APACMed
The voice of MedTech

Cybersecurity Incident Response Guide (CSIRG) for Medical Device Manufacturers in APAC

KNOWLEDGE PARTNER

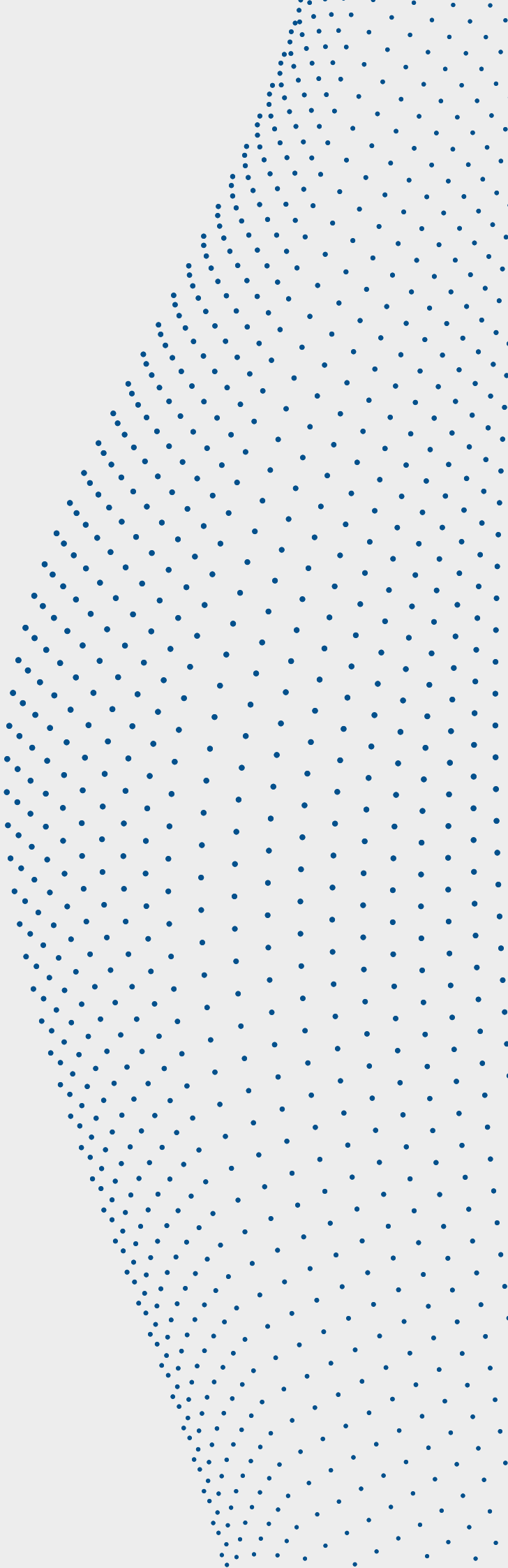
ENSIGN INFOSECURITY

HEALTH DATA

Contents

Overview of Cybersecurity Incident Response Guide (CSIRG) for Medical Device Manufacturers in APAC

Cybersecurity Incident Response Framework (CSIRF)



Cybersecurity Incident Response Plan (CSIRP)

Overview of Cybersecurity Incident Response Guide (CSIRG) for Medical Device Manufacturers in APAC

The Cybersecurity Incident Response Guide (CSIRG) aims to provide medical device manufacturers guidance in handling a cybersecurity incident. This document serves as a foundation for medical device manufacturers to build, maintain, and enhance their cybersecurity incident response capabilities to minimise the impact of cybersecurity incidents. These guidelines are not prescriptive. Medical device manufacturers should assess and select the approaches that best align with their unique needs and circumstances. The guide makes reference to the National Institute of Standards and Technology's (NIST) cybersecurity framework of Govern identify, Protect, Detect, Respond, and Recover as a foundation and adapted it to an incident response plan context.

The **CSIRG** is divided into two sections:

a. Cybersecurity Incident Response Framework (**CSIRF**)

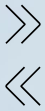
The CSIRF outlines the minimum capabilities the Cybersecurity Incident Response Team (CSIRT) should possess to effectively manage cybersecurity incidents based on NIST's pillars of Govern, Identify, Protect, Detect, Respond and Recover. The govern function in the incident respond context defines the policies and procedures that should be taken when an incident occurs and details the roles and responsibilities of each team member. This will be covered in detail throughout the CSIRF and CSIRP as sections are included in addition to the other five pillars in the NIST framework.

The framework lists the team structure and their roles and responsibilities during an incident and what needs to be included in the various steps of incident management (e.g., incident identification, reporting, assessment, responding, communication, post-incident analysis).

b. Cybersecurity Incident Response Plan (**CSIRP**)

The CSIRP focuses on the Detect, Respond and Recover phases of Incident Response to provide guidelines on executing the processes (e.g., incident identification, reporting, assessment, responding, communication, post-incident analysis). The guidelines are not prescriptive allowing medical device manufacturers to customise the execution of the processes. Contextualised examples are also provided to facilitate better understanding.

FRAMEWORK



PLAN

Discusses "what" is needed and "why"

Example:
Organisations must establish a comprehensive communications plan to promptly inform relevant stakeholders during incidents or crises ("what"), thereby mitigating the risk of misinformation and preventing unncessary panic ("why").

Discusses "how" to provide guidelines on implementing the framework

Example:
When an incident occurs, following the communications plan, an SMS is sent to all employees. Employees are expected to acknowledge within 5 minutes of receiving the SMS. If they have something important to report, they can do so by submitting a ticket via the link provided in the SMS.

Cybersecurity Incident Response Framework (CSIRF)

1. Team Structure / Roles and Responsibilities

This section outlines CSIRT's team structure and their roles and responsibilities. As a team, the CSIRT aims to protect the organisation by effectively handling cybersecurity incidents to minimise any impact and ensure the organisation can return to normal operations with minimal disruptions. The team also reflects from the incidents to further enhance future response capabilities by identifying any areas of improvement from managing the incident. Sections 1.1 to 1.6 are core roles that are required in the CSIRT. Sections 1.7 to 1.13 describe roles that belong to the Centre of Excellence (COE) and are considered an extension to support the CSIRT during incidents and crises. The difference between a CSIRT and a PSIRT is that the CSIRT is responsible for the organisation's cybersecurity posture, while the PSIRT is responsible for incidents arising specifically from the product. However, for organisations that do not have the manpower to have both a CSIRT and the PSIRT, the CSIRT will need to take over the role of the PSIRT. Alternatively, the organisation may consider hiring retainers (see 1.13) to supplement the CSIRT during incidents / crises.

1.1. Executive Management

- **Role:** Oversight and decision-making authority.
- **Responsibilities:**
  - Approve the CSIRP and ensure it aligns with corporate policies and regulatory requirements.
  - Provide necessary resources and support for incident response activities.
  - Communicate with regulatory bodies, partners, and customers as needed during major incidents.

1.2. Incident Commander

- **Role:** Direct resources and sense making of an incident.
- **Responsibilities:**
  - Lead and coordinate the incident response process.
  - Make strategic decisions on response actions.
  - Coordinate investigation actions and resources.
  - Ensure resolution of the incident.

1.3. Security Analysts

- **Role:** Triage, analyse and respond to incidents.
- **Responsibilities:**
  - Monitor digital assets for any potential incidents and to continue monitoring during and after incidents /crises.
  - Categorise incidents based on predetermined criteria (e.g., severity, impact).
  - Analyse incidents and implement measures for containment / eradication / recovery.
  - Escalate incidents up to next tier analysts if unable to handle due to complexity of incident or if unable to resolve incident in the stipulated amount of time.
  - Recommended to have 2 tiers of analysts; details will be specified in the CSIRP below.

1.4. Threat Intelligence Analysts

- **Role:** Threat Intelligence Sharing; understanding latest threats in relation to the incident.
- **Responsibilities:**
  - Analyse latest threats.
  - Contextualise the threats based on attack surface.
  - Identify indicators of compromise (IOCs) and threat actor tactics, techniques, and procedures (TTPs).
  - Update the team on intelligence gathered to ensure team is prepared on any emerging threats and help to prioritise incidents associated with high-risk threats.

1.5. 1.5. Digital Forensics Specialists

- **Role:** Conduct forensic analysis on the compromised system(s) and data.
- **Responsibilities:**
  - Collect and preserve digital evidence in a forensically sound manner.
  - Assist in root cause analysis and identification.
  - Document findings and be prepared to support the legal team for any potential legal actions.

1.6. IT Infrastructure Specialists

- **Role:** Maintain IT infrastructure and support services
- **Responsibilities:**
  - Ensure the availability and security of IT systems and networks.
  - Support the deployment of security patches and updates.
  - Assist in containing / eradicating the identified threats.
  - Perform system recovery and restoration to help organisation return to normal operations.
  - Verify that data integrity is maintained after system recovery / restoration.
  - Ensure system backups are available and refreshed constantly in accordance with the organisation's policy.

1.7. Legal and Compliance Officers

- **Role:** Ensure compliance with legal and regulatory requirements.
- **Responsibilities:**
  - Advise on regulatory requirements related to product security and incident response.
  - Manage communication with regulatory bodies.
  - Ensure all incidents comply with applicable laws and regulations.

1.8. Communications and Public Relations Specialists

- **Role:** Manage internal and external communications during incidents / crises.
- **Responsibilities:**
  - Develop and disseminate communication plans and statements.
  - Coordinate public disclosures and media interactions.
  - Advise senior management on all communications as necessary.
  - Ensure consistent and accurate message to stakeholders.
  - Monitor social media and issue statements against any false rumours / allegations that are being spread.

1.9. Risk Management Officers

- **Role:** Identify, assess, mitigate, and monitor risks associated with incidents / crises.
- **Responsibilities:**
  - Identify systemic risks arising from the actions of the Threat Actor and those taken in response to the threats.
  - Conduct risk assessments to identify potential vulnerabilities that may be exploited by threat actors.
  - Maintain and update a risk register regularly that documents the risk, impact, likelihood, and severity.
  - Perform an impact analysis based on the identified risks and breakdown the impacts into categories (e.g., technological, operational, reputational, legal).
  - Advise the potential systemic risks arising from incidents / crises and actions taken during the course of the incidents / crises.

1.10. Human Resource Officers

- **Role:** Manage employee issues and concerns, act as liaison between CSIRT and employees.
- **Responsibilities:**
  - Support in investigations involving employees such as conducting interviews and collating relevant information, especially when an insider threat is suspected.
  - Handles disciplinary actions in accordance with organisation's policies and/or legal requirements.
  - Keep track of employees' safety and status in an incident, ensuring all employees are accounted for in the event of any physical threats or evacuation.
  - Coordinate with internal communications to keep employees updated on incident developments.

1.11. Finance Analysts

- **Role:** Track and manage costs associated with responding to cybersecurity incidents / crises.
- **Responsibilities:**
  - Ensure there are sufficient financial resources allocated to CSIRT and facilitate additional allocation of funds (if required) during incidents or crises.
  - Track costs directly associated with the incident response (e.g., hiring retainers to conduct forensic analysis).
  - Quantify the financial impact of indirect costs (e.g., service and operational downtime translated into estimated monetary values).

1.12. Stakeholder Management Officers

- **Role:** Provide support to manage stakeholders (internal and external) during incidents / crises.
- **Responsibilities:**
  - Identify stakeholders that need to be notified based on the incident that occurred (e.g., customers, board of directors, regulatory bodies, media, public).
  - Develop tailored management plans for different stakeholder groups that address their specific needs and concerns.
  - Collect and relay feedback back to CSIRT to ensure they are aware of the stakeholders' concerns.
  - Foster and maintain trust with stakeholders by being transparent and proactive in notification and communication efforts so they can tailor incident response plans accordingly.

1.13. Retainers

- **Role:** Third-party specialists that provide support during incidents / crises and are only activated when needed.
- **Responsibilities:**
  - For organisations that are smaller in size and do not have the manpower to create a fully staffed CSIRT, consider hiring retainers.
  - Retainers could fulfill roles such as Threat Intelligence Analysts, Digital Forensics Specialists, Incident Response Analysts, Public Relations and Crisis Communication Specialists, Legal Counsel, Crisis Operations Advisors etc.
  - Retainers will only be activated when their skillsets are required, thus helping organisations save on the hiring and maintenance costs.

2. Identify

The CSIRT needs to know the attack surface of their organisation. This includes all connected systems. A System Criticality Matrix should be established and maintained to identify essential/important and critical systems needed to support the core services of their organisation.

In the medical devices manufacturers context, essential/important and/or critical systems could include:

- Electronic health records (e.g., patient's health information).
- Supply chain systems that manage logistics of inventory, suppliers, and distribution.
- Intellectual Property (e.g., proprietary technology, software code, patents, and/or trade secrets).
- Core IT systems required to keep operations running.
- Customer databases.

Example: A medical device manufacturer identified that their critical system is their database, which stores sensitive patient's health information and intellectual property. The CSIRT team conducted a threat landscape analysis and identified that healthcare providers in the region have been victims of ransomware attacks and data leaks. In response, the CSIRT developed a comprehensive plan to safeguard the database, which laid the groundwork for effective incident response.

3. Protect

The CSIRT needs to be aware of the protection safeguards that are in place to protect the attack surface of their organisation. This will enable them to respond more efficiently and effectively during incidents.
Protection safeguards include:

- Access Controls (i.e., use of multi-factor authentication and strong password policies).
- Zero Trust architecture to implement continuous reverification of users to mitigate against insider threats / unauthorised access.
- Inventory Tracking that includes the SBOM (Software Bill of Materials).
- Data Leak Prevention (DLP) tools to prevent sensitive data from being leaked.
- Endpoint Protection solutions (e.g., antivirus and antimalware software).

Example: To prevent the leak of sensitive patients' health information, the CSIRT proactively sets up DLP tools that would automatically detect the sensitive information (e.g., identification number) and prevent it from being sent out. The DLP is also configured to send an alert of any attempts to send such information out (regardless of accidental or intentional attempts). Zero trust is also implemented to repeatedly re-verify employees' identity, with endpoint protection solutions implemented to protect the DLP tools from being disabled. These measures will allow the CSIRT to respond effectively to any potential data leaks.

4. Detect

Detecting a cyber incident involves several high-level processes that are designed to detect, analyse and confirm the presence of a security incident effectively and efficiently.

4.1. Monitor

Description: Deploy a suite of tools that will monitor and analyse events as they occur in real-time. Some types of popular used tools include:

- **Security Information and Event Management (SIEM):** SIEM systems are used to collect, analyse and correlate security events in real-time.
- **Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS):** IDS / IPS are used to monitor network traffic for suspicious activities.
- **Endpoint Detection and Response (EDR):** EDR solutions are implemented to monitor and respond to threats on endpoints (e.g., end-user devices such as desktops, laptops, servers, and mobile devices).

4.2. Alert

Description: Configure alerts based to detect anomalies. Define what constitutes normal behaviour and activity for networks, systems, and users in your organisation to serve as a baseline (i.e., reference point to what is normal). Anything that deviates from these baselines are indications of potential incidents.

4.3. Logic Applied

Description: The CSIRT team needs to correctly interpret data and alerts by understanding their respective business processes. Correlating data from multiple sources such as network traffic and endpoint activities to identify patterns is helpful to direct sense making to reduce the occurrences of false positives.

5. Respond

Response procedures have the objective of mitigating the impact caused by the incident. In this phase, the Incident Commander leads the response efforts by the CSIRT (i.e., Security Analysts, Threat Intelligence Analysts, IT Infrastructure Specialists) with the Incident Secretariat offering support in administration, communication, and coordination areas. The Centre of Excellence (CoE) will each step up and prioritise their attention towards the incident response process as well.

5.1. Triage

Description: To effectively manage incidents as they occur, it is crucial to assess and prioritise the incidents that pose the greatest risk to the organisation. This is done by performing a triage. A triage is the process of evaluating and prioritisation of security alerts or incidents based on their severity, impact, and urgency. The process helps allocate resources effectively to ensure there are timely responses to the more critical incidents.

- **Severity Levels in Cybersecurity**

Severity levels help prioritise incidents based on their potential impact on systems and data. The NIST Cybersecurity Framework (CSF) categorises incidents from low to critical, guiding the allocation of resources. Low-severity incidents might involve minor unauthorised access, while critical incidents could include severe ransomware attacks. The main goal is to ensure timely and efficient responses, minimising damage and maintaining trust. This structured approach enables organisations to protect confidentiality, integrity, and availability of systems effectively.

- **Incident Categories**

Establishing incident categories, such as malicious code, unauthorised access, and denial of service, is crucial for effectively managing and responding to cybersecurity incidents. It allows organisations to quickly identify and classify threats, enabling a tailored response strategy that mitigates specific risks associated with each category. By doing so, organisations can allocate resources efficiently, prioritise actions, and minimise damage. The primary goal of categorising incidents is to streamline the incident response process, improve communication among stakeholders, and enhance overall security posture by providing a structured approach to handling diverse security threats.

5.2. Escalation

- **Description:** Clear guidelines need to be established for when and how to escalate an incident. The Incident Commander will make the executive decision on escalations. Incidents are escalated to crises when there are significant impacts to business operations, and this is when senior management and relevant stakeholders will be fully involved in the response processes.

- **Example:** A low-severity incident might involve "scans/probes/attempted access," where external scans detect vulnerabilities in non-critical systems, posing minimal immediate risk. Conversely, a high-severity incident could involve "malicious code" infiltrating product development systems, potentially compromising the integrity of life-supporting device software updates. Appropriate automated and manual pre-determined actions can then be taken to ensure a clean system by removing infected systems and/or files including a trace of the malware. It is important to preserve evidence of the attack through a forensically sound investigation manner from incident detection to recovery.

5.3. Incident Reporting

After an incident has been identified with sense making applied, the next step is to report the incident. Reporting can be done by using the tools listed below and by following the communication plans for internal / external communication.

Reporting Tools

- **Description:** There are a multitude of tools available to help facilitate reporting. While they are not compulsory, they provide immense benefits of notifying the relevant parties timely, logging and documentation of the incident and help with the communication within the organisation that will help bring the incident under control effectively.

- **Incident Reporting and Notification Tools:** The tools in this category are primarily used to notify relevant stakeholders and to escalate incidents as needed. They provide automated alerting and escalation based on predefined rules.

- **Security Information and Event Management (SIEM) Systems:** SIEM systems provide a centralised platform for monitoring, identifying and responding to incidents. The systems generate alerts and reports after a potential incident has been identified.

- **Ticketing and Workflow Management Tools:** These tools assist in managing the workflow of the incident response activities, enabling teams to assign tasks and track the completion progress of each task.

- **Incident/Crisis Management Systems:** These tools help to manage and track incidents/crises throughout their lifecycle. This is crucial for documenting the events as they unfold to establish timelines that will be used during post-incident reviews to upgrade existing cyber response capabilities, allocate appropriate resources and to secure all collected and transmitted event related information.

5.4. Communication

The CSIRT could consider integrating the use of the Traffic Light Protocol (TLP) 2.0 to control the dissemination of information. The CSIRT could also look into using VERIS (Vocabulary for Event Recording and Incident Sharing) for the uniform and consistent communication of incident / crisis related details. VERIS uses a set of metrics designed to provide a common language to describe security incidents in a structured and repeatable manner.

Internal Communication

Description: Internal channels are used to keep employees updated on the progress of the incident. Multiple channels should be prepared in the event one channel is down, there are other means to reach out to the employees. Alternative bands of communication should not belong to the same family of applications (e.g., Microsoft 365) to ensure communications are robust to single points of failures. Some channels include:

- Email
- Secure Messaging Apps
- Incident Management Systems
- Internal Portals
- Meetings (Virtual or in-person)
- SMS
- Push notifications
- Phone calls

External Communication

Description: External communications are conducted to assure external stakeholders that the organisation is aware of the incident and is currently handling it. It is imperative to maintain itself as the single source of truth and to control the narrative. If required, regulatory bodies and/or law enforcement need to be informed as well. Communication can be done through a variety of channels:

- Dark site
- Corporate Websites
- Secured Instant Messaging
- Media Conferences
- Social media
- Email
- Phone calls

Example: During an incident, the Incident Commander uses the SIEM system as a dashboard to monitor the incident response process and reallocates resources as required. Following the communication plan, SMS notifications are sent to all employees to inform them of the situation. Thereafter, the employees will each assume their assigned roles and responsibilities and help to mitigate the impact of the incident. Stakeholder Management Officers also follow external communication plans to reach out to affected stakeholders to update them about the situation. Communications and PR Specialists crafted a press release and published it to take control of the narrative to prevent rumours from forming.

5.5. Containment Strategies

Description: Immediate measures that must be taken to contain the incident to prevent further damage.

- **Access Control:** Strengthen access controls temporarily and implement stricter rules.
- **Network Segmentation:** Implement network segmentation to isolate affected systems.
- **Quarantine Devices:** Quarantine infected or compromised devices.
- **Monitor Isolated Systems:** Continue to monitor isolated systems for any signs of ongoing malicious activity to ensure containment is effective.

5.6. Eradication

- **Description:** Once the incident has been contained, the next steps will be to identify the root cause of the incident and to eradicate the threat. A forensic analysis can be performed to determine how the incident occurred and what vulnerabilities were exploited.

- **Example:** To contain the spread of ransomware, the Incident Commander implemented a network segmentation and decoupled the local servers from regional servers. The CSIRT team then quarantine the affected devices eradicate the ransomware from the systems before performing recovery.

6. Recover

Systems and business operations need to be restored back to normal. During this step, it is crucial to ensure that data integrity is maintained, and that no residual malware remains embedded in the system. Develop a recovery strategy and specify the systems that need to be prioritised and restored in sequential order. A Disaster Recovery Plan (DRP) that refers to the System Criticality Matrix should be established and utilised here. The DRP should minimally detail the Recovery Point Objective and the Recovery Time Objective of each system, in addition to outlining the step-by-step recovery procedures of each system.

Example: In the recovery phase after a ransomware attack, the CSIRT prioritises the decryption and restoration of essential systems using secure backups. The integrity of the restored data is verified to ensure the systems are free of any residual malware.

7. Evidence Collection and Preservation

It is critical to ensure evidence is collected and preserved in a forensically sound manner to maintain its integrity. This is to ensure that investigations can be done effectively and that any findings can be used in legal proceedings. Forensics specialists will need to be involved in this step. The overall idea is that no modifications made (intended or unintended) is allowed, and this can be done by using write blockers or storing the evidence on read-only media. The processes will be covered in more detail in the CSIRP.

Example: A chain of custody is maintained for each piece of evidence collected, detailing who had access to it, for what purpose, at what time, for how long etc. Write-blockers are also used to prevent modification done to the evidence.

8. Documentation

The documentation process ensures that all actions taken during an incident are thoroughly recorded for post-incident review to improve future incident responses.

Documentation Tools:

- Incident/Crisis Management Systems: These incident/crisis management systems will streamline, automate, and secure documentation and evidence collection to help with maintaining detailed, complete, and consistent records.

- Templates and Checklists: Use predefined templates and checklists to ensure comprehensive and consistent documentation across all incidents.

Example: The CSIRT and CoE upload their documented notes during the incident onto the incident management system after the crisis for collation purposes. They used predefined templates, therefore the information can be archived systematically by the system and sorted to provide a clear timeline of events.

9. Post-Incident Analysis

The objective of a post-incident analysis is to review and evaluate the incident response efforts that just occurred to identify opportunities for improvement.

9.1. Lessons Learned

Description: Identify both the successful aspects and challenges faced during the incident response process. Senior management should make it clear that the intention of doing a "Lessons Learned" session is not to point fingers and allocate blame, but rather to identify which areas require improvements.

Example: Two areas of improvement were identified: (1) There were too many alternative communication channels, employees were confused which to use; (2) The data owner and system owner were unclear about who should be responsible for the incident as they had co-ownership of the affected file. The Executive Management updated the incident response procedures and decided to send all employees for additional training so that they know what actions to take in future incidents.

10. Review and Update

Description: Develop a list of actionable items, prioritising the most crucial items. Prioritising factors could include the items that can be done in the shortest amount of time or by the impact it will have on existing plans; impactful changes will usually take a longer time to be implemented, therefore consider having multiple parallel processes.

Example: HR was assigned to keep track of employees' progress on completing the e-learning module. IT Infrastructure Specialists also closely monitored to see which endpoint device has yet to be updated and work with HR to identify these employees. HR reports back to Executive Management on uncooperative employees and there was a suggestion to induce a penalty for those that do not complete the module by a specified date.

11. Legal and Regulatory Compliance

Ensuring legal and regulatory compliance is met will help to protect the organisation from any legal liabilities, especially when individuals' health information and other personal identifiable information are at stake. Furthermore, adherence to industry standards helps build trust with stakeholders and present/future customers.

11.1. Compliance Requirements

Description: The organisation needs to understand and comply with the various data protection laws, breach notifications requirements and industry-specific regulations. These compliance requirements vary across countries. If possible, it is recommended to comply with the strictest compliance requirements so that the organisation will comply with all other countries' requirements thereafter. However, this may potentially impact business operations. Organisations need to have an internal discussion to achieve a balance between security and operations.

- **Data Protection Laws:** The organisation needs to comply minimally with national data protection laws where they have operations, but ideally with international data protection laws as well to demonstrate their efforts put into protecting the data of their customers.

- **Breach Notification Requirements:** Similarly to data protection laws, organisations need to comply with breach notification requirements.

- I**ndustry-Specific Regulations:** The healthcare industry is subject to extremely strict cybersecurity regulations because of the sensitive nature of the patients' medical information. Some examples in APAC include the My Health Records Act in Australia and the Health Data Privacy Code in New Zealand. The most known regulations for the healthcare industry would be the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the National Health Service (NHS) Data Security and Protection Toolkit in the United Kingdom.

11.2. Audit and Verification

Description: The audit and verification process ensures that the actions taken by the CSIRT are in compliance with legal and regulatory compliances. Failure to comply will result in financial penalties imposed by the regulatory bodies and loss of reputation in the process.

Example: In a data breach incident, as PHI was leaked, all affected patients must be notified within X hours on what data was lost, how this may impact them and the steps they can take to mitigate damage / the steps the organisation is taking to safeguard other data that have not been leaked. After the incident, the Executive Management hired the audit team to check if the organisations' incident response procedures complied with the new regulations on breach notifications that were just released by the local government.

Cybersecurity Incident Response Plan (CSIRP)

PERFORMED & MAINTAINED THROUGHOUT THE INCIDENT/CRISIS LIFECYCLE

1. Team Structure / Roles and Responsibilities

The team structure / roles and responsibilities identified in the CSIRP includes both the roles listed in the CSIRF and an extended list of roles that aims to further outline the tactical roles and responsibilities to support, coordinate and unify incident response to security incidents. Sections 1.1 to 1.8 are core roles required in the CSIRT. Sections 1.9 to 1.15 describe roles that belong to the Centre of Excellence (COE) and are considered an extension to support the CSIRT during incidents and crises. The difference between a CSIRT and a PSIRT is that the CSIRT is responsible for the organisation's cybersecurity posture, while the PSIRT is responsible for incidents arising specifically from the product. However, for organisations that do not have the manpower to have both a CSIRT and the PSIRT, the CSIRT will may need to take over the role of the PSIRT. Alternatively, the organisation may consider augmenting their internal resources with external retainers (see 1.15) to supplement the CSIRT during incidents / crises.

1.1. Executive Management

- **Role:** Oversight and decision-making authority.
- **Responsibilities:**
  - Approve the CSIRP and ensure it aligns with corporate policies and regulatory requirements.
  - Provide necessary resources and support for incident response activities.
  - Communicate with regulatory bodies, partners, and customers as needed during major incidents.

1.2. Incident Commander

- **Role:** Direct resources and sense making of an incident.
- **Responsibilities:**
  - Lead and coordinate the incident response process.
  - Make strategic decisions on response actions.
  - Coordinate investigation actions to ensure organisation is allocating resources effectively.
  - Ensure resolution of the incident.
  - Conduct post-incident reviews and integrate lessons learned into future response plans.

1.3. Incident Secretariat

- **Role:** Provide administrative, coordination and communication support for the incident response process.
- **Responsibilities:**
  - Bolster information management and apply sense-making for the CSIRT to act effectively.
  - Liaise between the CSIRT and other teams to coordinate incident response.
  - Support Incident Commander in other areas as required.

1.4. Security Analysts (Tier 1)

- **Role:** Triage, reviewing and categorise threats.
- **Responsibilities:**
  - Monitor security alerts and perform initial triage.
  - Perform detailed analysis of the escalated incidents.
  - Respond to incidents and implement measures for containment / eradication / recovery.
  - Escalate incidents to higher severity categories as necessary.
  - Forward potential incidents to Tier 2 analyst for follow-up actions.
  - Document initial findings and actions taken.

1.5. Security Analysts (Tier 2)

- **Role:** Proactive threat hunting; handle complex incidents.
- **Responsibilities:**
  - Proactively search for threats instead of passively waiting for alerts.
  - Manage and resolve high-severity incidents.
  - Analyse threat intelligence and emerging threats and adapt defenses according to the information gathered.

1.6. Threat Intelligence Analysts

- **Role:** Intelligence Sharing; understanding latest threats.
- **Responsibilities:**
  - Analyse latest threats.
  - Contextualise the threats based on attack surface.
  - Identify indicators of compromise (IOCs) and threat actor tactics, techniques, and procedures (TTPs).
  - Update the team on intelligence gathered to ensure the team is prepared for emerging threats and help to prioritise incidents associated with high-risk threats.
  -

1.7. Digital Forensics Specialists

- **Role:** Conduct forensic analysis on the compromised system(s) and data.
- **Responsibilities:**
  - Collect and preserve digital evidence in a forensically sound manner.
  - Assist in root cause analysis and identification.
  - Document findings and be prepared to support the legal team for any potential legal actions.

1.8. IT Infrastructure Specialists

- **Role:** Maintain IT infrastructure and support services.
- **Responsibilities:**
  - Ensure the availability and security of IT systems and networks.
  - Support the deployment of security patches and updates.
  - Assist in containing / eradicating the identified threats.
  - Perform system recovery and restoration to help organisation return to normal operations.
  - Verify that data integrity is maintained after system recovery / restoration.
  - Ensure system backups are available and refreshed constantly in accordance with the organisation's policy.

1.9. Legal and Compliance Officers

- **Role:** Ensure compliance with legal and regulatory requirements.
- **Responsibilities:**
  - Advise on regulatory requirements related to product security and incident response.
  - Manage communication with regulatory bodies.
  - Ensure all incidents comply with applicable laws and regulations.

1.10. Communications and Public Relations Specialists

- **Role:** Manage internal and external communications during incidents / crises.
- **Responsibilities:**
  - Develop and disseminate communication plans and statements.
  - Coordinate public disclosures and media interactions.
  - Advise senior management on all communications as necessary.
  - Ensure consistent and accurate message to stakeholders.
  - Monitor social media and issue statements against any false rumours / allegations that are being spread.

1.11. Risk Management Officers

- **Role:** Identify, assess, mitigate, and monitor risks associated with incidents / crises.
- **Responsibilities:**
  - Identify systemic risks arising from the actions of the Threat Actor and those taken in response to the threats.
  - Conduct risk assessments to identify potential vulnerabilities that may be exploited by threat actors.
  - Maintain and update a risk register regularly that documents the risk, impact, likelihood, and severity.
  - Perform an impact analysis based on the identified risks and breakdown the impacts into categories (e.g., technological, operational, reputational, legal).
  - Advise the potential systemic risks arising from incidents / crises and actions taken during the course of the incidents / crises.

1.12. Human Resource Officers

- **Role:** Manage employee issues and concerns, act as liaison between CSIRT and employees.
- **Responsibilities:**
  - Support in investigations involving employees such as conducting interviews and collating relevant information, especially when an insider threat is suspected.
  - Handles disciplinary actions in accordance with organisation's policies and/or legal requirements.
  - Keep track of employees' safety and status in an incident, ensuring all employees are accounted for in the event of any physical threats or evacuation.
  - Coordinate with internal communications to keep employees updated on incident developments.

1.13. Finance Analysts

- **Role:** Track and manage costs associated with responding to cybersecurity incidents / crises.
- **Responsibilities:**
  - Ensure there are sufficient financial resources allocated to CSIRT and facilitate additional allocation of funds (if required) during an incident or crisis.
  - Track costs directly associated with the incident response (e.g., hiring retainers to conduct forensic analysis).
  - Quantify the financial impact of indirect costs (e.g., service and operational downtime translated into estimated monetary values).

1.14. Stakeholder Management Officers

- **Role:** Provide support to manage stakeholders (internal and external) during incidents / crises.
- **Responsibilities:**
  - Identify stakeholders and their information needs based on the incident that occurred (e.g., customers, board of directors, regulatory bodies, media, public).
  - Develop tailored management plans for different stakeholder groups that address their specific needs and concerns.
  - Foster and maintain trust with stakeholders by being transparent and proactive in notification and communication efforts.
  - Collect and relay customer feedback to the CSIRT to ensure they are aware of the stakeholders' concerns so they can tailor incident response plans accordingly.

1.15. Retainers

- **Role:** Third-party specialists that provide support during incidents / crises and are only activated when needed.
- **Responsibilities:**
  - For organisations that are smaller in size and do not have the manpower to create a fully staffed CSIRT, consider hiring retainers.
  - Retainers could fulfill roles such as Threat Intelligence Analysts, Digital Forensics Specialists, Incident Response Analysts, Public Relations and Crisis Communication Specialists, Legal Counsel, Crisis Operations Advisors etc.
  - Retainers will only be activated when their skillsets are required, thus helping organisations save on the hiring and maintenance costs.

2. Detect

Detecting a cyber incident involves several high-level processes that are designed to detect, analyse and confirm the presence of a security incident effectively and efficiently.

2.1. Monitor

Description: Deploy a suite of tools that will monitor and analyse events as they occur in real-time. Some types of popular used tools include:

- **Security Information and Event Management (SIEM):** SIEM systems are used to collect, analyse and correlate security events in real-time.

- **Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS):** IDS / IPS are used to monitor network traffic for suspicious activities.

- **Endpoint Detection and Response (EDR):** EDR solutions are implemented to monitor and respond to threats on endpoints (e.g., end-user devices such as desktops, laptops, servers, and mobile devices).

2.2. Alert

Description: Configure alerts based to detect anomalies. Define what constitutes normal behaviour and activity for networks, systems, and users in your organisation to serve as a baseline (i.e., reference point to what is normal). Anything that deviates from these baselines are indications of potential incidents.

Example: The system detected a user attempting to send out a zip file that is 4GB large at 3am in the morning.

2.3. Logic Applied

Description: The CSIRT team needs to correctly interpret data and alerts by understanding their respective business processes. Correlating data from multiple sources such as network traffic and endpoint activities to identify patterns is helpful to direct sense making to reduce the occurrences of false positives.

Example: High data transfer rates done at 1am might be seen as a potential incident, but when cross-referencing data from multiple sources, it is made known that there is a backup operation scheduled to occur outside of office hours, so this may be a false positive after all.

3. Respond

Response procedures have the objective of mitigating the impact caused by the incident. In this phase, the Incident Commander leads the response efforts by the CSIRT (i.e., Security Analysts, Threat Intelligence Analysts, IT Infrastructure Specialists) with the Incident Secretariat offering support in administration, communication, and coordination areas. The Centre of Excellence (CoE) will each step up and prioritise their attention towards the incident response process as well.

3.1. Triage

Description: To effectively manage incidents as they occur, it is crucial to assess and prioritise the incidents that pose the greatest risk to the organisation. This is done by performing a triage. A triage is the process of evaluating and prioritisation of security alerts or incidents based on their severity, impact, and urgency. The process helps allocate resources effectively to ensure there are timely responses to the more critical incidents.

- **Severity Levels**

Description: Severity levels in incident response are critical for determining the urgency and extent of response efforts. One good industry accepted reference can be found in NIST 800-61r3 where severity levels are classified into four categories: Low, Medium, High, and Critical.

- **Low**

  Incidents with minimal impact, such as unsuccessful phishing attempts or benign malware, require limited response and resources. They can typically be addressed during regular operations without urgency.

- **Medium**

  These incidents have noticeable effects, potentially exposing non-critical data or disrupting some functions. They require prompt attention to prevent escalation and further impact.

- **High**

  Incidents causing significant disruptions or data breaches demand urgent and coordinated response efforts. Quick mitigation is essential to minimise damage and restore operations.

- **Critical**

  The most severe incidents, such as major cyber-attacks or large-scale data breaches, cause catastrophic damage. An immediate, comprehensive response is crucial to contain the impact and protect the organisation.

Medical Device manufacturers can define their own levels of severity, but each level needs to be unique and measurable to help with the prioritisation of incidents based on their potential impact on an organisation's operations, assets, and reputation.

- **Incident Categories**

Description: Defining incident categories is essential for standardising incident response procedures and ensuring consistent communication across the organisation. One good industry accepted reference can be found in NIST 800-61r3 where incident categories include scheduled penetration tests (recorded under Scans/Probes/Attempted Access") which are good to be tracked to allow for a more complete study of breach trends. The suggested incident categories are Unauthorised Access, Denial of Service, Malicious Code, Inappropriate Usage, and Scans/Probes/Attempted Access.

- **Unauthorised Access**

  Incidents where systems or data is accessed without explicit authorisations and approvals. This category includes scenarios like hacking attempts and insider threats where data is accessed without proper authorisation.

- **Denial of Service (DoS)**

  Attacks aimed at disrupting the availability of services or systems. DoS incidents can range from overwhelming a server with traffic to exploiting vulnerabilities that cause system crashes.

- **Malicious Code**

  Incidents involving the presence or use of malicious software such as viruses, worms, Trojan horses, ransomware, and spyware. This category covers a wide range of malware-related issues.

- **Inappropriate Usage**

  Instances where employees or users misuse their access to systems in a manner that violates organisational policies. This includes activities such as viewing inappropriate content or using systems for personal gain.

- **Scans/Probes/Attempted Access:**

  This category includes activities like network scanning, probing for vulnerabilities, or attempting to access systems without success. While these activities may not always lead to a breach, they are important to track as they can indicate potential threats.

Incident Categories helps prioritise and allocate resources effectively based on the nature of incidents, allowing for a focused and efficient response. Additionally, clear and unique categorisation facilitates compliance with regulatory requirements and supports continuous improvement through trend analysis and lessons learned.

3.2. Escalation

Description: Clear guidelines need to be established for when and how to escalate an incident. The Incident Commander will make the executive decision on escalations. Incidents are escalated to crises when there are significant impacts to business operations, and this is when senior management and relevant stakeholders will be fully involved in the response processes.

- **Technical Complexity**

Based on the complexity of the incident, the incident should be escalated to higher support levels (from Tier 1 to 2) if the lower tier analyst is unable to handle it. Specialised teams (e.g., legal, cybersecurity subject matter experts) should be contacted if internal analysts are unable to handle the incident.

- **Escalation to Crisis**

Incident is escalated to crisis once an incident reaches the predefined severity level (e.g., High) or if it breaches the business impact threshold (affected service downtime is estimated to cost >$100,000). Executive management and relevant stakeholders need to be involved to make executive decisions.

- **Regulatory Bodies**

Reporting incidents to regulatory authorities as required by law or industry regulations (e.g., GDPR, HIPAA).

- **Law Enforcement**

Engage law enforcement agencies for incidents involving criminal activities such as cybercrime or data theft.

- **Third-Party Vendors**

Contact third-party service providers or partners if the incident affects or involves their systems or services / if the incident is identified to be a supply chain attack.

Example: The SIEM reported potential unauthorised access and the CSIRT team responded accordingly. After the triage process, they confirmed it was not a false positive incident. The detection tool then detected sensitive information (e.g., contractual information) was accessed and confirmed it had been leaked. The Incident Commander marked the incident severity to "Critical" as the business impact of the designs were leaked (high business impact + high urgency factor). This incident is also escalated to a crisis as the estimated business impact costs is over >$100,000.

3.3. Incident Reporting

The reporting can be done by using the tools listed in the section below and by following the communication plans for internal / external communication. Depending on the severity and impact of the incident, the organisation may choose to escalate the incident through a more direct channel (e.g., direct call instead of sending notifications via apps, which may be easily overlooked).

Reporting Tools

- **Description:** There are a multitude of tools available to help facilitate reporting. While they are not compulsory, they provide immense benefits of notifying the relevant parties timely, logging and documentation of the incident and help with the communication within the organisation that will help bring the incident under control effectively.

- **Incident Reporting and Notification Tools:** The tools in this category are primarily used to notify relevant stakeholders and to escalate incidents as needed. They provide automated alerting and escalation based on predefined rules.

- **Security Information and Event Management (SIEM) Systems:** SIEM systems provide a centralised platform for monitoring, identifying and responding to incidents. The systems generate alerts and reports after a potential incident has been identified.

- **Ticketing and Workflow Management Tools:** These tools assist in managing the workflow of the incident response activities, enabling teams to assign tasks and track the completion progress of each task.

- **Incident/Crisis Management Systems:** These tools help to centralise coordination and communication efforts, automatically track incidents, aid in deploy resources and offer a secure repository of all event-related information. Through these features, they support post-incident analysis and reporting, enabling medical device manufacturers to learn from incidents and improve future response strategies.

3.4. Communication

The CSIRT could consider integrating the use of the Traffic Light Protocol (TLP) 2.0 to control the dissemination of information. The CSIRT could also look into using VERIS (Vocabulary for Event Recording and Incident Sharing) for the uniform and consistent communication of incident / crisis related details. VERIS uses a set of metrics designed to provide a common language to describe security incidents in a structured and repeatable manner.

Internal Communication

Description: Keep all internal stakeholders informed about the incident status, actions taken, and next steps. Respective managers will take over and manage employees that are most affected by the incident to see if there are any alternative solutions they can use to perform their job. Multiple channels should be prepared in the event one channel is down, there are other means to reach out to the employees. Alternative bands of communication should not belong to the same family of applications (e.g., Microsoft 365) to ensure communications are robust to single points of failures. Some channels include:

- Email
- Secure Messaging Apps
- Incident Management Systems
- Internal Portals
- Meetings (Virtual or in-person)
- SMS
- Push notifications
- Phone calls

Employees must be aware of the alternative communications channels if the primary channel used is down. Employees are also required to report any development they notice on the ground so that the CSIRT can respond timely; this can be done through a reporting channel direct to the CSIRT.

External Communication

Description: External communications are conducted to assure external stakeholders that the organisation is aware of the incident and is currently handling it. It is imperative to maintain itself as the single source of truth and to control the narrative. If required, regulatory bodies and/or law enforcement need to be informed as well. Communication can be done through a variety of channels:

- Dark site
- Corporate Websites
- Secured Instant Messaging
- Media Conferences
- Social media
- Email
- Phone calls

Example: During an incident, the Incident Commander uses the SIEM system as a dashboard to monitor the incident response process and reallocates resources as required. Following the communication plan, SMS notifications are sent to all employees to inform them of the situation. Thereafter, the employees will each assume their assigned roles and responsibilities and help to mitigate the impact of the incident. Stakeholder Management Officers also follow external communication plans to reach out to affected stakeholders to update them about the situation. Communications and PR Specialists crafted a press release and published it to take control of the narrative to prevent rumours from forming.

3.5. Containment Strategies

Description: Immediate measures that must be taken to contain the incident to prevent further spread and impact.

- **Access Control:** Strengthen access controls temporarily and implement stricter rules. This could be enforcing multi-factor authentication (MFA), having a shorter automatic logout timer, tightening firewall rules, and restricting remote access.
- **Halting Change Requests:** Temporarily stopping all modifications and updates to systems and applications to maintain stability, prevent further vulnerabilities, and focus resources on managing and mitigating the attack.
- **Network Segmentation:** Implement network segmentation to isolate affected systems from the rest of the network. This might involve moving affected systems to a separate VLAN or if necessary, physically disconnecting them.
- **Quarantine Devices:** Quarantine infected or compromised devices. For example, if a workstation is infected with malware, disconnect it from the network immediately. If this cannot be done, manually apply a force shutdown to the devices.
- **Monitor Isolated Systems:** Continue to monitor isolated systems for any signs of ongoing malicious activity to ensure containment is effective. This can be done by using SIEM tools.

3.6. Eradication

Description: Once the incident has been contained, the next steps will be to identify the root cause of the incident and to eradicate the threat.

- **Identify the Root Cause:** Conduct a thorough forensic analysis to identify the root cause of the incident. Determine how the incident occurred, what vulnerabilities were exploited, and what the attack vectors were; attack vector refers to the method used by the attacker to exploit system vulnerabilities.
- **Eliminate the Threat:** Neutralising malicious activities or software, which can be done using tools such as antivirus software, intrusion detection systems (IDS), firewalls, and endpoint detection and response (EDR) solutions.
- **Patch and Update:** Apply patches and updates to fix vulnerabilities that were exploited. This might include mandatory software / firmware patches.

Example: To respond to an unauthorised access being detected, the Incident Commander coordinates with the Security and Threat Intelligence Analysts to get a better understanding of the threat actor's motivation and objective. During this time, the Incident Secretariat helps to coordinate information exchange between the CSIRT core team and the CoE, which enables Legal and Compliance Officers and Communications and Public Relations Specialists Officers to start preparing their responses as well.

4. Recover

Systems need to be restored back to normal. During this step, it is crucial to ensure that data integrity is maintained, and that no residual malware remains embedded in the system. The Incident Commander oversees and coordinates the recovery process while the Incident Secretariat monitors the progress and updates the other members of the CSIRT and CoE of any updates.

- **Data Validation:** Validate the integrity of data before restoring it to ensure that it has not been tampered with or corrupted. This may involve comparing with backups, checksums, or using other validation techniques.
- **System Clean-up:** Ensure that affected files / systems are eradicated securely, ensuring no backdoors or malicious accounts remain.
- **Service Restoration:** Gradually bring systems and services back online. Monitor the behavior closely to detect any signs of residual / persistent threats.
- **Post-Restoration Monitoring:** Continue to monitor systems closely after restoration to ensure that operations and services are functioning as normal. Report any unexpected fluctuations as they may be indications of re-occurring threats.

Example: After the incident of an unauthorised access, the Incident Commander works with the IT Infrastructure Specialists to ensure that the systems are successfully restored, and thorough testing is performed to ensure systems are clean of any residual malware. The Forensics Analysts will ensure all evidence collected is preserved in a sound manner for use in legal proceedings (if any). Legal and Compliance Officers ensure that the recovery time and progress complies with industry regulations. This is crucial as in the healthcare industry, tolerance for system downtime may be strict and the organisation may face heavy penalties if the systems do not recover in time. Communications and Public Relations Specialists will continue to update relevant stakeholders on the recovery process.

5. Evidence Collection and Preservation

Description: It is critical to ensure evidence is collected and preserved in a forensically sound manner to maintain its integrity. This to ensure that investigations can be done effectively and that any findings can be used in legal proceedings.

- **Forensic Imaging:** Create a forensic image by capturing an exact copy of the system bit by bit, including deleted files and unallocated space etc.
- **Volatile Data Capture:** Collect volatile data before systems are turned off (e.g., RAM, running processes, network connections)
- **Write Blockers:** Use hardware or software write blockers to prevent any unintended / intended modifications to the system
- **Hash Digital Evidence:** Create a hash value for all digital evidence collected using industry standard hash algorithms (e.g., SHA-256). The hash will be used as additional evidence to demonstrate that integrity is maintained.
- **Preserve Media:** Store evidence on read-only media to prevent any accidental modifications and store the media in a secure location.
- **Chain of Custody:** Maintain a chain of custody log for all evidence collected. This log should detail who collected the evidence, when and where it was collected, how it was stored, and who had access to it throughout the incident's lifetime. Ensure that evidence is stored securely to prevent tampering, loss, or unauthorised access. Failure to do so may invalidate the evidence in legal proceedings.

Example: The Digital Forensics Analyst documents the chain of custody on the hard drive that was collected in an unauthorised access incident, detailing who had access to it and what was done as the hard drive changed hands. A write blocker USB is used to prevent any accidental modifications to the hard drive before the forensic image process begins. A hash value is created to demonstrate that the evidence’s integrity is maintained. All evidence collected is stored on a write-only media and is carefully protected in a secure storage area.

6. Documentation

Description: The documentation process occurs at every step of the incident response processes and ensures all actions taken are recorded in detail. The documentation will be used during post-incident review to improve future incident responses

Incident Logging: Document the initial detection of the incident, including the following details:

- Date and time
- Person who reported it
- Type of incident (e.g., ransomware, data breach)
- Systems affected
- Severity of the impact
- Observed indicators of compromise (IOCs)

- **Timeline of Events:** : Maintain a detailed timeline of how the incident unfolds and all actions taken from the initial detection through the resolution of the incident. Ensure timestamps are recorded for all actions to illustrate a clear sequence of events.
- **Actions Performed:** Document all actions taken and decisions made by all parties involved (CSIRT, IT Operations, Senior Management). Include details on who performed each action and when.
- **Communications Log:** Record all communications related to the incident, both internal and external. Include timestamps for all decisions made (e.g., decision made to force shutdown servers to prevent spread of ransomware).

Example: An employee reported unusual activity on their account. The reporting and unusual activity was recorded and reported as a suspected breach. Any changes made by this employee's account for the past 24 – 48 hours were recorded. Subsequent developments by the CSIRT were all documented and timestamped as well to establish a clear timeline of events.

7. Post-Incident Analysis

7.1. Lessons Learned

Description: Executive Management must take the lead and demonstrate that they are serious in conducting a post-incident analysis to improve existing incident response plans. Key weaknesses must be identified and addressed to prevent the occurrence of similar incidents in the future. Ensure that all the key points are disseminated within the whole organisation so that all employees know how to respond better to future incidents.

7.2. Continuous Improvement

Description: The following are strategies that can be executed to incorporate lessons learned to reduce Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR):

- Policy updates
- Providing additional training to employees
- Upskilling technical skills of CSIRT / IT teams
- Enhance / Upgrade existing tools and/or technologies
- Hire additional team members with specific skillsets that are absent from the current team
- Outsource certain tasks to external vendors (i.e., forensics investigation team)
- Hiring retainer services to be activated specifically during a crisis (e.g., crisis operations advisor to guide the senior management through the whole incident lifecycle)

Example: It was determined that the cause of the unauthorised access was due to an unpatched vulnerability on an endpoint device because the employee did not restart his computer and kept it in a perpetual hibernate state. Executive Management created a new policy that all systems must be shut down at the end of each working day for updates to take place. All employees must complete an additional e-learning module on the dangers of not updating their systems in time, especially in a medical device manufacturing organisation where there are proprietary blueprints that many competitors are after.

8. Review and Update

Description: After the post-incident review, it is crucial not to conclude the incident response without a clear plan on how and when the existing incident response plan will be updated.

- Clearly assign the action items to the respective teams and establish a deadline for the completion.
- Perform regular follow-ups to check ensure there is progress on the updates and that the changes are not "swept under the rug" as business operations revert to normal.
- Maintain version control for all documentation to track changes and how the incident response plan has evolved over time.

Example: HR was assigned to keep track of employees' progress on completing the e-learning module. IT Infrastructure Specialists also closely monitored to see which endpoint device has yet to be updated and work with HR to identify these employees. HR reports back to Executive Management on uncooperative employees and there was a suggestion to induce a penalty for those that do not complete the module by a specified date.

9. Legal and Regulatory Compliance

9.1. Compliance Requirements

Description: The organisation needs to understand and comply with the various data protection laws, breach notifications requirements and industry-specific regulations. These compliance requirements vary across countries. If possible, it is recommended to comply with the strictest compliance requirements so that the organisation will comply with all other countries' requirements thereafter. However, this may potentially impact business operations. Organisations need to have an internal discussion to achieve a balance between security and operations.

- **Data Protection Laws:** The organisation needs to comply minimally with national data protection laws where they have operations in (e.g., Singapore: Personal Data Protection Act; South Korea: Personal Information Protection Act), but ideally with international data protection laws (e.g., European Union: General Data Protection Regulation) as well to demonstrate their efforts put into protecting the data of their customers.
- **Breach Notification Requirements:** Similarly to data protection laws, organisations need to understand breach notification requirements to comply with. This includes the following:
- **Notification threshold:** What are the conditions that would trigger the organisation to send a notification?
- **Timeline:** How long after breach to notify (e.g., within one hour of data breach, within one day?)
- **Notification Content:** What needs to be included in the notification (e.g., what was breached, what is the potential harm it may cause to the impacted individuals, what measure are being taken to mitigate the damage?)
- I**ndustry-Specific Regulations:** The healthcare industry is subject to extremely strict cybersecurity regulations because of the sensitive nature of the patients' medical information. Conduct audit and verification checks to ensure compliance is met.

9.2. Audit and Verification

- **Planning and Preparation:** Define the scope of the audit and establish specific objectives. Select a team with the necessary expertise to perform the audit and ensure the relevant stakeholders are cooperative with the audit team.

  Example: The audit is to check for compliance with the Heath Data Privacy Code in New Zealand. The team assembled to perform the audit must have knowledge and experience in reviewing policies related to this code. Senior management should help to send an internal email to inform staff that their cooperation is vital for the audit to be completed in a timely manner and successfully.

- **Review of Policies and Procedures:** The audit team will verify the incident response policies (e.g., playbooks) to ensure that they meet legal, regulatory, and industry-specific requirements.

- **Report and Documentation:** The audit team will document all findings and present it to the senior management and other stakeholders for review and discussion. An action plan should be included to inform the stakeholders what needs to be done to meet the compliance requirements.

  Example: The Health Data Privacy Code released an updated version to regulate the use of patient data on AI tools, citing concerns on potential data leaks. An external audit team was hired to verify incident response procedures to comply with the update and state remediations that need to be done (if any).

Example: In a data breach incident, as PHI was leaked, all affected patients must be notified within X hours on what data was lost, how this may impact them and the steps they can take to mitigate damage / the steps the organisation is taking to safeguard other data that have not been leaked. After the incident, the Executive Management hired the audit team to check if the organisations' incident response procedures complied with the new regulations on breach notifications that were just released by the local government.

10. Sample Scenario

This sample scenario will use ransomware as a cyber incident to demonstrate the flow of the CSIRP:

Detect

The SIEM detected a potential incident. The Tier 1 Security Analysts responds to this immediately and conducts a triage to verify the validity of the alert. The Threat Intelligence Analysts started to check if there are any threat actors active in the region recently. Through incident reporting tools, the CSIRT received a screenshot from an employee and confirms a ransomware attack has occurred. The employee's laptop is connected to the company servers, which host critical design files and patient data. The laptop has been fully encrypted, and the ransomware is spreading to the servers at a rapid speed. The Tier 1 Analyst records the incident as Severity Level as "Severe" and Incident Category as "Malicious Code"

Respond

As the business impact is significant and exceeds the business threshold, the Incident Commander escalates this to a Crisis and notifies CoE and Executive Management. The Security Analysts continue to work together with the Digital Forensics Specialist and IT Infrastructure Specialists to determine the scale of the ransomware attack and to check if any data has been leaked. Following containment strategies, the Incident Commander recommends to Executive Management to invoke "Draw Bridge" protocol to decouple the network from regional offices in an attempt to contain the spread. The Tier 1 and 2 Security Analysts work together with IT Infrastructure Specialist to start eradication procedures to remove the ransomware.

The Incident Secretariat reaches out to the Legal and Compliance Officers to understand what legal implications are involved in this incident. Following the prepared communication plan, the Communications and Public Relations Specialists begin to craft public statements and press releases for Executive Management to address all stakeholders affected. HR Officers help to manage internal communications and IT begins searching for spare laptops for affected employees. Stakeholder Management Officers are assembled and begin to work closely with Communications and Public Relations Specialists await calls to communicate with external stakeholders after the information embargo is lifted. Finance Analysts start to quantify the financial costs of the damage the ransomware costs (i.e., service downtime, data recovery efforts).

Recover

After investigations, aside from encrypted endpoints, IT Infrastructure Specialists determined that 25% of the data in their cloud-based SharePoint was encrypted. The Incident Commander starts the recovery process, and the Incident Secretariat helped to monitor the recovery process and liaise with the other members of the CSIRT and CoE. The Digital Forensics Specialist ensured all evidence collected during the incident response is preserved in a forensically sound manner by using write-blockers and/or hashes.

Post-incident, the Incident Commander briefed the Executive Management and reported that the incident happened due to a zero-day vulnerability, as mentioned in a Spot Report sent by their cloud vendor. Legal and Compliance Officers begin deliberations on possible lawsuits against the vendor. Executive Management noted that the initial triage phase could had been done simultaneously while reaching out to the affected employees; in this incident, the employee reached out first to report the incident while the CSIRT team was investigating if the incident was a false positive. The Incident Commander acknowledges this and adds this into part of the incident response process.

Executive Management also decides to hire third-party auditors to ensure that the current incident response plan meets local, regional, and industry-specific regulatory requirements. Executive Management issued an organisation-wide notice to inform all employees to be cooperative with the auditors. Executive Management also noted the "fog-of-war" was thick and present amongst leaders and noted to investigate the onboarding of "Crisis Operations Retainers" to advise and assist the Chair of the Crisis Management Team (CMT) to pilot the CMT through the crisis.

Authors & Contributors

APACMed Secretariat

Su Fen Ong
Lead, Health Data & AI, APACMed

Authors

Leonard Koh
Head, Crisis Operations and Training, Ensign InfoSecurity, CISA, CDPSE, OXELP

Yeo Quan Ren
Consultant, Crisis Operations and Training, Ensign InfoSecurity, MSc, MBA

Contributors

Asok Kumar Raghavan Nair
Quality and Regulatory Director, Global Strategic Regulatory Affairs, Abbott

Jagathesh Rajavasagam
Risk and Cybersecurity Officer, APAC, Abbott

James Chan
Regulatory Affairs Director, APAC, Varian Medical Systems

Joern Lubadel
Global Head of Product Security, B. Braun Group

Juan Gomez
Regional ICT Director, APAC, Terumo

Paul Chua
Cybersecurity Officer, Greater Asia, BD

Stefan Gentsch
Cybersecurity Officer, Asia Pacific, Siemens Healthineers

About Ensign

Ensign InfoSecurity is the largest comprehensive cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Their core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is in-house research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

APACMed
The voice of MedTech

About APACMed

The Asia Pacific Medical Technology Association (APACMed) represents manufacturers and suppliers of medical equipment, devices and in vitro diagnostics, industry associations, and other key stakeholders associated with the medical technology industry in the Asia Pacific region. APACMed's mission is to improve the standards of care for patients through innovative collaborations among stakeholders to jointly shape the future of healthcare in Asia-Pacific. For more information, visit **www.apacmed.org**