



Cyber Security Health Check Fact Sheet v2.3



Businesses are heavily reliant on technology for managing critical information and effectively running their business operations to deliver better service, experience and productivity. However, business who embrace technology have increasingly become target of hackers and organised crime groups. Cyber-attacks are increasing, especially those that involve data leakage or the compromise of sensitive business or customer information. Reputational damage, legal action and fines or compensation payouts are among the many consequences victimised companies face. More so with the regulated population.



CHECK YOUR CYBER IMMUNITY

Have you ever considered what would happen if your sensitive business or customer information was compromised or your computer systems, technology dependent enterprises or networks were exploited? Building cyber resilience capabilities have become a high priority for many companies operating in critical sectors. Privasec can help identify your cyber threats and risks and assess the existence, effectiveness and efficiency of a range of industry better practice security controls across a complete range of domains.



HOW THIS SERVICES HELPS

As business' reliance on technology increases, the risk from cyber-attacks also increases. Privasec can assist to determine, evaluate and manage your cyber risks and take actions to improve your cyber resilience. Our Cyber Security Health Checks helps you identify your current security strengths and weaknesses and ensure that you are protecting your most important business assets. Privasec' experienced consultant help you design a strategic security roadmap or simply identify specific solutions to resolve your business' security weaknesses.



HOW THIS SERVICE WORKS

1. A dedicated Senior Consultant coordinates workshops with your key SMEs to review your critical business processes and functions, technologies used and networks to identify and qualify cyber threats and risks.
2. Based on the information obtained the Senior Consultant will assess the existence of a range of industry better practice security controls for their effectiveness and efficiency.

3. A Health Check report is provided to you that identifies and explain all the areas where adequate controls are either missing or deficient and will prioritise the risks to your business operations.
4. A report with practical recommendations will be proposed and prioritised to create a high-level security roadmap.

The onsite component of this service can be delivered in person at your offices or over the phone (video conference) over one to two days.



WHAT YOU GET

We will provide you with a concise report that:

- Describes your current cyber threats and risks.
- Identifies and prioritises the key findings observed.
- Includes a strategy and a roadmap to reduce your cyber risks and help build cyber resilience capabilities.



PREPARE FOR YOUR HEALTH CHECK

The following people may be asked to provide information during the workshops:

- Key business stakeholders involved in managing and operating your IT operations.
- Information Security Manager or staff responsible for Information/IT Security.
- Administrators of the systems and network(s) processing, containing and/or supporting your business operations.
- Third party SMEs who may be involved in your IT operations and ongoing management.

We will need to review your existing documentation to assess your current risks. We recommend you gather the following documentation (if it exists) for the initial workshop.

- Network diagram showing the systems and networks supporting your business operations
- Configuration standards of the servers and network devices in scope (if existing)
- Information Security Policy
- Acceptable Use Policy
- Information Classification Policy
- User Provisioning Processes
- Hiring, Induction and Termination Processes
- Vulnerability Management (Patching) Policy
- Security Incident Management Standard

Privasec

GRC
GOVERNANCE
AND INFORMATION
SECURITY PARTNERS

RED
RED TEAMING &
ADVANCED ETHICAL
HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia