SINGAPORE POLYTECHNIC | SP

SCHOOL OF COMPUTING

DIPLOMA IN INFOCOMM SECURITY MANAGEMENT

ST2610 SECURITY POLICY AND INCIDENT MANAGEMENT

ASSIGNMENT 2 (INCIDENT RESPONSE PLAN)

Class: DISM/FT/2A/23

Student Number	Full Name
2123222	Urias Francis Paul John Bato
2123602	Shushant Shashwat
2107095	Md Amirul Adeeb
2123392	Marcus Wong Yu Xuan

Table of Contents

1. Overview

1.1 Events and Incidents

An event can be defined as any observable occurrence or activity that may indicate a potential security incident. Events can be generated by various sources such as security systems, logs, and network traffic. Events can either have a negative outcome or not.

A computer security incident refers to any event that violates or threatens to violate the security of an organization that jeopardizes the confidentiality, integrity, or availability of computer systems, networks, or data. Examples of incidents are:

- Attempts to obtain the organization’s sensitive data by gaining unauthorized access
- An organization may experience a malware infection if an employee inadvertently downloads or opens a malicious file
- Denial-of-service attack on the organization’s information
- Loss of protected data from insider threats

1.2 Incident Priority

		Impact		
		High Business Unit, Department, Location	Medium Multiple Users	Low Single User
Urgency	High Primary work functions can no longer be performed	1	2	3
	Medium Work functions impaired	2	3	4
	Low Inconvenient	3	4	5

Priority	Description	Target Resolution Time
1 (Critical)	Incidents that cause significant harm to an organization's operations can lead to the shutdown of critical business processes, compromising sensitive information and impacting users. These incidents have the potential to be disastrous for the organization. Examples: - System-wide outages - Network-wide outages - Data breaches - Cybersecurity attacks	1 hour
2 (High)	Incidents in which operations are severely impacted can disrupt the ability to conduct business effectively and reduce the productivity of a significant majority of users. Examples: - Network outages - System failures - Critical IT Asset is lost or not working	8 hours
3 (Medium)	Incidents that are less severe and may not require an immediate response. These incidents may still cause some disruption or inconvenience to the organization. Examples: - Software and Hardware errors affecting some devices - Slower performance in devices and network	24 hours
4 (Low)	Incidents that are the least severe and typically do not require an immediate response from the incident response team. These incidents may not have any significant impact on the organization's operations or assets.	48 hours

	Examples: - Minor software glitches - Printer malfunctions	
5 (Planning)	Incidents are mostly informational. These incidents may be notifications about potential security threats or alerts about system vulnerabilities. Examples: - security bulletins system updates - notifications about new software releases. - Password reset for a user	1 week

2. Purpose and Scope of Report

The purpose of the Incident Response Plan (IRP) is to equip organizations with the ability to respond promptly and appropriately to information security incidents while ensuring compliance with relevant regulations. This is to effectively reduce the impact of the incident and minimize a loss on the organization's assets and reputation, allowing business services to be restored as soon as possible.

The scope of this IRP encompasses any individual or entity designated by the organization to handle information security incidents occurring within the organizational premises, particularly those affecting the sensitive information stored in the servers.

3. Roles and Responsibilities

Computer Security Incident Response Team (CSIRT)

The computer security incident response team (CSIRT) is the most important in the incident response process. This team is a group of professionals responsible for preventing and responding to security incidents. This team is responsible for responding to cybersecurity incidents, including the identification, containment, and resolution of the incident. This team is typically made up of security personnel, IT personnel, and other experts as needed.

Project Officer (PO)

The project officer (PO) is the first point of contact for any person reporting a possible incident occurring within the SPIM Consulting and Monitoring premise. The PO is required to maintain an understanding of the Security Policies and Incident Response Plan (IRP) defined within the SPIM Consulting and Monitoring premise and must review the IRP periodically with expert advice from the technical IT team to make sure the IRP is relevant in achieving its goal to protect SPIM Consulting and Monitoring Pte Ltd during an incident. The PO is to ensure their contact information is made known to everyone and remain contactable and reachable to respond to incoming incidents as soon as possible.

Incident Response Manager (IRM)

Throughout the incident, the incident manager has total control and authority. All aspects of the incident response effort are coordinated and supervised by them. Until they assign that function to someone else, the incident manager, as a general rule, oversees all duties and responsibilities. The IRM will report to the CSO when the incident severity level reaches high or critical and will help exchange information between the PO, CSIRT team and the CSO.

Chief Information Officer (CIO)

The chief information officer (CIO) will work with the Project Officer (PO) to ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed. The CIO must ensure that CSIRT members are given the necessary authority to conduct investigations and stop activities that can aid in minimizing SPIM's loss during an incident.

Chief Security Officer (CSO)

The CSO is responsible for the overall security strategy and direction of an organization. The CSO is responsible for developing and implementing security policies and procedures, managing security risks and threats, and ensuring that the organization's assets are protected. The CSO is also responsible for managing the CSIRT team and ensuring that they have the necessary resources to carry out their responsibilities when the severity level reaches high or critical. The CSO will also have to ensure the incident is completely contained within a certain timeframe and report to the CIO.

Security Operations Center (SOC) Team

The SOC team is the main team involved in the detection phase of the incident response plan. This team is responsible for monitoring security systems and identifying potential security incidents. If the SOC team finds something suspicious like strange network traffic or unexpected changes, they can escalate the situation to other teams, such as the technical IT team to double check, or the incident response team if the situation requires urgency.

Technical IT Team

The technical team specialises in the technical aspects of incident response, such as the investigation and analysis of the incident, the identification of the cause, and the implementation of measures to contain the incident. Additionally, they are the team that are highly involved with the implementation of the preparation stage of the incident response plan; they are the team that can configure the security measures of the systems and network implementation of the security controls.

Communications Team

The communications team is very important in the incident response process. This team is responsible for coordinating communication both internally and externally during an incident. This includes keeping key stakeholders informed of the status of the incident and ensuring timely and accurate information is shared.

Forensics Team

The forensics team is the team responsible for conducting forensic investigations and collecting evidence related to the incident. This team helps to identify the root cause of the incident and tries to find who the attacker is using the evidence.

Business Continuity (BC) Team

The BC team is responsible for ensuring that critical business operations continue during and after the incident. The BC team is also involved in developing and implementing a Business Continuity Plan (BCP) that outlines steps for maintaining or restoring critical business processes, such as data backup and recovery procedures, alternative site arrangements, and communication plans. This team aims to ensure that organizations can quickly resume normal business operation to minimize the financial and reputational impact of an incident.

Legal Team

The legal team is responsible for ensuring that the incident response plan is compliant with legal and regulatory requirements and for providing advice on legal issues arising from the incident. This means that this team aims to protect the organization and its employees by making sure that the organisation’s systems and services adhere to the laws and regulations of the industry.

5. Incident Response Workflow (Citrix Vulnerability)

5.1 Preparation

The preparation phase in the incident response workflow is one of the most important steps. This is the step that aims to prevent incidents by ensuring that the systems, networks, and applications of the organisation are sufficiently secure in advance. To do this, we must identify which parts of the organisation are critical or are vulnerable to threats. In the case of the Citrix vulnerability, we need to ensure that all the systems are updated with the latest security patches and have proper security controls in place. For example, NOTROBIN is a backdoor trojan that exploits the Citrix vulnerability. The NOTROBIN malware operates by performing a POST request to the desired target which originates from a TOR node. The request targets newbm.pl, a vulnerable script on the host that causes a number of commands to be injected into the device; but it is unclear how the NOTROBIN malware moves from the POST request to a state of command injection. To prevent the NOTROBIN exploit, we should ensure that we install the following patch updates: SD-WAN patch, ADC patch, and Citrix Gateway patch. Another way to prevent the NOTROBIN exploit is to implement pre-emptive blocks using a list of identifiers; if these identifiers are found, we should try to block the IP of the user of this exploit. Additionally, we should establish clear lines of communication with incident response team members and stakeholders in case the vulnerability is exploited, so that they are able to react quickly.

5.2 Detection and Analysis

The detection phase refers to collecting data from IT systems, security tools, publicly available information, and people inside and outside the organization, and identifying precursors and indicators of compromise. This step involves monitoring systems and networks for indicators of an incident, such as suspicious network activity, unusual behaviour, or system failures. Precursors are signs that an incident may happen in the future, while indicators are signs that an incident has happened or is happening currently. In the case of the Citrix vulnerability, the precursors of an exploit are the result of a lack of the “preparation” stage in the workflow, meaning that not trying to put proper security controls in place will result in the following precursors: outdated software such as the Citrix ADC or Gateway, unpatched systems that have not applied security patches, and weak security controls such as firewalls, intrusion detection systems, or endpoint protection. The indicators of the exploit are found through logs of monitoring systems. For example, the previously mentioned NOTROBIN exploit has the following indicators of compromise: abnormal network activity as NOTROBIN communicates with remote servers, suspicious file activity as NOTROBIN creates new files on the file system, unexpected system behaviour as NOTROBIN may cause slow performance and unexpected shutdowns, and security alerts as they may be generated by Intrusion

Detection Systems (IDS), firewalls, or endpoint protection software. To be efficient in detecting the exploit, we should listen on the UDP Port 18634 as the exploit uses that port.

The analysis step is used to determine the incident's root cause and identify the systems, data, and users that may have been affected. This may involve reviewing logs, conducting forensic analysis, or consulting with technical experts. The goal is to gain a complete understanding of the incident and determine the best course of action. In the case of the Citrix vulnerability, we need to make use of the IDS to collect logs so that we are able to analyse them. These logs allow us to obtain information about incidents such as the attacker or the target. Examining and analysing logs can prevent future attacks because we can learn how to strengthen the defences of systems, networks, and applications of the organisations.

In many cases, the first point of contact is a member of the organization's IT or security team who detects or is alerted to the incident. This could include a member from the SOC team, a security analyst, a network administrator, or a system administrator. The individual who first detects the incident should first inform the PO and begin to document the incident, including the time of detection, any relevant details about the incident, and any actions taken in response.

Table for reference of Severity level and Escalation:

Severity Level	**Description**	**Escalation**
Critical	An attacker has gained access; confidential data has been exfiltrated; Denial of Service	First point of contact to inform the PO PO to inform the IRM CIO, CSO and the full CSIRT team to commence on investigation. CIO to escalate the incident to the CEO. CSO to inform the relevant authorities IRM to coordinate the response activities of the CSIRT team.
High	An attacker has gained access; non-sensitive data has been exfiltrated	First point of contact to inform the PO PO to inform the IRM,CIO, CSO and the CSIRT team to commence on investigation. CSO to inform the relevant authorities IRM to coordinate the

		response activities of the CSIRT team.
Medium	Attacker has attempted to do reconnaissance; port scanning, identifying systems	First point of contact to inform the PO PO to inform the IRM. IRM to coordinate the response activities of the Technical IT team and SOC team.
Low	Minor network equipment performance issues	First point of contact to inform the PO. PO to inform the Technical IT team and SOC team.

Identifying the attack host might not be possible, especially if the attacker has used techniques such as IP spoofing to obfuscate their identity.

Identification Method for Citrix	**Description and Tool that can be used**
Network Traffic Analysis	Network traffic analysis can help identify the originating IP address or addresses used in the attack. The analysis can be performed using network monitoring tools, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), to identify the IP addresses of systems that have sent the malicious traffic. Wireshark and Snort can also be used to capture and analyse network traffic. It can be used to identify the source IP address of the malicious traffic associated with the Citrix vulnerability.
Log Analysis	Organizations should collect and analyse system logs to identify any suspicious activity associated with the Citrix vulnerability. This can include analysing firewall logs, server logs, and application logs to identify signs of compromise. SIEM tools such as Splunk can be used to collect and analyse log data from various systems, including firewalls, servers, and endpoints. It can help identify the source of the attack traffic and provide valuable insights into the attack.
Digital forensics	Volatility is a memory forensics tool that can be used to analyse memory dumps from compromised systems. It can be used to identify the processes and network connections associated with the attack and provide insights into the attacker's techniques

Finding information about the IP Address through the internet	Conducting an online search using the source IP address of an attack may yield additional information about the attacker, such as a mailing list message discussing a similar attack.

5.3 Containment

The containment phase refers to implementing measures to stop the spread of the vulnerability and prevent further damage. This may include isolating affected systems from the network, disabling access to sensitive information, or taking systems offline. Therefore, the goal of containment is to stop the attack before it overwhelms resources or causes damage. In the case of the Citrix vulnerability, it is integral that we respond immediately. There are two ways to try to contain the Citrix vulnerability. The first way is through system isolation, which is when systems affected by the vulnerability are disconnected from the network to prevent the spread of the vulnerability. The second way is through network segmentation, which achieves a similar result of isolation, but instead of disconnecting the affected system, we need to configure firewalls, routers, or other network devices to prevent the spread of the vulnerability. Do not suddenly power off the affected system as that may cause loss of evidence for investigation

5.4 Eradication

The eradication phase refers to eliminating the root cause of the incident and restoring the systems and data to a secure state, which includes applying patches to vulnerable systems, removing malware from affected systems, and updating security configurations to prevent similar incidents from occurring in the future. In the case of the Citrix vulnerability, the “eradication” comes in the form of trying to remove the NOTROBIN malware that exploits the vulnerability; to do this, we can update the system to patch the vulnerability. If the IP address of the attacker is found, blacklist the IP address.

5.5 Recovery

The recovery phase refers to restoring normal operations as quickly as possible, while ensuring that the systems and data are secure and that any risks have been addressed, which includes the usage of backups or snapshots to restore systems and data, testing the systems to ensure that they are working properly, communicating with stakeholders to inform them of the status of the recovery process, and last and most importantly, we need to review and update the incident response plan based on the lessons learnt from the incident; this ensures that the attack will not happen again because we will have the knowledge and experience on how to deal with the vulnerability. Additionally, reset passwords of affected systems to prevent future attacks.

Citrix Vulnerability		
Process	Procedures	Teams Involved
Preparation	• *All systems should be updated with the latest security patches* • *All systems should have proper security controls in place* • *Implement pre-emptive blocks* • *Establish clear lines of communication* • *Do not suddenly power off the affected system as that may cause loss of evidence for investigation*	• *Technical IT Team* • *Communications Team*
Detection and Analysis	• *Monitoring systems and networks for indicators of compromise*	• *SOC Team*
Containment	• *System isolation; affected systems are disconnected from the network* • *Network segmentation; configure firewalls, routers, and other network devices*	• *CSIRT Team* • *Technical IT Team* • *BC Team*
Eradication	• *Remove the NOTROBIN malware by patching the Citrix vulnerability* • *Blacklisting of attacker IP*	• *CSIRT Team* • *Technical IT Team*
Recovery	• *Usage of backups or snapshots to restore systems and data* • *Inform stakeholders of the recovery process* • *Reset passwords of affected systems*	• *CSIRT Team* • *Technical IT Team* • *Communications Team*

6. Incident Response Workflow (Ransomware)

6.1 Preparation

In the case of ransomware, security measures and access controls need to be put in place to prevent and mitigate the risk of ransomware.

When it comes to preventing attackers from doing a ransomware attack on the organisation's systems, there are a few ways to do it. The first way is to apply software patches and updates that combat ransomware such as operating system updates and anti-virus software updates. The second way is to train employees to be cautious when opening emails and attachments from unknown sources that may be malicious; to reduce the chances of this, the company can implement email filtering and scanning to block phishing emails. The third way is to define reporting procedures that show employees what to look out for and who to contact if they feel that there may be a potential ransomware attack on the organisation.

When it comes to mitigating the risk of ransomware would be to do regular backups and snapshots of the data and intellectual property of the organisation and its stakeholders. They should be securely stored offline, as putting the backups and snapshots online puts them at risk of being accessed by attackers.

6.2 Detection and Analysis

To detect ransomware, the IT operations team of the organisation should ensure that logging and monitoring of systems and networks are implemented to detect the signs of a potential ransomware attack. Logging and monitoring should be done for the entire organisation, including the systems, networks, communications, and processes.

After these measures are implemented, it is the responsibility of the SOC team to analyse the logs, so that the organisation can detect any signs of malware quickly; allowing the organisation to respond immediately and to try to mitigate the risks

Table of reference for Severity level and Escalation:

Severity level	Description	Escalation
Critical	The ransomware has spread throughout the entire network, infecting majority to all connected devices and systems; attacker demands payment for decryption	First point of contact to inform the PO PO to inform the IRM CIO, CSO and the full CSIRT team to commence on investigation. CIO to escalate the incident to

		the CEO. CSO to inform the relevant authorities IRM to coordinate the response activities of the CSIRT team.
High	Attacker encrypts data on a few systems within the organisation; attacker demands payment for decryption	First point of contact to inform the PO PO to inform the IRM,CIO, CSO and the CSIRT team to commence on investigation. CSO to inform the relevant authorities IRM to coordinate the response activities of the CSIRT team.
Medium	Attacker gains access through phishing emails or unpatched vulnerability; attempted to do reconnaissance; port scanning, identifying systems	First point of contact to inform the PO PO to inform the IRM. IRM to coordinate the response activities of the CSIRT team
Low	Attacker sends suspicious attachments or links that seem malicious to attempt to spread malware	First point of contact to inform the PO. PO to inform the CSIRT team

Identification Method for Ransomware	**Description and Tool that can be used**
Log Analysis	SIEM tools such as Splunk can be used to collect and analyse log data from various systems, including firewalls, servers, and endpoints. It can help identify the source of the attack traffic and provide valuable insights into the attack.

Endpoint detection and response (EDR)	Endpoint Detection and Response can be useful in identifying potential attacks at their early stages, including detecting viruses within the first few days. It also helps to isolate infected devices, preventing further damage outside of the local system while retaining important forensic data
Finding similar Incidents through the internet	The US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT. Available at: https://www.cisa.gov/uscert/ncas/current-activity#:~:text=The%20US%2DCERT%20Current%20Activity,reported%20to%20the%20US%2DCERT.

6.3 Containment

In case the defensive measures against ransomware are not effective and the organisation is attacked, the first thing we should do is to try to contain the ransomware to ensure that it does not spread to other systems in the network to minimise further damage. One way to contain ransomware is by isolating the affected systems from the rest of the organisation's infrastructure by physically disconnecting the infected systems and devices; this method is used to limit the damage done. Another way to contain ransomware is by quarantining the affected systems by limiting the access or permissions of the infected systems and devices while still allowing them to remain connected to the network; the affected system still functions so that it can be analysed and repaired.

6.4 Eradication

After containing the ransomware to minimise the damages, we should try to remove it by eliminating the root cause of the incident.

1. If possible, the IT operations team should try to decrypt any encrypted files or data, so that we can get back the data; making the ransom useless.

2. If the malware comes in a form of malware, the IT operations team should attempt to remove the malware.

3. If the ransomware is due to a known vulnerability, the IT operations team should patch the vulnerability that was exploited by updating any outdated software.

6.5 Recovery

After removing the ransomware, we will need to restore the data and services to their states before the attack. The main way we do recovery in the case of ransomware is through the usage of backup and snapshots; paying the ransom to recover the data is highly not recommended because of the massive financial loss, and the lack of guarantee that the attacker will give back the data.

Assuming steps to prevent ransomware have been set, recent backups and snapshots should be available to restore data. These recovery points ensure that we can restore the data that the attackers have encrypted without having to pay the ransom.

After ensuring that the malware has been removed from affected systems, we can return systems that were isolated or quarantined to the network.

Ransomware Vulnerability		
Process	Procedures	Teams Involved
Preparation	• *Apply software patches and updates that combat ransomware* • *Train employees to be cautious when opening emails and attachments from unknown sources* • *Define reporting procedures* • *Ensure that regular backups are done on systems*	• *Technical IT Team* • *Communications Team* • *CSIRT Team*
Detection and Analysis	• *Ensure that logging and monitoring of the entire organisation should be implemented* • *Analyse logs to detect signs of malware quickly*	• *Technical IT Team* • *SOC Team*
Containment	• *System isolation; affected systems are disconnected from the network* • *System quarantining; affected system still functions to allow for analysis and repair*	• *Technical IT Team* • *CSIRT Team*
Eradication	• *Attempt decryption of encrypted files and data* • *Remove the malware causing the ransomware* • *Patch any vulnerabilities causing ransomware*	• *Technical IT Team* • *CSIRT Team*
Recovery	• *Restore backups and snapshots for data and snapshots* • *Return isolated and quarantined systems to networks*	• *Technical IT Team* • *CSIRT Team* • *Communications Team* • *BC Team*

7. Guidelines

Many inquiries and issues come up over the course of responding to an incident, each of which may be distinct for each incident. Guidelines for resolving common problems and inquiries are provided in this section.

7.1 Insider Threats

If an insider threat is detected, the suspect should be brought before SPIM Consulting and Monitoring Pte Ltd.'s Disciplinary Committee for questioning. The suspected individual shall be questioned by the Disciplinary Committee as necessary to ascertain their goals and whether they are indeed an insider.

Insiders and moles in SPIM who are malevolent shall be reported to the police and tried in court as appropriate. Depending on the outcome, they may be charged either civilly or criminally under the Security and Futures Act (SFA).

Depending on the seriousness of the occurrence, different penalties may be imposed on negligent insiders in SPIM who inadvertently threatened SPIM. The person may anticipate having their access to the SPIM facility revoked in more serious circumstances.

7.2 Interactions with Law Enforcement

Only after seeking legal counsel from the legal team should any interactions and conversations with external law enforcement agencies be initiated. When the Chief Information Officer (CIO) approves, the Computer Security Incident Response Team (CSIRT) will collaborate with law enforcement to identify the information needs and share only the information that is essential for the incident response.

The Computer Security Incident Response Team (CSIRT), in collaboration with the legal team's legal advisors, will decide if notification is necessary, its format, and timeliness. Part 6A of the Personal Data and Protection Act 2012 mandates notification to the Personal Data Protection Commission (PDPC) of Singapore.

7.3 Communications Plan

The Personal Data Protection Commission (PDPC) of Singapore will be the sole point of contact between the Computer Security Incident Response Team (CSIRT) and SPIM in the event that there are reasonable grounds to believe that a breach has taken place.

If SPIM determines that it is appropriate following an internal evaluation to confirm the incident is notifiable, based on section 6A of the Personal Data and Protection Act 2012, the point of contact will immediately report the incident to the point of contact from the Personal Data Protection Commission (PDPC) of Singapore. If SPIM determines that it is appropriate following an internal evaluation to confirm the incident is notifiable, based on section 6A of the Personal Data and Protection Act 2012, the point of contact will immediately report the incident to the point of contact from the Personal Data Protection Commission (PDPC) of Singapore.

7.3.1 Communications with the Commission

SPIM Consulting and Monitoring Pte Ltd. will establish clear lines of communication with the Personal Data Protection Commission (PDPC) of Singapore to ensure timely and accurate reporting of any potential data breaches. The point of contact for communications with the PDPC will be the Computer Security Incident Response Team (CSIRT).

In the event of a data breach, the CSIRT will immediately notify the PDPC's point of contact and provide all necessary details, including the nature of the breach, the scope of data affected, and the steps being taken to remediate the situation. The CSIRT will work closely with the PDPC to ensure compliance with all reporting requirements under the Personal Data and Protection Act 2012.

All communications with the PDPC will be conducted in a timely and transparent manner, with the goal of minimizing any potential harm to affected individuals while also complying with all legal and regulatory requirements. The CSIRT will keep detailed records of all communications with the PDPC, including the timing and content of all reports and updates.

7.3.2 Communications with Affected Individuals

If SPIM determines that the incident is a personal data breach that is likely to result in significant harm to affected individuals, SPIM will notify affected individuals without undue delay. The notification will include clear and concise information about the nature of the personal data breach and the data subjects impacted. The notification will also provide information about the measures that SPIM is taking to address the breach, including any mitigating steps that have been taken or are being taken to prevent further harm. SPIM will also provide contact information for individuals who may have further questions or concerns about the breach.

7.3.3 Communications with External Media Agencies

In the event of a cyber security incident, SPIM Consulting and Monitoring Pte Ltd. (SPIM) should only communicate with external media agencies through a designated spokesperson who is authorized to speak on behalf of the company. All communication should be consistent, accurate, and transparent to maintain credibility and protect the interests of the company and its clients.

Before communicating with external media agencies, the spokesperson should seek guidance from the legal team and coordinate with the Cyber Security Incident Response Team (CSIRT) to ensure that the information shared is appropriate, factually correct, and does not compromise the ongoing investigation.

Any media inquiries should be handled in a timely manner, and a record of all communications should be maintained. If the incident involves personal data, SPIM should follow the Personal Data Protection Commission (PDPC) guidelines on notification and make appropriate disclosures to affected individuals and the public.

7.3.4 Communications with Internal Teams

Internal team discussions about prospective occurrences are extremely confidential and ought to be kept private outside of the context of an investigation. The Computer Security Incident Response Team (CSIRT) is informed of the incident's preliminary findings in the initial communications, as well as in updates throughout the incident (such as during internal assessments, eradication efforts, and recovery), as well as after the incident (such as findings from the incident, lessons learned, and post-incident activities). When communion isn't done in person, it's necessary to employ secure, encrypted means of communication like emails and a dedicated incident status website.

7.4 Privacy

Privacy is a critical concern for SPIM Consulting and Monitoring Pte Ltd. To safeguard the privacy of its clients, employees, and partners, the following guidelines must be followed:

1. Access to sensitive information should be restricted to only authorized personnel who have a legitimate need to access such information.
2. Personal data should be processed lawfully and fairly, and only for the purpose for which it was collected. Any processing of personal data must be done in accordance with the Personal Data Protection Act 2012.
3. Personal data should be kept confidential and protected from unauthorized access, disclosure, alteration, or destruction.
4. Employees should be trained on data protection principles, and data privacy policies and procedures should be reviewed regularly.
5. Third-party service providers who handle personal data on behalf of SPIM Consulting and Monitoring Pte Ltd should be selected carefully and monitored regularly to ensure compliance with data protection standards.
6. Incident response plans should be in place to address any privacy breaches that may occur. In the event of a privacy breach, affected individuals should be notified promptly and provided with information on the steps being taken to mitigate the breach.

7. Regular reviews of privacy policies and procedures should be conducted to ensure that they are up to date with changes in the legal and regulatory environment.

By following these guidelines, SPIM Consulting and Monitoring Pte Ltd can maintain the privacy of its clients, employees, and partners and ensure compliance with relevant data protection regulations.

7.5 Staffing

The Incident Response Manager (IRM) will try to keep adequate employees on hand to handle any incident's investigation and response from start to finish. External third-party IT suppliers will be hired to assist with the incident response if internal manpower is not available or adequate owing to a high volume of occurrences. The internal Computer Security Incident Response Team (CSIRT) will inform the third-party vendor of the status of the incident, findings, and actions that have been taken up to that point when a third-party IT vendor is brought in for the purpose of incident response, and then continue to keep monitoring tools and detecting new incidents.

When there are few occurrences, SPIM Consulting and Monitoring Pte Ltd will implement a staff duty schedule. The internal Computer Security Incident Response Team (CSIRT) will be divided into two groups during this period. The functions of incident response will be allocated to half of the Computer Security Incident Response Team (CSIRT) members, while system administration in other departments will be assigned to the other half of the team. This schedule is designed to ensure that the Computer Security Incident Response Team (CSIRT) always has a member available to respond to emergencies.

The Computer Security Incident Response Team (CSIRT) may frequently need to collaborate closely with other SPIM Consulting and Monitoring Pte Ltd departments, such as the legal team while responding to incidents. The Incident Response Manager (IRM) will determine which SPIM Consulting and Monitoring Pte Ltd departments and employees are crucial to the current incident so that redundancy of effort and disputes are averted.

7.6 Training Plans

Through adequate continuous training, SPIM Consulting and Monitoring Pte Ltd (SPIM) will make sure that the Computer Security Incident Response Team's (CSIRT) and Security Operations Center (SOC) Team’s competency is sustained over time with high standards. Processes, rules, and standards are continuously evaluated, tested, and improved as seen by the continual development of incident response and handling procedures. On a regular cycle, training programs will be assigned to each member of the Computer Security Incident Response Team (CSIRT) and Security Operations Center (SOC) Team, focusing on the following skill sets:

1. Security Awareness
2. Incident Handling and Reporting
3. Information Gathering and Incident Analysis
4. Evidence Preservation
5. Training for Third-Party Tools

6. Communication Skills

It is critical to develop a consistent and appropriate reaction to new occurrences and that post-incident findings be integrated into policy and practice since the internet is continually evolving. To maintain familiarity with the systems and environment they are working with, members of the Computer Security Incident Response Team (CSIRT) and Security Operations Center (SOC) Team will also get ongoing training on new protocols and technologies utilized in SPIM.

8. References

Avertium (2020) NOTROBIN malware exploiting Citrix CVE-2019-19781, Avertium. Available at: https://www.avertium.com/blog/notrobin-malware-exploiting-cve-2019-19781 (Accessed: February 11, 2023).

Baker, K. (2023) 10 pro tips to prevent ransomware: CrowdStrike, crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-prevent-ransomware/#:~:text=Ransomware%2DProof%20Data%20with%20Offline,Test%20an%20Incident%20Response%20Plan (Accessed: February 12, 2023).

Chai, W. and Lewis, S. (2020) What is an incident response team? definition from whatis.com, Security. TechTarget. Available at: https://www.techtarget.com/searchsecurity/definition/incident-response-team#:~:text=Responsibilities%20of%20an%20incident%20response,for%20all%20incident%20handling%20measures. (Accessed: February 12, 2023).

CISA (2020) Alert (AA20-031A), CISA. Available at: https://www.cisa.gov/uscert/ncas/alerts/aa20-031a#:~:text=CVE%2D2019%2D19781%20is%20an,control%20of%20an%20affected%20system. (Accessed: February 11, 2023).

Commvault (2022) Ransomware: 4 ways to protect and recover, Commvault. Available at: https://www.commvault.com/resources/ransomware-4-ways-to-protect-and-recover (Accessed: February 12, 2023).

Critical Start. (2021). SOC vs. CSIRT: What's the Difference? Critical Start. https://www.criticalstart.com/soc-vs-csirt-whats-the-difference/ (Accessed: February 17, 2023).

Cynet (2022) Incident response team: A blueprint for success, Cynet. Available at: https://www.cynet.com/incident-response/incident-response-team-a-blueprint-for-success/#:~:text=There%20are%20three%20main%20types,Security%20Operations%20Center%20(SOC). (Accessed: February 12, 2023).

Cynet (2022) NIST Incident Response Plan: Building your IR process, Cynet. Available at: https://www.cynet.com/incident-response/nist-incident-response/#:~:text=An%20incident%20response%20plan%20(IRP,plans%2C%20and%20standardized%20response%20protocols. (Accessed: February 11, 2023).

Gallagher, S. (2020) Unpatched citrix vulnerability now exploited, Patch Weeks away, Ars Technica. Available at: https://arstechnica.com/information-technology/2020/01/unpatched-citrix-vulnerability-now-exploited-patch-weeks-away/ (Accessed: February 11, 2023).

Groot, J.D. (2022) A history of ransomware attacks: The biggest and worst ransomware attacks of all time, Digital Guardian. Available at: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#:~:text=Some%20of%20the%20most%20advanced,common%20types%20of%20advanced%20malware. (Accessed: February 12, 2023).

Imperva (2021) What is ransomware: Attack types, protection &amp; removal: Imperva, Learning Center. Available at: https://www.imperva.com/learn/application-security/ransomware/ (Accessed: February 12, 2023).

IMY (2021) The purposes and scope of GDPR, IMY. Available at: https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/the-purposes-and-scope-of-gdpr/#:~:text=One%20of%20the%20purposes%20of,on%20Human%20Rights%20(ECHR). (Accessed: February 13, 2023).

IT Process Wiki - the ITIL® Wiki. (2023). Checklist Incident Priority | IT Process Wiki. [online] Available at: https://wiki.en.it-processmaps.com/index.php/Checklist_Incident_Priority.https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities

O'Donnell, L.L. (2020) Unpatched citrix flaw now has Poc Exploits, Threatpost English Global threatpostcom. Available at: https://threatpost.com/unpatched-citrix-flaw-exploits/151748/ (Accessed: February 11, 2023).

PDPC (2021) PDPC: PDPA Overview, Personal Data Protection Commission. Available at: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act#:~:text=What%20is%20the%20PDPA%3F,Banking%20Act%20and%20Insurance%20Act. (Accessed: February 13, 2023).

Plotlights (2022) Ransomware attacks: A quick guide for communicators, Plotlights. Available at: https://www.plotlights.com/blog/ransomware-attacks-a-quick-guide-for-communicators/ (Accessed: February 12, 2023).

Proofpoint (2023) What is ransomware? - definition, prevention &amp; more: Proofpoint us, Proofpoint. Available at: https://www.proofpoint.com/us/threat-reference/ransomware (Accessed: February 12, 2023).

SANS (2022) Security policy templates, Information Security Policy Templates | SANS Institute. Available at: https://www.sans.org/information-security-policy/ (Accessed: February 11, 2023).

SearchSecurity. (2023). CERT vs. CSIRT vs. SOC: What's the difference? [online] Available at: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference.https://www.atlassian.com/incident-management/incident-response/roles-responsibilities (Accessed: February 17, 2023).

Trellix (2023) What is endpoint security? how it works &amp; its importance, Trellix. Available at: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html#:~:text=Endpoint%20security%20is%20the%20practice,the%20cloud%20from%20cybersecurity%20threats. (Accessed: February 13, 2023).

U.S. Department of Homeland Security. (n.d.). Current Activity. Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/uscert/ncas/current-activity#:~:text=The%20US%2DCERT%20Current%20Activity,reported%20to%20the%20US%2DCERT (Accessed: February 16, 2023)

William Ballenthin (2020) Vigilante deploying mitigation for Citrix NetScaler vulnerability while maintaining backdoor, Mandiant. Available at: https://www.mandiant.com/resources/blog/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor (Accessed: February 11, 2023).

Appendix

INCIDENT RESPONSE PLAN			
Student Name/ID	Item	Description	Reference/Comments
Francis/2123222	Incident Response Workflow (Citrix Vulnerability), Incident Response Workflow (Ransomware)	Workflows with the 5 phases to address the Citrix vulnerability and Ransomware	
Shushant/2123602	Guidelines, Roles, and Responsibilities	Guidelines for the Incident Response Plan	
Adeeb/2107095	Purpose and Scope of Report - Communications with the Commission - Communications with Affected Individuals - Communications with External Media Agencies - privacy		
Marcus/2123392	- Overview -Roles and Responsibilities -Incident Response Workflow on Detection and Analysis and containment (Citirix Vulnerability and Ransomware)		