

INCIDENT RESPONSE CHECKLIST

Incident Response Checklist

Change History Log

Version Number	Release Date
1.0	15 March 2021
2.0	23 April 2021

Incident Response Checklist

Incident response can be stressful, especially when the incident is severe and business operations are disrupted. Having a robust incident response plan ready before an incident can help organisations quickly and more effectively contain threats and recover, instead of only reacting when the incident happens and trying to make plans on the fly. An incident response plan which has been thought through and rehearsed beforehand is key to containing the incident and limiting the damage and disruption to business operations.

This *Incident Response Checklist* is structured around the IPDRR (Identify, Protect, Detect, Response, Recover) framework developed by the U.S. National Institute of Standards and Technology (NIST), and is intended to guide organisations in preparedness, response and recovery to cyber incidents.

Broadly, there are four stages to an incident response plan:

1. Preparations	
Preparations for an incident response is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks and applications are sufficiently secure.	
Preparing to handle incidents	Identify key contact information <ul style="list-style-type: none"> <input type="checkbox"/> Designate an incident response handler within your organisation <input type="checkbox"/> Appoint a third-party incident response provider <input type="checkbox"/> Contacts for product/service vendor(s) <input type="checkbox"/> Regulatory bodies <input type="checkbox"/> Law enforcement agencies <input type="checkbox"/> SingCERT <input type="checkbox"/> Clients <input type="checkbox"/> Others: _____
	Identify investigation resources <ul style="list-style-type: none"> <input type="checkbox"/> List of key assets and data and where they are located/hosted <input type="checkbox"/> Network diagrams <input type="checkbox"/> Current baseline of IT systems' activities <input type="checkbox"/> Documentation of IT systems and software versions <input type="checkbox"/> Back-ups of important data <input type="checkbox"/> Others: _____
	Develop the relevant plans <ul style="list-style-type: none"> <input type="checkbox"/> Prevention and detection plans <input type="checkbox"/> Containment, eradication and recovery plans <input type="checkbox"/> Crisis management and communications plan <input type="checkbox"/> Business continuity plans <input type="checkbox"/> Others: _____

Incident Response Checklist

Preventing incidents	<p>Identify and understand the type of attacks that could affect your organisation. Develop action plans to deal with each type of attack</p> <ul style="list-style-type: none"> <input type="checkbox"/> Malware <input type="checkbox"/> Phishing <input type="checkbox"/> Distributed denial of service <input type="checkbox"/> Ransomware <input type="checkbox"/> Data breach <input type="checkbox"/> Data corruption <input type="checkbox"/> Others: _____
Communicating and exercising the plans	<p>Action plans developed to respond to common incidents should be accessible and any updates should be communicated to relevant parties (e.g. employees, etc.).</p> <ul style="list-style-type: none"> <input type="checkbox"/> Communications with the employees and key stakeholders <input type="checkbox"/> User awareness and training <input type="checkbox"/> Regular reviews and updates of plans (e.g. when systems are onboarded, new hires, or at regular scheduled intervals) <input type="checkbox"/> Walk-through/exercise the plans <input type="checkbox"/> Others: _____
<p>2. <u>Detection and Analysis</u> Detection and analysis of an incident is the first step to identifying an incident and understanding its impact and severity.</p>	
Recognising possible attack vectors	<p>Organisations should generally be prepared to handle any incident but focus should be on being prepared for incidents that use common attack vectors, such as:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Poorly designed web applications <input type="checkbox"/> Misconfigured systems <input type="checkbox"/> Internet downloads <input type="checkbox"/> Poor cyber hygiene practices (e.g. use of weak or default passwords, use of outdated software, etc) <input type="checkbox"/> Human lapses <input type="checkbox"/> Authorised third parties <input type="checkbox"/> Others: _____
Reviewing possible sources of precursors and indicators	<ul style="list-style-type: none"> <input type="checkbox"/> Security software (e.g. Intrusion Detection Systems [IDS], Security Information and Events Management System [SIEM], anti-virus software, third party monitoring services etc) <input type="checkbox"/> Logs (e.g. operating system logs, service and application logs, network device logs, netflow logs etc) <input type="checkbox"/> Publicly available information (e.g. SingCERT alerts, alerts from products/services vendors on vulnerabilities, etc) <input type="checkbox"/> People from within your organisation <input type="checkbox"/> Others: _____

Incident Response Checklist

<p>Making an initial assessment and prioritising the next steps</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Correlate events against the baseline to determine if an incident has occurred <input type="checkbox"/> Check incidents against known threats precursors and indicators <input type="checkbox"/> Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch <input type="checkbox"/> Prioritise the incident handling activities, including whether to activate crisis management, and crisis communications plans <input type="checkbox"/> Others: _____
<p>Gathering evidence</p>	<p>Evidence gathering may serve two purposes – incident resolution and legal proceedings. Some of the evidence that need to be documented include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Summary of the incident <input type="checkbox"/> Incident indicators <input type="checkbox"/> System events <input type="checkbox"/> Actions taken during the incident <input type="checkbox"/> Logs of affected systems <input type="checkbox"/> Forensic copies of affected systems <input type="checkbox"/> Others: _____
<p>Knowing your Stakeholders and/or Fiduciary Obligations</p>	<p>Notify relevant stakeholders and affected parties</p> <ul style="list-style-type: none"> <input type="checkbox"/> Board of Directors <input type="checkbox"/> Regulators, law enforcement and other government agencies (SPF, PDPC, CSA, SGX etc.) <input type="checkbox"/> Clients <input type="checkbox"/> Media <input type="checkbox"/> Others: _____
<p>3. <u>Containment, Eradication & Recovery</u></p> <p>This is one of the most critical stages of incident response. The strategy for containment and recovery is based on the information and indicators of compromise gathered during the analysis phase. The threat needs to be thoroughly eradicated before normal operations can resume to minimise subsequent repeated disruptions.</p>	
<p>Developing a Containment Strategy</p>	<p>Containment strategies vary depending on the type of incident, and a strategy should be developed for different incident types to contain the incident and minimise damage. Some of the more common strategies are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Isolate all or parts of the compromised network by disconnecting all affected systems <input type="checkbox"/> Re-route or filter network traffic <input type="checkbox"/> Firewall filtering <input type="checkbox"/> Close vulnerable ports and mail servers <input type="checkbox"/> Block further unauthorised access to the system <input type="checkbox"/> Others: _____

Incident Response Checklist

Eradicating the threat	<p>After containing the incident, eradication may be necessary to eliminate all traces of the incident. This includes:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Wiping out the malware <input type="checkbox"/> Disabling breached user accounts <input type="checkbox"/> Patching vulnerabilities that were exploited. This should be applied to all affected hosts within the organisation <input type="checkbox"/> Others: _____
Taking steps towards recovery	<p>This may entail:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Restoring systems from backups <input type="checkbox"/> Rebuilding systems from scratch <input type="checkbox"/> Changing passwords (both administrators and users) <input type="checkbox"/> Tightening network perimeter security <input type="checkbox"/> Confirming the integrity of business systems and controls <input type="checkbox"/> Others: _____
Monitoring and maintaining vigilance	<ul style="list-style-type: none"> <input type="checkbox"/> Continue to monitor the network for any anomalous activity or signs of intrusion <input type="checkbox"/> Depending on the incident, organisations may need to consider higher levels of system logging or network monitoring <input type="checkbox"/> Others: _____
<p>4. <u>Post-Incident Review</u></p> <p>Organisations should proactively review their plans and response activities to identify and resolve deficiencies and strengthen their security posture.</p>	
Conducting post-incident review	<ul style="list-style-type: none"> <input type="checkbox"/> Identify and resolve deficiencies in systems and processes that led to the incident <input type="checkbox"/> Identify and resolve deficiencies in planning and execution of your incident response plan <input type="checkbox"/> Assess if additional security measures are needed to strengthen the security posture of your organisation <input type="checkbox"/> Communicate and build on lessons learnt <input type="checkbox"/> Others: _____

Incident Response Checklist

REFERENCES

- The United States Department of Commerce, National Institute of Standards and Technology (April 2018), *Framework for Improving Critical Infrastructure Cybersecurity*. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- The United States Department of Commerce, National Institute of Standards and Technology (August 2012), NIST *Special Publication 800-61 Rev2. Computer Security Incident Handling Guide*. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- The United States Department of Justice (September 2018), v2.0. *Best Practices for Victim Response and Reporting of Cyber Incidents*. <https://www.justice.gov/criminal-ccips/file/1096971/download>
- CREST Version 1 (2013). *Cyber Security Incident Response Guide*.