advance

Cybersecurity Incident Response Plan

From Expense to Defence: How To Build a CIRP That Delivers Savings

Introduction

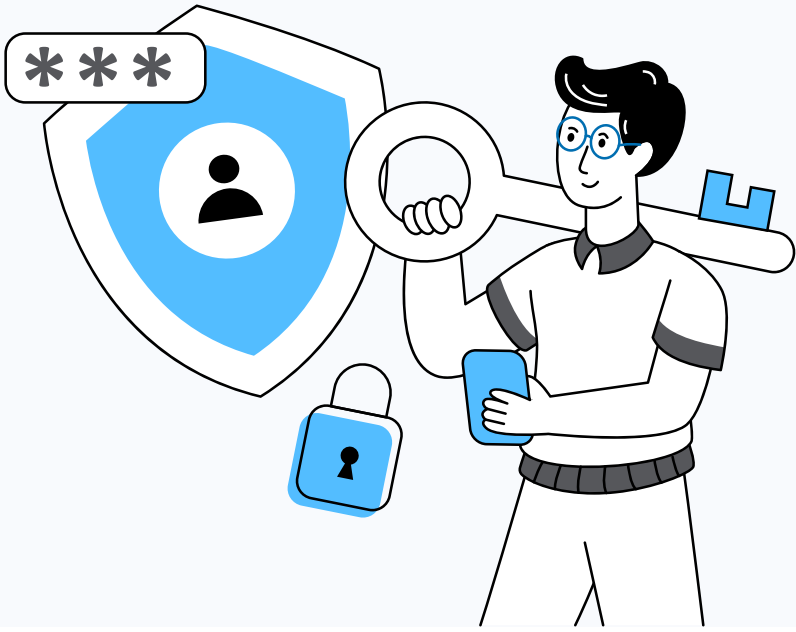
As organisations become more technically advanced, cybersecurity incident response plans (CIRP) become a key tool to deal with cybersecurity incidents thoroughly and, most importantly, cost-effectively.

A CIRP is a comprehensive plan that outlines how an organisation will detect, assess, and respond to cybersecurity incidents, from data breaches and malware attacks to system vulnerabilities and insider threats.

The CIRP guides the team's actions as it works to:

- Minimise the impact of cyber incidents,
- Swiftly restore normal operations,
- Ensure all compliance and regulatory standards are met,
- And make sure each step is completed in the most efficient and economical way possible.

In the following sections, we'll delve into the essential components of a CIRP and how to create one that suits your organisation's specific needs.



The Importance of Proactive Incident Management

A CIRP empowers business leaders to take a proactive, predictable approach to cybersecurity incident management—rather than waiting for an incident to occur and trying to determine how to respond under intense pressure.

A plan developed with cool heads, one that's been tested and refined through multiple 'fire drills', will always provide better results in both reducing the cost of managing cybersecurity incidents and reducing their impact on the organisation.

Key Steps to Create a CIRP

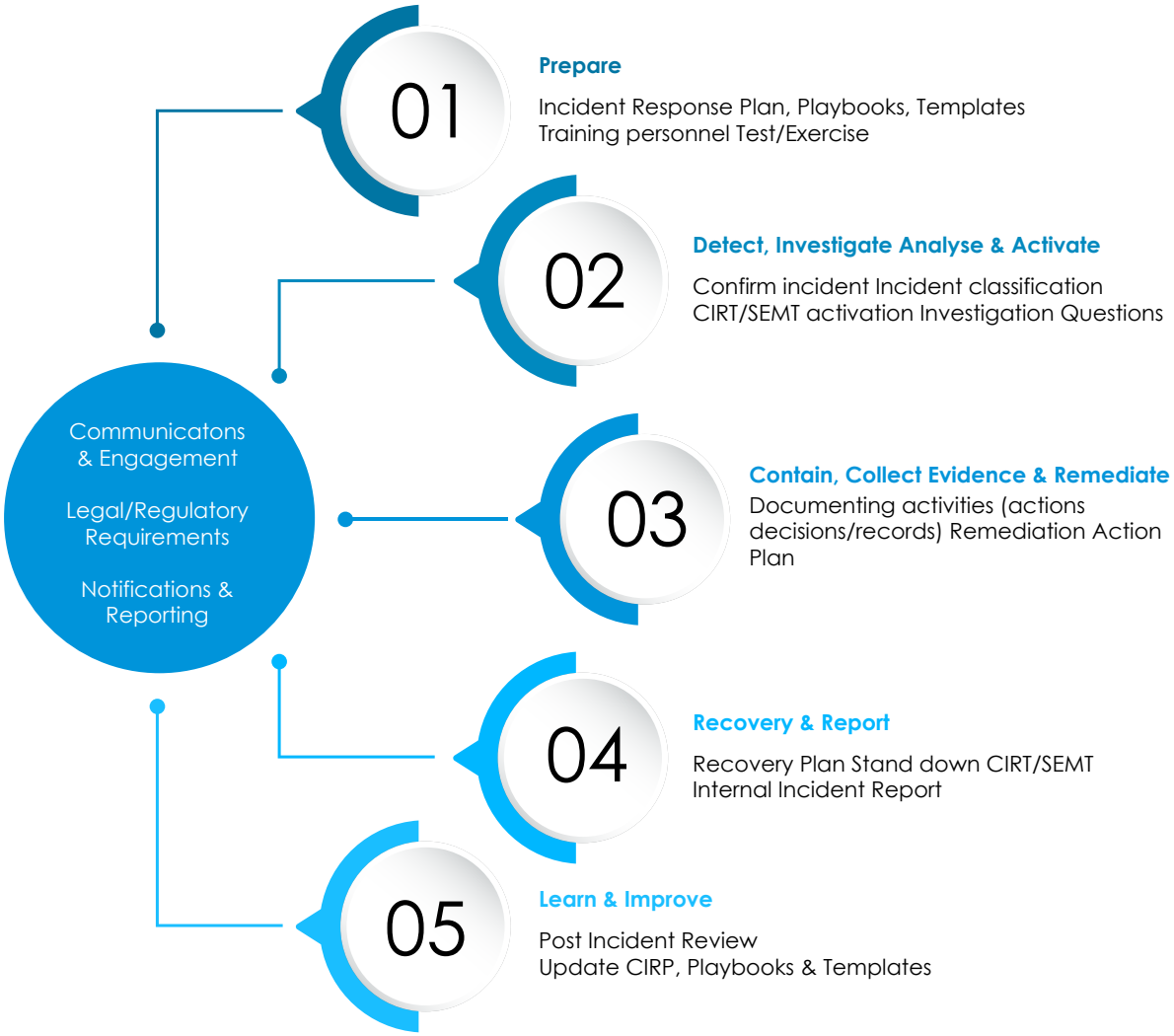


Figure 1: High-Level Incident Response Process

01

Step 1: Create a Cybersecurity Incident Response Policy

To begin, it's essential to establish a cybersecurity incident response policy. This policy serves as the foundation of your CIRP, outlining the overarching strategies and objectives for incident response. Involving stakeholders in policy creation ensures alignment with your business's unique needs and goals.

The policy should define the scope of incidents that the organization will address, as well as the severity levels and response criteria for each. It should also outline the chain of command and responsibilities during an incident, clarifying who takes charge and what actions should be taken at each level. A well-crafted policy sets the direction for each step that follows.

02

Step 2: Define an Incident Response Team with Set Responsibilities

The heart of any CIRP is the incident response team. This team should be carefully composed, with each member having well-defined roles and responsibilities. Clear leadership and decision-making processes within the team will ensure swift and effective responses to any cybersecurity incident.

Who should be on an IR team? There is usually a team leader or incident commander, a technical lead, legal counsel, public relations representative, and IT personnel with expertise in cybersecurity. Each role should be clearly spelled out, and team members should be trained regularly so they're ready to act when an incident occurs.

03

Step 3: Develop Playbooks

Incident response playbooks are invaluable assets. These documents outline predefined responses to common incidents, making sure that your team knows what actions to take and when. Tailoring playbooks to address specific threats enhances your readiness to face different cybersecurity challenges.

A playbook should include step-by-step procedures for identifying, containing, eradicating, and recovering from various types of incidents. They can cover scenarios like malware infections, data breaches, or denial-of-service attacks. Regularly updating and testing these playbooks is crucial to adapt to evolving threats effectively.

04

Step 4: Create a Communication Plan

Communication is at the core of effective incident response. Having a well-crafted communication plan in place is essential to keep stakeholders informed and manage the public perception of an incident. This plan should encompass both internal and external communications.

Internally, your plan should define how and when your team will report incidents to senior management and other relevant personnel. Externally, it should outline how you will communicate with customers, partners, regulatory bodies, and the media, if necessary. Clarity, transparency, and consistency in communication can help mitigate reputational damage during a cybersecurity incident.

05

Step 5: Test the CIRP

Once you've established your incident response plan, it's time to put it to the test. Testing gives you the chance to identify gaps, assess the effectiveness of your processes, and ensure that your team is well-prepared to handle real incidents.

There are various testing methods, including tabletop exercises, simulations, and full-scale drills—which simulate different cybersecurity scenarios and assess how your team responds. Regular testing helps identify weaknesses and areas for improvement in your incident response procedures, ultimately enhancing your organization's resilience to cyber threats.

06

Step 6: Identify Lessons Learned

After your organisation experiences an incident, it's crucial to conduct a thorough post-incident analysis to identify lessons learned. This step is crucial in refining and imporving your incident response capabilities.

During the analysis, evaluate the response process, communication, and the effectiveness of playbooks and policies. Identify what worked well and what didn't. Use these insights to update your incident response procedures, playbooks, and policies—ensuring continuous improvement and readiness for future incidents.

07

Step 7: Build a Schedule for Continual Testing of the CIRP

Cyber threats are constantly evolving, and so should your CIRP. To stay prepared, it's critical to build a schedule for regular testing and improvement.

Set a cadence for tabletop exercises, simulations, and other testing methods—consider conducting them at least annually or whenever there are significant changes in your organisation's infrastructure or threat landscape.

Scope of the Cybersecurity Incident Response Plan

The CIRP should include common cybersecurity threats, as well as organisation-specific risks identified through the organisation's risk management process.

Each scenario should have a playbook associated with it, which includes all five steps from Figure 1.

Top Five Cybersecurity Threats

Threat Vector	Description
Phishing	Phishing is a fraudulent attempt to obtain sensitive information from employees by posing as a trusted entity, often through email or other electronic communication.
Malware	Malware, such as viruses, trojans, and ransomware, can infect an organization's systems, steal data, or disrupt operations, causing significant damage.
DDoS Attacks	Distributed denial of service (DDoS) attacks aim to overwhelm an organization's network or website, rendering it inaccessible to legitimate users.
Social Engineering	Social engineering techniques manipulate employees into divulging sensitive information or performing actions that compromise organizational security.
Insider Data Theft	This threat vector involves employees or insiders stealing sensitive data or intellectual property for personal gain or malicious purposes.

Conclusion

In a world of interconnected business systems, cybersecurity incidents can be extremely costly, leading to financial losses, reputational damage, and legal consequences. By proactively investing in a CIRP, organisations can avoid trying to determine the best course of action while under the pressure of a cybersecurity incident. Pre-determined response plans can be tested and updated to ensure they're comprehensive,affordable, and complete.

This results in lower costs to resolve incidents, reduced financial and operational impact of incidents, overall improved business resilience and reduced risk. The proactive approach of planning and preparation for cybersecurity events is not only a sound financial decision but also a fundamental responsibility in safeguarding the interests of the organisation and its stakeholders.

Contact info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au