tabletop exercise

—

When a cyber incident strikes, the way that organisational leaders respond dramatically influences the effectiveness of response, the scale of the impact, and the speed with which the organisation recovers. However, most cyber incidents force those same leaders to make decisions in a situation they've never found themselves in before. These decisions would be improved if the leaders had experience within similar situations - something that a tabletop exercise can provide.

WHAT IS A TABLETOP EXERCISE?

Tabletop exercises are face-to-face scenario-based training for senior business managers and crisis management teams. They test response plans, train teams, and improve understanding of cyber risks. With a wide range of scenarios available, the exercise can be tailored to address specific organisational areas and plans, such as Business Continuity Planning, Disaster Recovery, Incident Handling, and more.

cyberSuite's tabletop exercises combine our team's expertise in running wargaming and scenario-based trainings with an understanding of modern business risks to deliver an effective exercise to your management teams. Our exercise provides your team with an opportunity to respond to a cyber event and identify improvements without the consequences inherent to a real cyber incident.

WHY CONDUCT A TABLETOP EXERCISE?

Response Plan Improvements
As part of the exercises, your response plans (such as your Business Continuity Plan and/or Incident Response Plan) will likely be used and tested. The strengths and weaknesses of the plans will be discovered, and your team can then take the lessons learned to improve and strengthen your response planning.

Preparation and Training
The better prepared an organisation is for a crisis, the better they will respond when it occurs. This scenario-based training will guide key decision makers in understanding the considerations required in the event of a cyber incident.

Improved Communications
Understanding the lifecycle of a cyber incident - and the roles and responsibilities required to respond effectively - enables key staff to communicate more effectively, both internally and to external stakeholders.

tabletop exercise

—

OUTCOMES

Face-to-Face Training Session
Our team will work with your business managers and crisis management teams in a facilitated session. We will guide the conversations and assist in defining the scope, maintaining flow, and guiding the session.

Lessons Learned
Following the session, our team will provide you with notes regarding lessons learned and any key takeaways our team identified. Along with the notes taken by your team, these can allow for improvement of incident management processes.
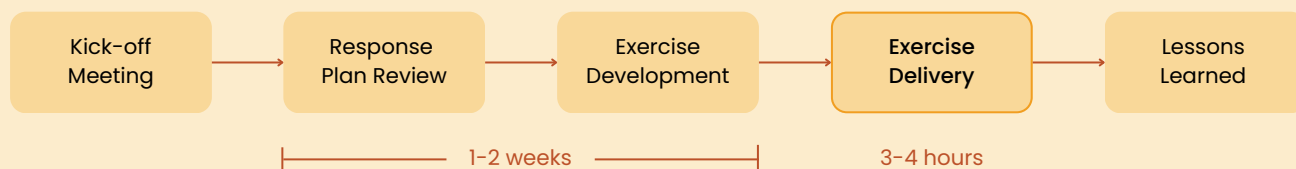
Confidence
Exercise participants gain confidence in their knowledge and skills for responding to a cyber incident. In addition, other stakeholders can gain higher confidence in your organisation's ability to respond to cyber incidents, thus increasing their overall confidence in your organisation generally.

SERVICE DELIVERY

Delivery Timeline

Kick-off Meeting → Response Plan Review → Exercise Development → Exercise Delivery → Lessons Learned

1-2 weeks (Response Plan Review — Exercise Development)

3-4 hours (Exercise Delivery)

Delivery Formats

- On-site at your office
- On-site at our Sydney office

- Video Conferencing
- Hybrid

Contact the cyberSuite team for more information, pricing* and bookings.

*Preferential pricing available for Emergence Insurance Policyholders.

📞 1300 829 237
✉ info@cybersuite.com.au
🌐 cybersuite.com.au

cyberSuite

who we are

cyberSuite is your trusted ally in navigating the intricate landscape of cybersecurity. Our team of cyber advisory specialists is dedicated to empowering individuals and businesses of all sizes. We enable you to safeguard your digital assets, offering tailored solutions to fortify your defences against evolving threats. With cyberSuite, embark on a journey of resilience, innovation, and unwavering protection in the digital age. Your cybersecurity success story begins here.

OUR TEAM

Cris White | Head of Advisory

Cris leads cyberSuite's cyber advisory team, combining his military background and risk management expertise to help organizations build resilience and navigate uncertainty. His hands-on approach spans all service areas, including conducting tabletop exercises and offering vCISO consultations.

Tai Tran | Senior Cyber Security Analyst

Tai has in-depth expertise in technology and change leadership. As an ISO27001 Lead Auditor and a holder of CISSP and CISM, Tai is passionate about assisting organisations to improve and solidify their governance and compliance practices.

Chris Lea | Cyber Security Analyst

Chris is our excited and cheerful security analyst who leads several service areas, including our Cyber Security Assessments and eDiscovery Service. He is an Associate of ISC2 and loves finding ways to improve processes and systems.

Chali Tillakaratne | Security Operations Analyst

Chali leads our Security Operations and Cyber Threat Intelligence capabilities. With a background in IT system administration, he is well versed in Microsoft platforms, as well as specialised security tooling such as Black Kite and Sentinel One.

Allana Boyd-Boland | Solicitor

Allana is a Solicitor focused on privacy and cyber law. Her expertise assists organisations by providing clarity around Privacy legislation, practical privacy policies, and providing advice for data breach eDiscovery.

OUR SERVICES

ADVISORY

- Security Assessment
- vCISO Trusted Advisor
- Supply Chain Risk
- Cyber Threat Intelligence

TRAINING

- Tabletop Exercises
- Cyber Awareness Training
- Privacy Training

SECURITY OPERATIONS

- Monitored EDR
- Vulnerability Management

INCIDENT RESPONSE

- Post Breach Remediation
- eDiscovery
- Digital Forensics

PRIVACY

- General Privacy Advice
- Privacy Training
- Data Protection