

INCIDENT RESPONSE PLAN AND EXERCISE

Prepare, Protect, Prevail.

With the ever-increasing use of technology and the internet, cyber criminals have become more sophisticated in their methods of attack, and the consequences of their actions have become more severe. It is no longer a matter of if but when an attack will occur, and being prepared for it is of utmost importance.




It is crucial for individuals, businesses, and organisations to take proactive measures in strengthening their cybersecurity systems and being prepared for any potential attacks. This includes investing in the latest cybersecurity technologies, regular training and having a comprehensive incident response plan in place to minimise the impact of an attack.



WHAT IS INCIDENT RESPONSE PLAN AND EXERCISE?

A cyber security incident response plan is a crucial component of an organisation's overall cyber security strategy. It is a document that outlines the steps that need to be taken in the event of a cyber-attack. An incident response plan helps organisations respond quickly and efficiently to secure data, minimise the damage and get your organisation back to business after a cyber-attack.

Building an incidence response plan:

- PHASE 1**   IDENTIFY STAKEHOLDERS
- PHASE 2**   DEFINE THE SCOPE AND SEVERITY OF INCIDENTS
- PHASE 3**   CREATE COMMUNICATION PLAN
- PHASE 4**   DEVELOP A REPORTING PLAN AS PER THE REQUIREMENT OF THE NOTIFIABLE DATA BREACH (NDB) SCHEME
- PHASE 5**   DEVELOP THE INCIDENT RESPONSE PLAN
- PHASE 6**   REVIEW AND TEST THE PLAN

Conducting a cyber security simulation exercise:

- PHASE 1**   DEFINE THE SCENARIO
- PHASE 2**   REVIEW ANY INCIDENT RESPONSE PLANS AND PREVIOUS SIMULATIONS DOCUMENTS
- PHASE 3**   GATHER THE STAKEHOLDERS
- PHASE 4**   CONDUCT THE EXERCISE
- PHASE 5**   MAKE CHANGES AS NECESSARY TO THE INCIDENT RESPONSE PLAN
- PHASE 6**   REPEAT ON AN ANNUAL BASIS

BENEFITS

Having an incident response plan and testing it on a regular basis is essential for any organisation. It helps minimise the impact of cyber security incidents by ensuring compliance with regulatory requirements as well as reducing downtime and financial impact. Organisations that review their incident response plan and test it regularly, are better prepared when responding to cyber security attacks and protecting their critical data.

WHY ORETA?

Oreta has a team of certified cyber security specialists who are dedicated to helping organisations stay secure in the digital age. With years of experience in the industry, Oreta has the knowledge and expertise needed to provide effective cyber security advisory services.

Oreta's services include everything from vulnerability assessments and penetration testing to security strategy development and incident response planning. Whether you're a small business or a large enterprise, Oreta can help you identify potential security risks and develop a plan to mitigate them.

At Oreta, we understand that every organisation has unique security needs. That's why we take a personalised approach to our services. Our team works closely with each client to understand their specific requirements and develop a customised solution that meets their needs.

For more information about how you can benefit from our services, please contact:

 sales@oreta.com.au

 [Oreta.com.au/security-services](https://oreta.com.au/security-services)

 [Linkedin.com/company/oreta/](https://linkedin.com/company/oreta/)



ABOUT ORETA

Empowering business outcomes through advisory, delivery and managed services using network, cloud, security, and analytics technologies since 2015.



Trusted by 250+ Businesses



Scale and flexibility on demand



Time given back to internal IT



Invested in your success



Partnership for now and the future

