



The elements of a solid Incident Response plan



▶ Preparing for the inevitable: The importance of an Incident Response plan

Cybersecurity professionals work hard to protect the confidentiality, integrity, and availability of their organisation's assets. While strong measures are essential, no defence is completely foolproof, making a proactive plan crucial for minimising the impact of security incidents.

A well-prepared incident response plan is vital. It provides clear guidance on how to respond swiftly and effectively, helping organisations recover quickly and minimise disruption to their operations.

The do's and don'ts of effective crisis management

When a security incident occurs, responding quickly and effectively is crucial to minimising damage. Following these do's and don'ts will help guide your team through the crisis and ensure a more controlled and organised response. It's equally important to work in partnership with all areas of the company, as a collaborative approach is key to managing the incident smoothly and successfully.

D0's:

- ✓ Bring in the specialist quickly every second counts!
- ✓ Take immediate steps to contain the breach and secure your network.
- ✓ Communicate effectively keep all stakeholders informed with regular updates.
- Keep a detailed log of all actions and decisions made during the incident.
- Consult with legal experts to understand your obligations and manage the response.

DON'Ts:

- Don't panic it will only make things worse.
- Don't shut down compromised systems – this could hinder investigation efforts.
- others unless specifically directed to do so. **×** Don't use admin credentials

* Don't discuss the incident with

breached environment. Don't engage threat actors

to access the

directly – leave this to the experts.

The 5 elements





Governance: Establishes the framework for cybersecurity

leadership and accountability.

- Establish clear leadership and

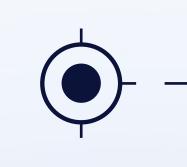
Actionable steps:

- assign specific roles within the incident response team - Develop a clear incident
- response policy - Implement regular audits

Engage internal teams,

Recommendation:

including legal, HR, and communications, alongside third-party partners, to ensure comprehensive oversight and a well-rounded response.





Involves readiness and planning for potential incidents.

Preparation:

Actionable steps: Recommendation:

- Risk assessment - Training and simulations

- Create and update playbooks

Prepare detailed procedures for high-impact

incidents and test annually.





Focuses on identifying and monitoring potential threats.

Detection:

Recommendation: Actionable steps: - Implement Invest in advanced continuous monitoring

- Alert prioritisation - Integration of

threat intelligence

detection tools to spot sophisticated attacks early.

Recommendation:

containment actions.





Actionable steps:

Response:

- Bringing systems back to Establish pre-approved normal, ensuring they're are authority for quick

Outlines actions taken to manage and mitigate incidents.

secure before reconnecting to them the network. It may

- also mean, rebuilding systems from "clean backups" - Containment and eradication - Collaboration across teams - Documentation of actions - Forensic analysis and investigation

- Post-incident activities: Involves reviewing and improving processes after an incident.

- Conduct post-mortem analysis

and process improvement

Actionable steps:

- Lessons learned

- Reporting and compliance

Recommendation:

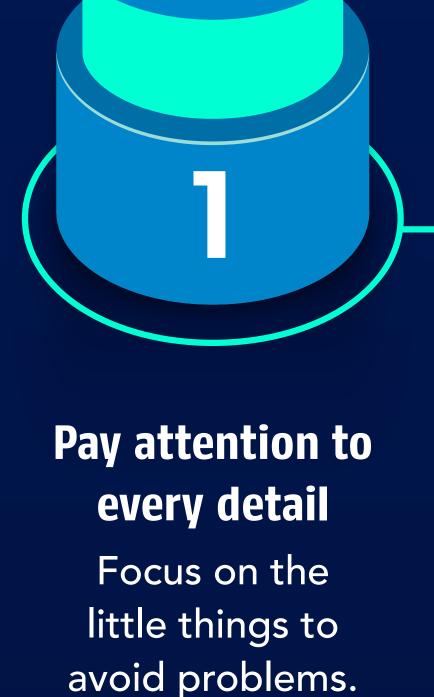
improvements.

Create a feedback loop for

ongoing preparedness

WHY DO YOU NEED IT

The four pillars of protection



Address all possibilities Be ready for

Quick action and strong data security Act fast and keep your data safe.

Protect your reputation Keep the public's trust by managing your image. C&W Business: Your guide to cybersecurity & digital growth

any situation to reduce risks.

C&W Business is a leader in enterprise solutions, offering exceptional service as a strategic partner to help customers thrive in their digital transformation. We support you through every stage, from designing and implementing to managing your cybersecurity solution, using industry frameworks and expertise gained from delivering services across the region.

STAY SECURE, STAY PROTECTED!

Safeguarding your business locally with global expertise. Contact C&W Business today to plan your cybersecurity strategy.