

SURVIVING THE **DIGITAL** **REVOLUTION**

All organisations should have a robust information security framework to protect them from disruptive, damaging or possibly lethal cyber breaches. The risks are too great to ignore and are becoming increasingly common.

We can assess your vulnerabilities and help you put protocols and systems in place to survive. Don't wait until it's too late!



CYBER Risk Management - B17

CYBER RISK MANAGEMENT

PROTECTION FOR THE
NETWORKED WORLD

Saab Australia is a Defence, Security and Air Traffic Management solutions provider specialising in computer based command, control and communication systems. With a reputation for high reliability, mission critical systems and complex systems integration, the business has proven its capabilities in Australia for thirty years.

Saab Australia is part of Saab AB, one of the world's leading high-technology companies, with major operations in defence, aviation and civil security engineering. In today's complex and turbulent world, Saab's *thinking edge* is behind the innovative products and solution which are helping to safeguard people and society.

saab.com.au

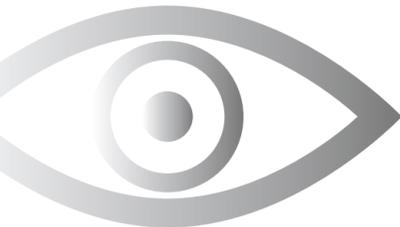
© Kenner | 123rf.com

ARE YOU PREPARED FOR A **CYBER ATTACK?**

Over the past few decades digital technology has transformed the scope, scale and potential for business. Organisations have moved their systems, information and processes online to connect, share and access data. Whilst this has created priceless efficiencies and opportunities, it also opens up vulnerabilities.



CYBER THREATS ARE A **SERIOUS BUSINESS RISK** A TRADE-OFF OF THE INTER-CONNECTED WORLD



The proliferation of ransomware, intellectual property theft and financial fraud are just a few threats we face today. Information security is not an 'IT' problem! Information security is a business risk and all business areas are part of the solution. The key is to identify what is important, what are the threats, and how you can reduce the associated risks to an acceptable level without impacting upon the organisation's objectives.

Ninety-five percent of all Australian businesses don't have the scale or resources for in-house cyber security management teams.

Our comprehensive information security advisory services can help you identify risk and safeguard your business from a devastating information security breach.

Our professional assessors, analysts and information technology specialists are trusted and respected by federal, state and local governments nation-wide and have assisted organisations in the

defence, health, education, law and finance portfolios. Services available through Saab Australia include consulting, penetration testing, information security auditing, training programs, as well as creating and implementing a complete strategic framework.

Saab Australia has security assessors who are IRAP certified by the Australian Department of Defence's Australian Signals Directorate. Conforming to the Australian Government's stringent protocols, they are highly qualified and endorsed to make independent information security assessments.

Assessments that will help you understand, identify and manage information security threats and the associated risks.

NOTIFIABLE DATA BREACHES

Is your company prepared?
As of February 2018, under the Privacy Amendment (Notifiable Data Breaches) Act 2017, organisations must report breaches of personal data to the individual and the Australian Information Commissioner.

Between July 2015–June 2016, CERT Australia responded to 14,804 cyber security incidents in Australian businesses, a 34% increase over the previous year.

SYMANTEC CORPORATION DISCOVERED MORE THAN 430 MILLION NEW AND UNIQUE PIECES OF **MALWARE** IN 2015, A 36% INCREASE ON THE PREVIOUS YEAR

MORE THAN 4,000 **RANSOMWARE** ATTACKS HAVE OCCURRED EVERY DAY SINCE THE BEGINNING OF 2016 (A 300% INCREASE OVER 2015)

THE AMOUNT OF **PHISHING** EMAILS CONTAINING A FORM OF RANSOMWARE GREW TO 97.25% DURING Q3 2016, UP FROM 92% IN Q1 2016

78% OF PEOPLE CLAIM TO BE AWARE OF THE RISKS OF UNKNOWN **LINKS IN EMAILS** AND YET THEY CLICK ANYWAY.

APRA REQUIRES **BOARD MEMBERS & EXECUTIVES** TO FULLY UNDERSTAND CURRENT CYBER SECURITY RISKS YET ONLY THE TOP 20% OF COMPANIES DO

STATISTICS ARE TAKEN FROM A SNAPSHOT IN TIME TO DEMONSTRATE THE RAPID INCREASE IN CYBER CRIME & NEED FOR PROTECTION

Data sources: Australian Government Australian Cyber Security Centre Threat Report 2017; Panda Labs — Quarter 2 Report 2017; United States Department of Justice, Computer Crime and Intellectual Property Section — Protecting Networks from Ransomware; Kaspersky Labs — Security Bulletin 2016; PhishMe Q3 Malware Review; Friedrich-Alexander University Germany presented at Black Hat USA 2016

PROTECTION SERVICES & ADVICE

Cyber security has progressed well beyond firewalls and virus protection software. For organisations to protect themselves from the enormity of a cyber breach, only a combination of products, services and activities can keep them safe. Saab Australia has the complete suite of professional services to offer this protection.

PENETRATION TESTING

Testing infrastructure, operating systems, services and applications to identify vulnerabilities and assess risk through exploitation.

VULNERABILITY ASSESSMENTS

Similar to penetration testing without vulnerability exploitation. A preliminary exercise to identify vulnerabilities without confirming their exploitability.

SOCIAL ENGINEERING

Tests security controls through people and processes by identifying staff awareness and resilience to the most successful and commonly-used attack vector today.

NETWORK DESIGN & SECURITY ARCHITECTURE REVIEWS

Determine whether controls within a network/communications environment are effective and appropriate for current business requirements, and aligned with vendor and industry best practise recommendations.

SYSTEM CONFIGURATION & SECURITY REVIEWS

Assess server and IT system configurations against industry and vendor best practise. Typically cover security configuration, password strength testing, software maintenance, firewalls, network infrastructure etc; tailored to your needs.

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK ACCESS REVIEW

Assess appropriate technical controls and protection to handle information and services that meet current business and regulatory requirements.

GOVERNANCE, RISK AND COMPLIANCE REVIEWS

Measure organisations commitment to standards (e.g. ISO 27001 and the Department of Defence Information Security Manual) policies and procedures to review an organisation's maturity and ability to manage risk.

RECOVERY SOLUTIONS

Saab's SAFE security and safety management platform is a workflow management system that guides organisations or operations through crisis or emergency situations. Used by airports, prisons, public transport networks, police departments, the system is easily customised to manage your unique tasks, resources and actions to restore.

