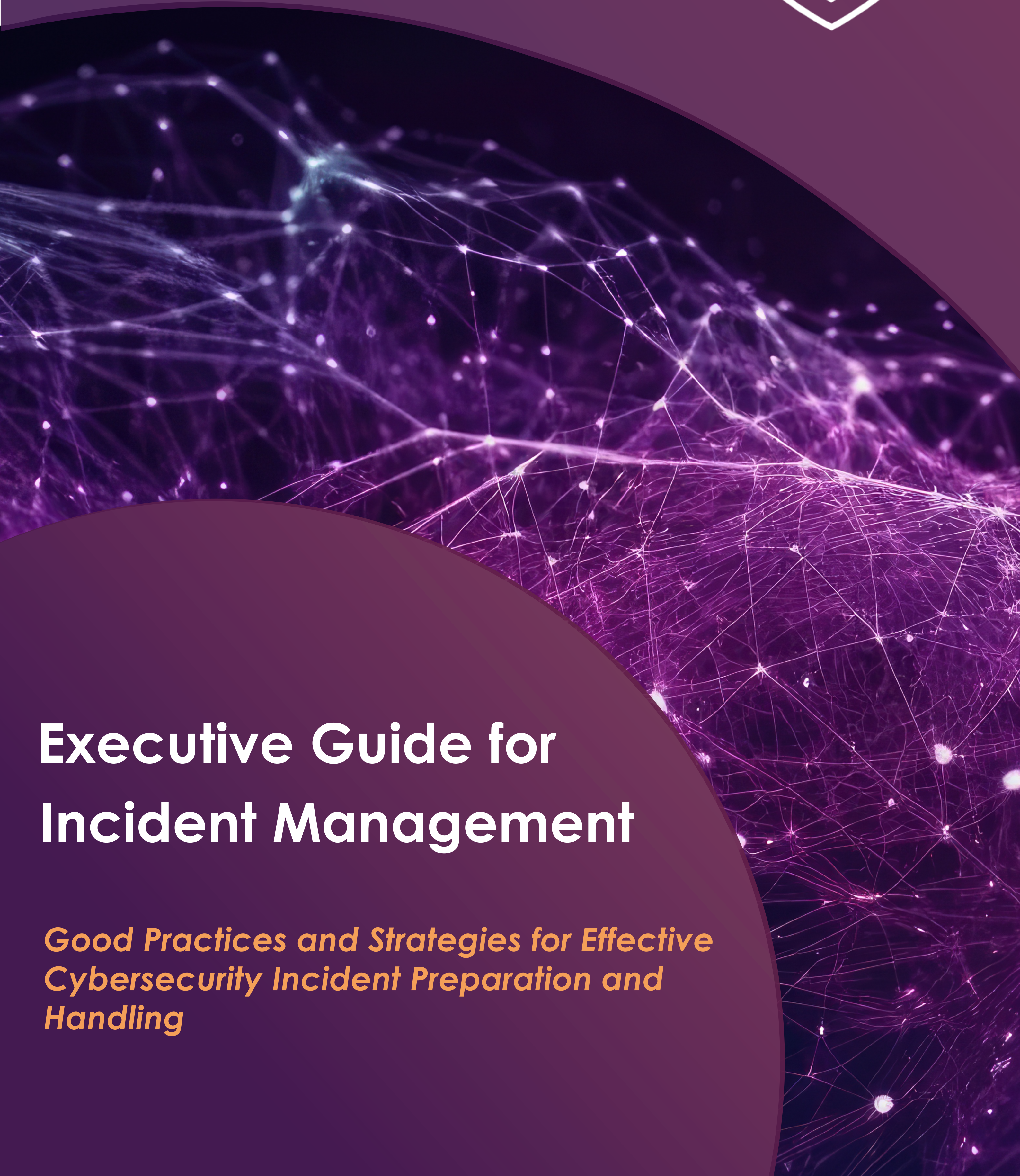


Executive Guide for Incident Management

Good Practices and Strategies for Effective Cybersecurity Incident Preparation and Handling

INTRODUCTION

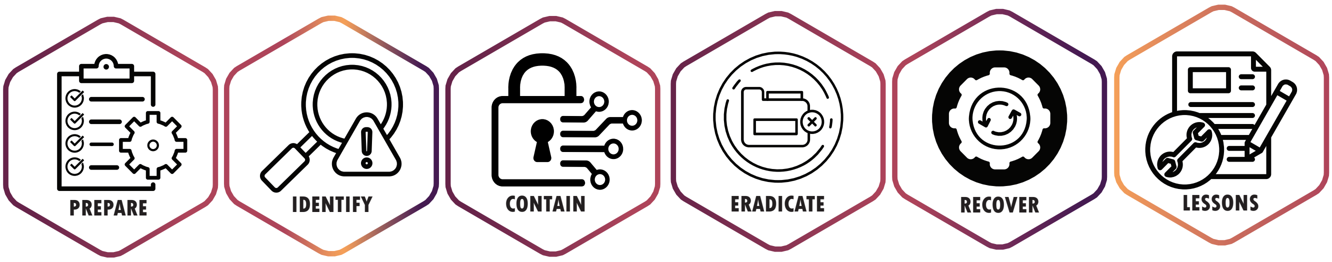
Cybersecurity is an ever-evolving landscape, and as leaders in your organization you understand the critical role that technology plays in today's business environment. With the increasing frequency and sophistication of cyberattacks, it is not a question of ‘if’ your organization will face a cyber incident, but ‘when’. When that time comes, how you have prepared and how you respond can make all the difference in minimizing damage, protecting your organization, and ensuring cybersecurity resiliency.

PURPOSE

The Executive Guide for Incident Management will provide a comprehensive high-level overview of good practices to follow in preparation for and during a cyber incident. This guide will equip executives and decision-makers with the knowledge and strategies necessary to confidently navigate incident management.

AUDIENCE

The Executive Guide for Incident Management is a non-technical document tailored for executives, board members, and senior leaders who play a pivotal role in making strategic decisions related to incident management.



IN-SCOPE

- Description of good practices.
- High-level strategies.
- Tips and suggestions.
- Checklists.

OUT-OF-SCOPE

- Troubleshooting the attacks.
- Attack specific remediation.
- How-to material/guides.
- All-encompassing solutions and practices.
- Technical guidance for cybersecurity concerns.

PREPARATION

The best way to handle an incident is to prevent it from happening in the first place. This can be aided by establishing and adhering to cybersecurity policy instruments and implementing preventative measures. However, incidents are bound to occur, thus organizations should proactively develop, maintain, and disseminate information on incident response and planning.

RACI MATRIX

	IT Teams	CISO	CEO	Users
Prepare	R	A	I	-
Identify	R/A	C	C	R/A
Contain	R	C	I	I
Eradicate	R/A	I	I	-
Recover	R/A	I	I	-
Lesson Learned	R/A	C	I	C

Critical Contacts Card

Incident Response Team: ______________

Phone Number: (___) - ___ - ____

CIO/CISO: ______________________________

Phone Number: (___) - ___ - ____

Communication Team: ________________

Phone Number: (___) - ___ - ____

Other Contacts: ______________________

Phone Number: (___) - ___ - ____

CHECK LIST

Governance

There should be high-level support within the organization to establish policies surrounding cybersecurity and the protection of information assets.

- □ Executive support
- □ Policies, standards, & procedures

Plans and Procedures

Methods to report incidents should be developed proactively and be easy to use. There should be procedures in place to return the business to normal operations after a disaster or incident has occurred.

- □ Incident response plans and reporting methods.
- □ Business Continuity Plan (BCP)
- □ Disaster Recovery Plan (DRP)

Communication

The contact information of key individuals/ stakeholders should be pre-established. This information should be easily identifiable and accessible in the event of an incident.

- □ Emergency communication plan
- □ Staff training on incident response procedures
- □ Security Oversight Committee
- □ Communication phone tree

TIP!

Developed plans and procedures should be continuously tested at pre-determined intervals.

IDENTIFY

Before any action can be taken, it is important to identify if an event is an incident. If it is in fact a cyber incident, then the assigned incident handler(s) can begin to identify affected assets and key stakeholders.

TIP !

Identifying the type of attack helps guide later steps.

CONTAIN

Containment is a critical phase in the incident handling process. It is aimed at stopping the spread of an incident, minimizing it’s impact, and preventing further damage to the affected systems and network.

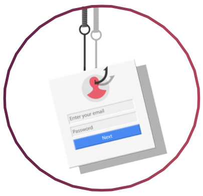
TIP !

Do not panic, take a deep breath. Remember there are plans in place!

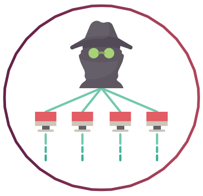
Common Attack Types

Ransomware

Phishing



DoS/DDoS



Malware

Key Steps and Strategies for Containment

□ Once an incident is identified, time is of the essence. Take immediate steps to contain it to prevent further damage or spread.

□ Isolate affected systems or networks to limit the attacker's access.

□ Implement temporary measures to stop the attack or malware from spreading.

□ Preserve evidence for forensic analysis while containing the incident.

ERADICATE

The Eradication phase of the incident handling process focuses on identifying and eliminating the root cause of the cyber incident. This phase is essential to ensure the incident does not recur and that the organization's systems return to a secure and stable state.

TIP !

Ensure the root cause of the indicident has been accurately identified.

Key Components of the Eradication Phase

□ Identify the root cause of the incident and remove any malware, unauthorized access, and/or vulnerabilities.

□ Patch and/or update affected systems to prevent similar incidents in the future.

□ Conduct a thorough analysis to ensure that all traces of the incident are removed.

RECOVERY

The Recovery phase involves activites that help restore assets post incident, with the goal of returning systems to a fully operational status. As with the Containment phase, time is of the essence, and a misstep at this stage may allow the attacker to re-enter the system later.

TIP !

Ensure the restored systems' integrity has been validated.

Key Components of the Recovery Phase

□ Once an incident has been resolved, plans to restore systems should be completed as soon as feasibly possible.

□ Make an informed decision about when to resume operations.

□ Enact the Business Continuity Plan and/or Disaster Recovery Plan.

□ Once the system has been restored, continuously monitor for anomolous activity until you are reasonably confident the system is clean.

LESSONS LEARNED

The Lessons Learned phase is a time to question how and why the incident occurred, and what can be done to reduce the risk of future incidents. It is during this stage that questions should be asked on whether security tools are properly implemented and if policies and procedures are meeting the needs of the organization.

TIP !

Start as soon as possible, once the dust has settled, incidents can fade from memory.

Key Components of the Lessons Learned Phase

- ☐ **Review the incident response plan for any updates or modifications that have been identified. It is essential this plan is updated to remain current.**
- ☐ **Documenting the incident creates a record that may be referred to when responding to future incidents.**
- ☐ **Create a lessons learned report, this report should conclude with a 'Recommendations' section that details areas of improvement. These recommendations can include updating existing polices, generating new policies, and implementing additional security controls.**