a valid need-to-know. Oversees and prioritizes actions during detection, analysis and containment of an incident. Convey special requirements of high severity incidents to the rest of the company. Provision resources, funding, staff and time commitment for incident response planning and execution.

Security Analyst | *Oleh Goy*
Research the time, location and detail of the incident; collecting meaningful metrics such as type, severity, attack vector, impact and root cause for future remediation purposes. Alert IT team on actions required. Filter out false positives and watch for potential intrusions. Threat Researching.

Internal Operations | *Yuriy Horich*
Called when requirements come up for internal logistics operations need to be actioned and/or communicated to staff.

Human Resources | *Andrea Kuzmyn*
Called when employee is involved with an incident.

Privacy Officer / Risk Management | *Bohdan Cup / Tom Wilson*
Develop Threat Matrix and vulnerability assessments and encourage best practices across the organization.

Public Relations | *Ivanna Purkiss*
Communicate with team leaders, ensuring an accurate account of any issues is communicated to stakeholders and press.

Legal Council | *Adrian Bilyk*
Ensure evidence collected maintains forensic value if the company must pursue legal action. Provide advice regarding liability issues if an incident affects customers, vendors and/or general public.

External Forensics | *Synchroworks Consulting*
Recover key artefacts and maintain integrity of evidence to ensure forensically sound investigation.

CIRP Security Threat Identification/Scenarios

Network Type Threats

Denial-of-Service (DoS) / Distributed Denial-of-Service (DDoS)

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike attacks that are designed to enable the attacker to gain or increase access, denial-of-service doesn't provide direct benefits for attackers. For some of them, it's enough to have the satisfaction of service denial. However, if the attacked resource belongs to a business competitor, then the benefit to the attacker may be real enough. Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched. One common example is session hijacking, which I'll describe later.

There are different types of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.

Session Hijacking and Man-in-the-Middle Attacks

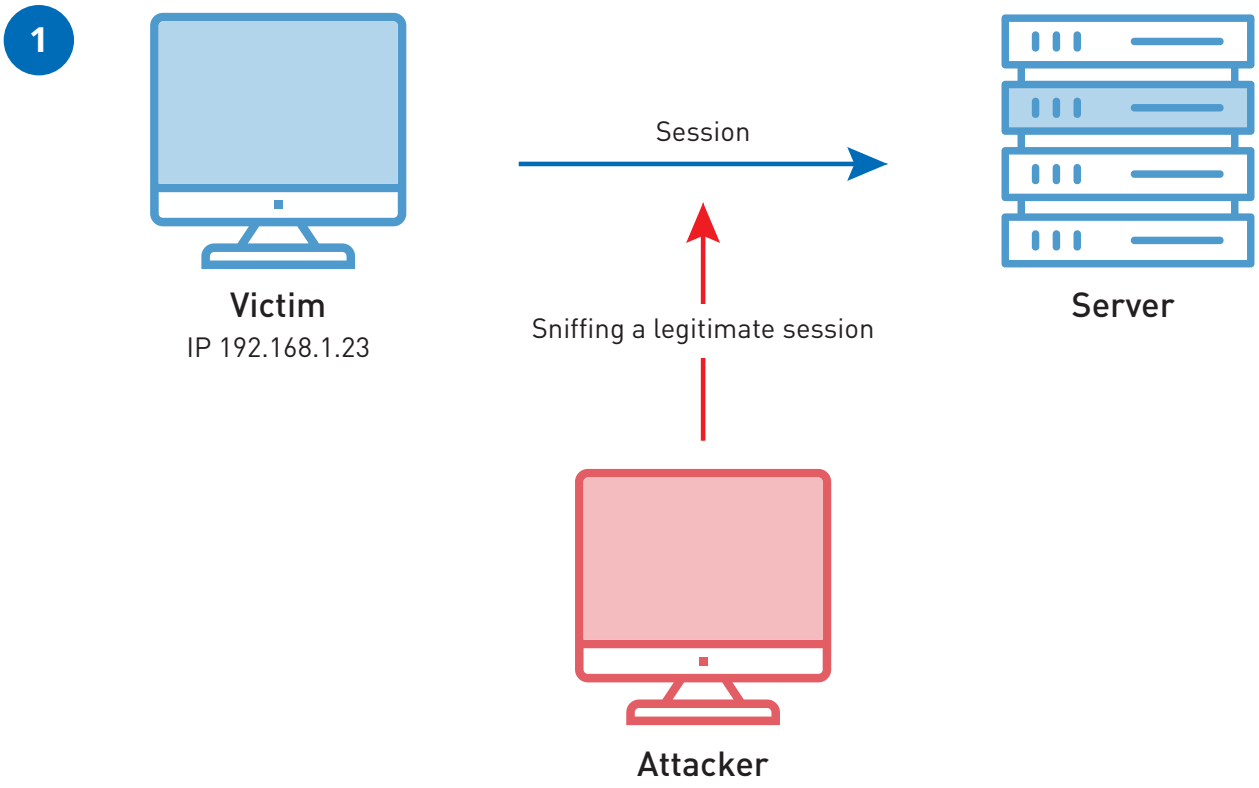
A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

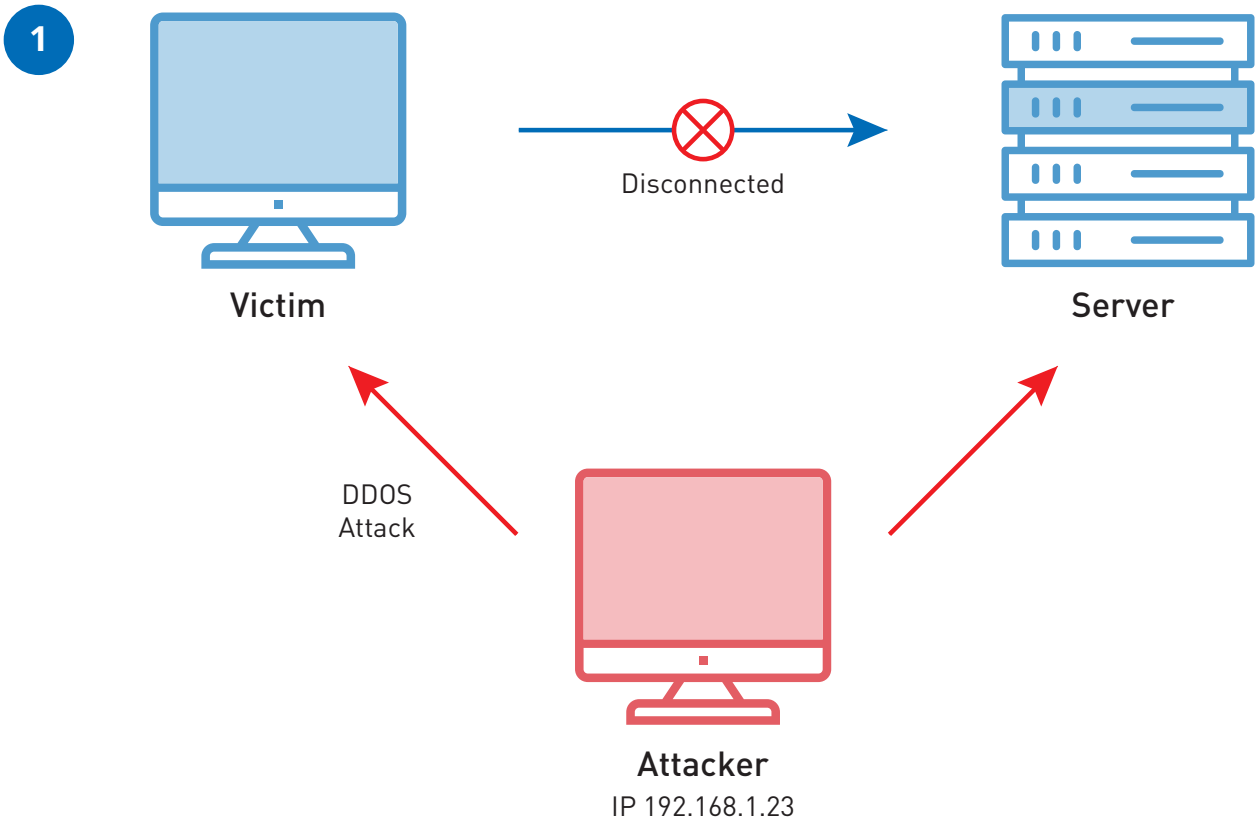
Session Hijacking

In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. For instance, the attack might unfold like this:

1. A client connects to a server.
2. The attacker's computer gains control of the client.
3. The attacker's computer disconnects the client from the server.
4. The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
5. The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

* See diagram on page 7 for more information.


1
Victim
IP 192.168.1.23
Session
Server
Sniffing a legitimate session
Attacker


1
Victim
Disconnected
Server
DDOS
Attack
Attacker
IP 192.168.1.23

Replay

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This type can be easily countered with session timestamps or nonce (a random number or a string that changes with time).

Currently, there is no single technology or configuration to prevent all MitM attacks. Generally, encryption and digital certificates provide an effective safeguard against MitM attacks, assuring both the confidentiality and integrity of communications. But a man-in-the-middle attack can be injected into the middle of communications in such a way that encryption will not help — for example, attacker "A" intercepts public key of person "P" and substitute it with his own public key. Then, anyone wanting to send an encrypted message to P using P's public key is unknowingly using A's public key. Therefore, A can read the message intended for P and then send the message to P, encrypted in P's real public key, and P will never notice that the message was compromised. In addition, A could also modify the message before resending it to P. As you can see, P is using encryption and thinks that his information is protected but it is not, because of the MitM attack.

So, how can you make sure that P's public key belongs to P and not to A? Certificate authorities and hash functions were created to solve this problem. When person 2 (P2) wants to send a message to P, and P wants to be sure that A will not read or modify the message and that the message actually came from P2, the following method must be used:

1. P2 creates a symmetric key and encrypts it with P's public key.
2. P2 sends the encrypted symmetric key to P.
3. P2 computes a hash function of the message and digitally signs it.
4. P2 encrypts his message and the message's signed hash using the symmetric key and sends the entire thing to P.
5. P is able to receive the symmetric key from P2 because only he has the private key to decrypt the encryption.
6. P, and only P, can decrypt the symmetrically encrypted message and signed hash because he has the symmetric key.
7. He is able to verify that the message has not been altered because he can compute the hash of received message and compare it with digitally signed one.
8. P is also able to prove to himself that P2 was the sender because only P2 can sign the hash so that it is verified with P2 public key.

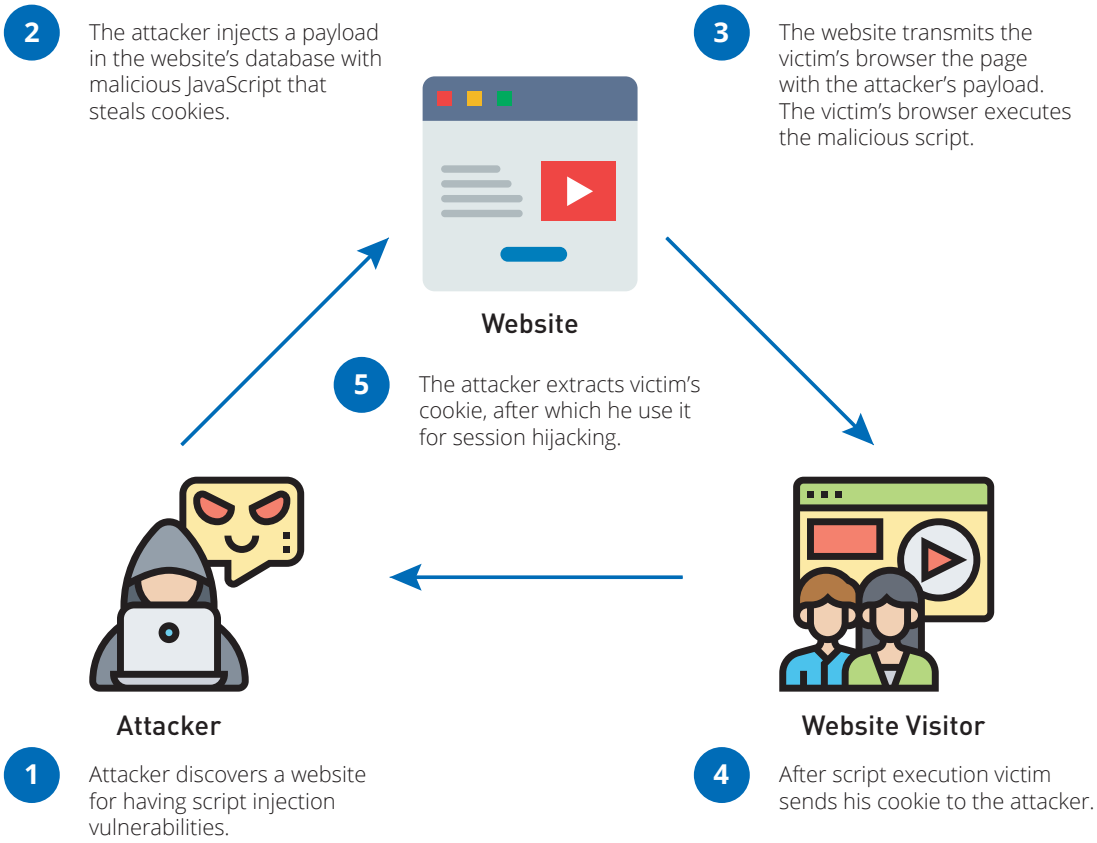
Drive-by Attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.

To protect yourself from drive-by attacks, you need to keep your browsers and operating systems up to date and avoid websites that might contain malicious code. Stick to the sites you normally use — although keep in mind that even these sites can be hacked. Don't keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are that can be exploited by drive-by attacks.

Cross-Site Scripting (XSS)

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. For example, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities can enable an attacker to not only steal cookies, but also log keystrokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.



While XSS can be taken advantage of within VBScript, ActiveX and Flash, the most widely abused is JavaScript — primarily because JavaScript is supported widely on the web.

To defend against XSS attacks, developers can sanitize data input by users in an HTTP request before reflecting it back. Make sure all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches. Convert special characters such as ?, &, /, <, > and spaces to their respective HTML or URL encoded equivalents. Give users the option to disable client-side scripts.

SQL Injection Attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

For example, a web form on a website might request a user's account name and then send it to the database in order to pull up the associated account information using dynamic SQL like this:

"SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"

While this works for users who are properly entering their account number, it leaves a hole for attackers. For example, if someone decided to provide an account number of "' or '1' = '1'", that would result in a query string of:

"SELECT * FROM users WHERE account = '' or '1' = '1';"

Because '1' = '1' always evaluates to TRUE, the database will return the data for all users instead of just a single user.

The vulnerability to this type of cyber security attack depends on the fact that SQL makes no real distinction between the control and data planes. Therefore, SQL injections work mostly if a website uses dynamic SQL. Additionally, SQL injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. J2EE and ASP.NET applications are less likely to have easily exploited SQL injections because of the nature of the programmatic interfaces available.

In order to protect yourself from a SQL injection attacks, apply least0privilege model of permissions in your databases. Stick to stored procedures (make sure that these procedures don't include any dynamic SQL) and prepared statements (parameterized queries). The code that is executed against the database must be strong enough to prevent injection attacks. In addition, validate input data against a white list at the application level.

Malware

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware:

- *Macro viruses* — These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
- *File infectors* — File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.
- *System or boot-record infectors* — A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.

- *Polymorphic viruses* — These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.
- *Stealth viruses* — Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
- *Trojans* — A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.
- *Logic bombs* — A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- *Worms* — Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.
- *Droppers* — A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- *Ransomware* — Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.
- *Adware* — Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.
- *Spyware* — Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

Password Attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

- Brute-force password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.
- In a dictionary attack, a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results. ansomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

DNS Tunnelling

DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. However, there are also malicious reasons to use DNS Tunneling VPN services. They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker's infrastructure. It can also be used for command and control callbacks from the attacker's infrastructure to a compromised system.

Brute-Force and Dictionary Network Attacks

Dictionary and brute-force attacks are networking attacks whereby the attacker attempts to log into a user's account by systematically checking and trying all possible passwords until finding the correct one.

The simplest method to attack is through the front door since you must have a way of logging in. If you have the required credentials, you can gain entry as a regular user without creating suspicious logs, needing an unpatched entry, or tripping IDS signatures. If you have a system's credentials, your life is even simplified since attackers don't have these luxuries.

The term brute-force means overpowering the system through repetition. When hacking passwords, brute force requires dictionary software that combines dictionary words with thousands of different variations. It is a slower and less glamorous process. These attacks start with simple letters such as "a" and then move to full words such as "snoop," or "snoopy."

Brute-force dictionary attacks can make 100 to 1000 attempts per minute. After several hours or days, brute-force attacks can eventually crack any password. Brute force attacks reiterate the importance of password best practices, especially on critical resources such as network switches, routers and servers.

CIRP Security Threat Identification/Scenarios

Peripheral Type Threats

Software/Firmware Vulnerabilities

Firmware is the essence of your hardware. It's basic software that's embedded into every piece of hardware within your machine. Essentially, its function is to communicate with the software you install on the computer and ensure the hardware executes the software's commands correctly. It's only compatible with the make and model of the computer it's installed on, and it can usually be rewritten, removed, or uninstalled.

Firmware poses a huge risk to your organization because firmware producers usually don't design their firmware with security in mind.

Firmware malware will exploit this lack of security by attaching their code to the firmware's code. Since the firmware isn't secured by a cryptographic signature, it won't detect the infiltration, and the malware will be hidden within the firmware code.

Once the firmware is in, it can be used for several purposes such as spying on your activity, exfiltrating your data, and remote control of your hardware.

Unauthorized/unwanted software/computer/device on the network

Network growth and complexity is skyrocketing. Before the explosion of IP-connected devices, networks typically grew with the number of connected users. However, now networks must scale three to five times for each employee based on the number of IP devices we use to do our work. This means the challenge of managing and securing endpoints has also become much more difficult.

When you consider all of the IP-connected devices on your network—PCs and laptops, VOIP phones and "bring your own device" (BYOD) netbooks, tablets, smartphones and more—how many do you think you have? It's a fundamental question that needs to be answered. Without any indication, you can't adequately plan for capacity or manage the network to maximum efficiency. But there is also a deeper implication to this question. Often lurking out there are rogue devices that have the potential to cause harm to your network. The larger your network, the greater the potential risk. All it takes is one rogue device to wreak havoc

CIRP Security Threat Identification/Scenarios

Workstation/Server Threats

Employee negligence/threat.
Not every network attack is performed by someone outside an organization.

Inside attacks are malicious attacks performed on a computer system or network by an individual authorized to access the system. Insiders that carry out these attacks have the edge over external attackers since they have authorized system access. They may also understand the system policies and network architecture. Furthermore, there is less security against insider attacks since most organizations focus on defending against external attacks.

Insider threats can affect all elements of computer security and range from injecting Trojan viruses to stealing sensitive data from a network or system. The attackers may also affect the system availability by overloading the network or computer processing capacity or computer storage, resulting in system crashes.

End-user exploitation: spearphishing/phishing/vishing/smishing.
Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the “From” section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

A whale phishing attack is a type of phishing that centers on high-profile employees such as the CFO or CEO. It is aimed at stealing vital information since those holding higher positions in a company have unlimited access to sensitive information. Most whaling instances manipulate the victim into permitting high-worth wire transfers to the attacker.

The term whaling signifies the size of the attack, and whales are targeted depending on their position within the organization. Since they are highly targeted, whaling attacks are more difficult to notice compared to the standard phishing attacks.

In a business, system security administrators can lessen the effectiveness of such a hack by encouraging the corporate management staff to attend security awareness training.

To reduce the risk of being phished, you can use these techniques:

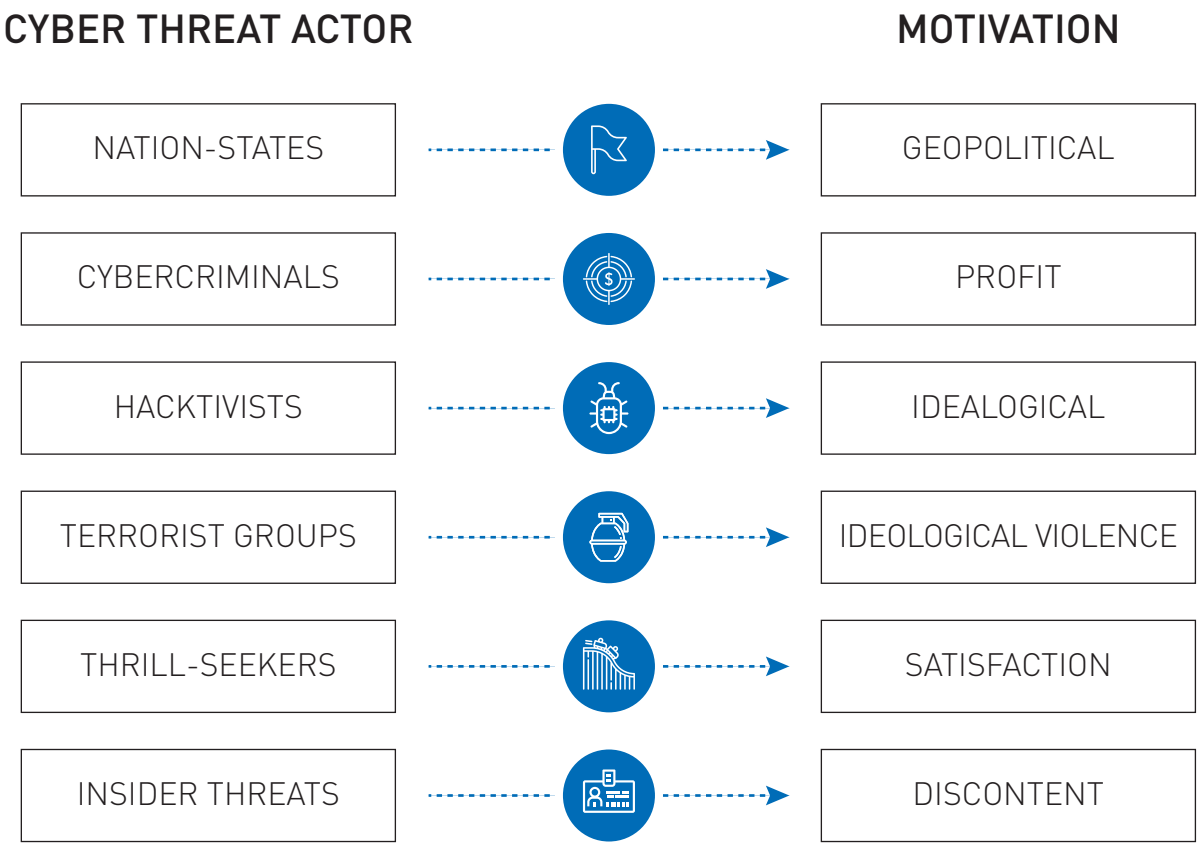
- *Critical thinking*
  Do not accept that an email is the real deal just because you're busy or stressed or you have 150 other unread messages in your inbox. Stop for a minute and analyze the email.
- *Hovering over the links*
  Move your mouse over the link, but do not click it! Just let your mouse cursor h over over the link and see where would actually take you. Apply critical thinking to decipher the URL.
- *Analyzing email headers*
  Email headers define how an email got to your address. The "Reply-to" and "Return-Path" parameters should lead to the same domain as is stated in the email.
- *Sandboxing*
  You can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

CIRP Threat Actors

Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.

Motivations

Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation.



CIRP Tabletop Exercises

Tabletop exercises are meant to help the organization consider different risk scenarios and prepare for potential cyber threats. All the exercises featured in this document can be completed in as little as 15 minutes, making them a convenient tool.

Each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

Tips and tricks

- Designate a single individual to facilitate the exercise.
- Break the scenario into meaningful learning points.
- Read the scenario aloud to the group and ensure their understanding.
- Facilitate a conversation about how your organization would handle the scenario, focusing on key learning points as you discuss.
- Include applicable members of other business units.
- Be sure to follow up on any gaps identified during the exercise.

CIRP Tabletop Exercises

Exercise 1 | The Quick Fix

Scenario:
Joe, your network administrator, is overworked and underpaid. His bags are packed and ready for a family vacation to Disney World when he is tasked with deploying a critical patch. In order to make his flight, Joe quickly builds an installation file for the patch and deploys it before leaving for his trip. Next, Sue, the on-call service desk technician, begins receiving calls that nobody can log in. It turns out that no testing was done for the recently installed critical patch.

What is your response?

Discussion questions

- What is Sue's response in this scenario?
  - Does your on-call technician have the expertise to handle this incident? If not, are there defined escalation processes?
- Does your organization have a formal change control policy?
  - Are your employees trained on proper change control?
- Does your organization have disciplinary procedures in place for when an employee fails to follow established policies?
- Does your organization have the ability to "roll back" patches in the event of unanticipated negative impacts?

Processes tested: Patch management

Threat actor: Insider

Asset impacted: Internal network

CIRP Tabletop Exercises

Exercise 2 | A Malware Infection

Scenario:
An employee within your organization used the company's digital camera for business purposes. In the course of doing so, they took a scenic photograph that they then loaded onto their personal computer by inserting the SD card. The SD card was infected with malware while connected to the employee's personal computer. When re-inserted into a company machine, it infected the organization's system with the same malware.

What is your response?

Discussion questions

- Who within the organization would you need to notify?
- How would your organization identify and respond to malware infecting your system through this vector?
  - What is the process for identifying the infection vector?
- What other devices could present similar threats?
- What should management do?
- How can you prevent this from occurring again?
  - Does your organization have training and policies in place to prevent this?
  - Do policies apply to all storage devices?

Processes tested: Detection ability/User awareness

Threat actor: Accidental insider

Asset impacted: Network integrity

CIRP Tabletop Exercises

Exercise 3 | The Unplanned Attack

Scenario:
A hacktivist group threatens to target your organization following an incident involving an allegation of use of excessive force by law enforcement. You do not know the nature of the attack they are planning. How can you improve your posture to best protect your organization?

What is your response?

Discussion questions

- What are the potential threat vectors?
- Have you considered which attack vectors have been most common over the past month?
  - Are there other methods you can use to prioritize threats?
- Have you checked your patch management status?
- Can you increase monitoring of your IDS and IPS?
  - If you don't have the resources to do so, is there another organization that could be called upon to assist?
- What organizations or companies could assist you with analyzing any malware that is identified?
- How do you alert your help desk?
- Do you have a way of notifying the entire organization of the current threat (bulletin board, etc.)?
- Does your Incident Response Plan account for these types of situations?

Processes tested: Preparation

Threat actor: Hacktivist

Asset impacted: Unknown

CIRP Tabletop Exercises

Exercise 4 | The Cloud Compromise

Scenario:
One of your organization's internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive. You have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data stored in the cloud provider's infrastructure may have been compromised.

What is your response?

Discussion questions

- Does your organization have current polices that consider 3rd party cloud storage?
- Should your organization still be held accountable for the data breach?
- What actions and procedures would be different if this was a data breach on your own local area network?
- What should management do?
- What, if anything, do you tell your constituentsHave you considered which attack vectors have been most common over the past month?
    - How/when would you notify them?

Processes tested:Incident response

Threat actor: External threat

Asset impacted: Cloud

CIRP Tabletop Exercises

Exercise 5 | Financial Break-in

Scenario:
A routine financial audit reveals that several people receiving paychecks are not, and have never been, on payroll. A system review indicates they were added to the payroll approximately one month prior, at the same time, via a computer in the financial department.

What is your response?
INJECT: You confirm the computer in the payroll department was used to make the additions. Approximately two weeks prior to the addition of the new personnel, there was a physical break-in to the finance department in which several laptops without sensitive data were taken.

OPTIONAL INJECT: Further review indicates that all employees are paying a new "fee" of $20 each paycheck and that money is being siphoned to an off-shore bank account.

Having this additional information, how do you proceed?

Discussion questions

- What actions could you take after the initial break in?
- Do you have the capability to audit your physical security system?
- Who would/should be notified?
- Would you able to assess the damages associated from the break in?
- Would you be able to find out what credentials may have been stored on the laptop?
- How would you notify your employees of the incident?
- How do you contain the incident?
    - Optional Inject question: How do you compensate the employees?

Processes tested: Incident response

Threat actor: External threat

Asset impacted: HR/Financial data

CIRP Tabletop Exercises

Exercise 6 | The Flood Zone

Scenario:
Your organization is located within a flood zone. Winter weather combined with warming temperatures has caused flooding throughout the area. Local authorities have declared a state of emergency. In the midst of managing the flooding, a ransomware attack occurs on your facility, making computer systems inoperable.

What is your response?

Discussion questions

- Do you have a COOP (Continuity of Operations Plan) or DRP (Disaster Recovery Plan)?
  - If so, do you carry out an annual simulation to ensure the COOP or DRP is sufficient and running smoothly?
- Do you have an Incident Response Plan (IRP) that specifically details ransomware steps?
  - What steps will you take if restoring from backup is not an option?
  - Does your IRP only take into account the financial implications of a cybersecurity incident, or does it consider the severity of the situation as well?
  - Do you have a plan in place for how to acquire bitcoin?
  - Have you considered that a targeted ransomware attack may require more bitcoin than is easily accessible on the market?
- Do you have a backup for completing Emergency Operations Center (EOC)? processes without a computer system?
  - Can you route emergency communications/processes through a neighboring entity?
- Who do you need to notify, and how will you do so?
  - Consider that increased phone traffic may be congesting the lines.

Processes tested: Emergency response

Threat actor: External threat

Asset impacted: Emergency Operations Center Processes

Incident Response Plan Annual Checklist

This checklist is used internally by IT staff to evaluate the readiness and accurateness of our Cyber Incident Response Plan. This checklist is part of a larger set of internal strategies, guidelines, policies, and procedures that are meant to help respond efficiently to an incident.

Plan Element	In Place	Needs Attention
Our plan is in place and was reviewed and updated as appropriate within the last year.		
Our plan was tested within the past year via a realistic simulation or an actual significant incident.		
Our plan involves, and clearly delineates roles and responsibilities for, all relevant stakeholders in the organization, such as IT, legal, communications, operations, and senior management.		
Our plan contains clearly defined severity ratings and triggers for escalation to legal and senior management.		
Our plan contains 24/7/365 contact information for all incident response team members and their backups.		
Our organization requires workforce members to report suspicious emails and other potential cybersecurity incidents.		
Our plan establishes how our organization handles reports of potential cybersecurity incidents, regardless of types and source.		
Our plan includes a summary of the key cybersecurity regulatory requirements for each jurisdiction in which our organization operates.		
Our plan provides guidance for how our organization plans to interact with law enforcement and other governmental authorities in the event of an incident.		
Our plan includes information on key vendors of identity theft protection and related services, so that we can quickly mobilize to provide such services if needed.		
Our plan includes information on key vendors of forensics and other technology services our organization may need in the event of an incident.		
Our plan includes information on outside counsel we will involve in the event of an incident.		
Our plan coordinates with our organization's business continuity plan, so that any operational disruption potentially caused by a cybersecurity incident is addressed consistently with our plan.		
Our plan calls for post-incident debriefings and analyses to be applied to improve our organization's posture and plan.		

Incident Response Plan - Before an Incident Checklist

This checklist contains processes and procedures that are used internally by IT staff after an incident or breach. This list is meant to be reviewed quarterly.

Plan Element	In Place	Needs Attention
Create a prioritized list of information assets critical to the functioning of your organization.		
Identify the stakeholders responsible for each critical asset.		
Create an Incident Response Team (including individuals from legal, corporate communications, and HR) that will be responsible for all incidents.		
Ensure proper monitoring and tracking technologies are in place (such as firewalls, IPS, and anti-virus software) to protect your organization's information assets.		
Provide media training to the proper individual(s).		
Provide a company-wide process for employees, contractors, and third parties to report suspicious or suspected breach activities.		
Provide company-wide training on breach awareness, employee responsibility, and reporting processes.		

Incident Response Plan - During an Incident Checklist

This checklist contains processes and procedures that are used internally by IT staff during an incident or breach. This list is meant to be reviewed quarterly.

Plan Element	In Place	Needs Attention
Record the issues and open an incident report.		
Convene the Incident Response Team.		
Convene a teleconference with the appropriate internal stakeholders to discuss what must be done in order to restore operations.		
Convene a management teleconference with the appropriate internal stakeholders in order to provide situational awareness to executive management.		
Triage the current issues and communicate to executive management.		
Identify the initial cause of the incident, and activate the specialists to respond to the current issues to restore operations.		
Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action.		
Communicate to affected third parties, regulators, and media (if appropriate).		

Incident Response Plan - After an Incident Checklist

This checklist contains processes and procedures that are used internally by IT staff after an incident or breach. This list is meant to be reviewed quarterly.

Plan Element	In Place	Needs Attention
Update the incident report and review exactly what happened and at what times.		
Review how well the staff and management performed during the incident.		
Determine whether or not the documented procedures were followed.		
Discuss any changes in process or technology required to mitigate future incidents.		
Determine what information was needed sooner.		
Discuss whether any steps or actions taken might have inhibited the recovery.		
Determine which additional tools or resources are needed to detect, triage, analyze, and mitigate future incidents.		
Discuss what reporting requirements are needed (such as regulatory and customer).		
If possible, quantify the financial loss caused by the breach.		

Incident Response Plan - Report Template

The following is a sample incident report. The report is an example of the types of information and incident details that will be used to track and report security incidents for our organization.

Contact Information and Incident			
Last Name		First Name	
Job Title			
Phone		Alt Phone	
Mobile			
Email			

Incident General Information					
Incident #		Source of Incident	☐ External ☐ Internal	Type of Incident	
Date/Time of Incident Occurred			Date/Time of Incident Detected		
Site			Severity Level		
Impact Category			Confidential/Personal Identifiable Information Affected?		☐ Yes ☐ No
Systems and Services Impacted					

Incident Summary
Comments

Incident Mitigation

Comments

Recommendation

Comments *(Follow-on actions recommended to be taken, if any.)*

Additional Comments/Notes

Comments *(Any additional notes, information or observations related to the security incident or this report.)*