A DO-IT-YOURSELF CYBER INCIDENT EXERCISE

The First Hour, Rehearsed.

A ready-to-run tabletop exercise for Australian businesses. No facilitator training required. One scenario, the sheets to run it, and an honest way to see where your response actually stands.

Why run a tabletop

A cyber incident is not really a technical event. It is a test of decisions made under pressure, who has authority, who is reachable, what you can still see, and what you are obliged to do. Most businesses discover the gaps in that response for the first time during a real incident. A tabletop lets you find them in a meeting room instead, for the cost of an hour.

How to run this exercise

- **Pick a facilitator.** One person reads the scenario, keeps time, and stays neutral. Their job is not to have the answers, it is to keep the room moving and to resist rescuing it.
- **Get the right people in the room.** Not just IT. The value comes from having the people who would actually make these calls, including someone who can commit the business.
- **Set the ground rules.** No blame. Decisions are made out loud. 'I do not know who owns that' is a valid and useful answer, write it down rather than gloss over it.
- **Work in real time.** The scenario runs on a clock. Do not skip ahead. The pressure is the point.
- **Watch the response, not the malware.** The temptation is to solve the technical puzzle. Resist it. What you are testing is on the next page.
- **Debrief and capture.** Spend the last fifteen minutes filling in the action and scoring sheets while it is fresh.

WATCH THESE FIVE THINGS THROUGHOUT

- **Ownership.** Does someone clearly own each decision, or does it hang in the air?
- **Containment authority.** Who is actually allowed to take systems offline, and are they reachable right now?
- **Visibility.** Can you still see what is happening as it unfolds?
- **Evidence preservation.** Are you protecting what you will later need, or destroying it in the rush?
- **Pressure to restore.** How does the room behave when someone demands everything back online now?

SCENARIO 1 OF 1 · RUNS 25 MINUTES + 15 MINUTE DEBRIEF

Ransomware on One Workstation.

At 9:10 on an ordinary Tuesday, a staff member calls the helpdesk. Their screen is locked with a ransom demand. Start the clock and work through it out loud.

The injects

00:05 MIN

CONTAINMENT AUTHORITY

That machine is still switched on and sitting on your network. In this room, who is actually allowed to pull it offline, and can they do it in the next sixty seconds?

00:10 MIN

OWNERSHIP & TRADE-OFF

The spread is heading toward a server the business cannot run without. Taking it offline protects it but halts operations. Who owns that trade-off, and who do they have to speak to before they decide?

00:15 MIN

VISIBILITY

The monitoring you were relying on to watch the spread stops reporting. What can you still see, and what have you just lost the ability to know?

00:20 MIN

EVIDENCE & RESTORE PRESSURE

A director wants a straight answer on how long until things are back, and raises whether the insurer should be called. What has to happen before anyone restores from backup or engages with the ransom demand?

00:25 MIN

BREACH NOTIFICATION

Someone asks the question nobody wants to own: did personal information leave the building? Who in the room decides whether this has become a notifiable breach?

> *Facilitator note: resist the pull to work out which ransomware strain this is. That is not the test. Watch how the response holds together under pressure, and whether the five things above actually happen.*

THE AUSTRALIAN OVERLAY: IS THIS A NOTIFIABLE BREACH?

Inject 00:25 is where many businesses freeze, because they have never decided who owns the call. Under the Notifiable Data Breaches scheme in the Privacy Act 1988, if personal information is likely to have been accessed or stolen and this is likely to result in serious harm, you must notify the affected people and the Office of the Australian Information Commissioner. You are expected to assess a suspected breach expeditiously, as a guide within 30 days of becoming aware of it.

Two questions worth settling before you ever need them: who is authorised to declare a notifiable breach, and does your cyber insurer need to be contacted before you act or engage with a ransom demand? This is general information, not legal advice.

FILL THIS IN BEFORE YOU START

Who Is In The Room.

Assign each role to a real person. If you cannot fill a row, or the person is not reachable after hours, that is your first finding. Write it down.

Role	Name	Backup / who covers	Reachable after hours?
Executive / decision-maker authority to halt the business			
Finance payments, ransom position, insurance excess			
IT / infrastructure containment and technical actions			
Legal / privacy notifiable-breach decision, obligations			
Communications staff, customers, media			
Insurance / risk contact who calls the insurer, and when			
Facilitator runs the clock, stays neutral			
Scribe fills the action and scoring sheets			

Add your own rows for any role your business relies on that is not listed above.

FILL THIS IN DURING THE DEBRIEF

What We Need To Fix.

The exercise is only worth it if you leave with actions. Some common ones are pre-filled, tick the ones that apply and assign an owner. Then add your own.

Action	Owner	By when
Take out cyber insurance, or confirm we have current cover		
Read our actual policy terms and conditions, and know what the insurer requires		
Print an offline contact list: insurer, IT, legal, key staff, out of hours		
Confirm who has authority to isolate systems, in writing		
Confirm who can declare a notifiable data breach		
Locate our backups and confirm they have been tested by restoring from them		
Agree our position on ransom payment before the moment arrives		

The single most useful observation

Write down the first moment the response stalled, because a decision-maker was missing, an access was not in place, or an approval could not be found. That is where your next improvement starts.

SCORE HONESTLY, ON WHAT ACTUALLY HAPPENED

How Did We Do.

Score each area on what happened in the room, not on how you feel. A first run usually lands low to middle. That is not a bad result, it is a map of what to work on.

0	1	2	3
Never came up	We realised we could not	Partial / slow answer	Handled cleanly

Area	Score	Note
Containment authority, someone could take systems offline, fast	/3	
Decision ownership and speed under pressure	/3	
Visibility, we could still see what was happening	/3	
Evidence preservation, we protected what we would later need	/3	
Restore-pressure discipline, we did not rush past the right steps	/3	
Breach-notification awareness, we knew who decides and what triggers it	/3	
Insurer engagement, we knew who to call and when	/3	

Total out of 21. Re-run the exercise in a few months and watch the number move. The goal is not a perfect score, it is fewer surprises next time.

Most teams finish with more questions than answers.

That is exactly the point. The value of a tabletop is in the gaps it surfaces, the decision nobody owned, the access nobody had, the obligation nobody was sure about. A facilitated session goes further: a neutral facilitator injects the curveballs, holds the room to the hard calls, and catches the gaps a team talks past on its own. A live-fire exercise goes further again, testing whether your detection and containment actually work rather than whether you can describe them.

See where you stand right now. Start the free two-minute check:
app.vintaris.com

HOW VINTARIS CAN HELP

Understand where you stand
- Cyber security assessment
- Cyber security health check
- Essential Eight assessment
- Compliance readiness

Protect and defend
- Endpoint protection (EDR)
- Identity protection
- Data loss prevention
- Vulnerability management
- API security

Prepare and respond
- Incident response training
- Tabletop & live-fire exercises
- Incident response planning
- Digital forensics

Advise and lead
- Consulting & virtual CISO
- AI agent security
- Security awareness training

Enterprise-grade security, sized for the mid-market. Delivered remotely across Australia. See the full range at **vintaris.com/services**