

Cyber Security Guide

10 Steps to
Information Security
Success



Information systems are being breached every single day. Financial loss, reputational damage and even the complete demise of organisations occurs on an ever-increasing basis.

Hackers operate in a low risk, high return environment. Funded by criminal syndicates, they exploit inadequate information security measures and poor user awareness whilst capitalising on the rich tapestry of social media information openly available. In doing this, cyber criminals perpetrate damaging information breaches to organisations across Australia and the world. This guide will help your organisation protect itself from information security breaches.

About Sententia

Sententia is a leading managed cyber security services provider, IT solutions provider and trusted business consultant and advisor. Sententia works with local, state and federal government departments, media organisations, finance, insurance and banking providers and corporate, enterprise and not-for-profit customers to safeguard them from the unknown.

Sententia has been helping organisations across Australia, New Zealand and South East Asia secure their information technology infrastructure since 1989 and is a recognised leader in information security.

Sententia possesses some of the highest levels of accreditation and certification available today. Offering preventative services, proactive monitoring and support as well as breach remediation, incident response services and information security consulting services, Sententia can offer your organisation the best cyber security solutions available today.



Table of Contents

Information Security Basics.....	4
Ten Steps to Information Security Success.....	5
Step One: Have an Information Security Plan.....	5
Step Two: Secure Your Devices, Network and Electronic Infrastructure	6
Step Three: Keep Software and Applications Up to Date.....	7
Step Four: Secure Your Cloud Environment.....	7
Step Five: Have a Backup of Your Organisations Data.....	8
Step Six: Implement a Data Loss Prevention Strategy.....	8
Step Seven: Educate Your Staff, Suppliers and Customers.....	9
Step Eight: Undertake a Regular Cyber Security Assessment.....	9
Step Nine: Consider Purchasing a Good Cyber Breach Insurance Policy.....	10
Step Ten: Consider a Cyber Security Managed Service.....	10
Industry Certifications	11
Cyber Security Threat Assessments.....	12
Initial Cyber Security Assessment.....	13
Comprehensive Cyber Security Assessment.....	13
External Vulnerability Assessment.....	14
Social Media Threat Assessment.....	15
User Awareness Assessment.....	15
Managed Cyber Security Services.....	16



Information Security Basics

Information security was traditionally perceived by most organisations as a niche issue confined to the IT department, with little significance to the organisation's day to day operation. The risks associated with a cyber breach was viewed as a nuisance when compared to more traditional organisational risks that received mindshare by an organisations leadership.

With the advent of digitisation, the connected world and the reliance by organisations on their information systems, today, information security is now considered a major business risk. Governments around the world consider cyber security as a top line threat of national and international significance and have legislated to counter this risk.

The Sententia Cyber Security Guide illustrates key action points that organisations can take to protect their information, comply with the law and protect their confidential data, customer data and organisational reputation.

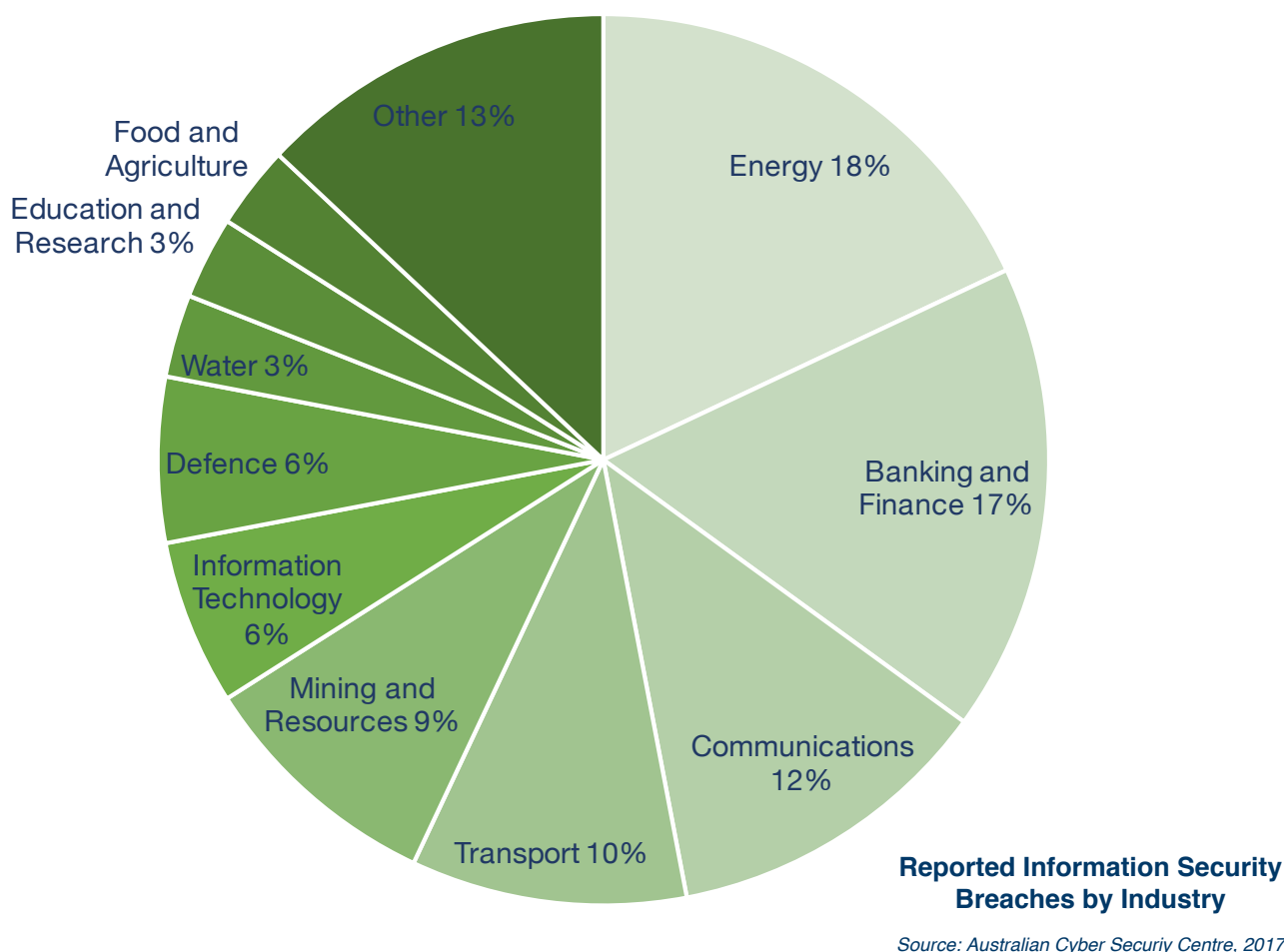
Ten Steps to Information Security Success

Step One: Have An Information Security Plan

Until recently, organisations operated under the belief that hackers simply weren't interested enough in them to perpetrate damage. This misplaced complacency led to decision makers assigning few resources to information security, whilst fewer still had a meaningful plan to avoid or mitigate a breach.

Sadly, hackers think otherwise. There are now countless high-profile breaches that continue to be reported in the media from organisations large and small. In addition, tightened regulations around the mandatory reporting of cyber breaches means that organisations are increasingly aware that there is both a business need as well as a regulatory need to protect against cyber breaches.

Interestingly, organisations where information technology has traditionally been considered peripheral to the organisations core functions (such as those organisations in the energy, transport, mining and resources industries) are the ones most likely to be targeted. As the below graph indicates, this is undoubtedly due to the lack of strong cyber security defences in these organisations.



Strategic planning around information security is essential. An Information Security Plan, a Business Continuity Plan, a Risk Management Plan and a Business Impact Assessment are crucial. In addition, the planning for these strategies must be owned by the key decision makers in an organisation such as a board or at CXO-level to ensure success.

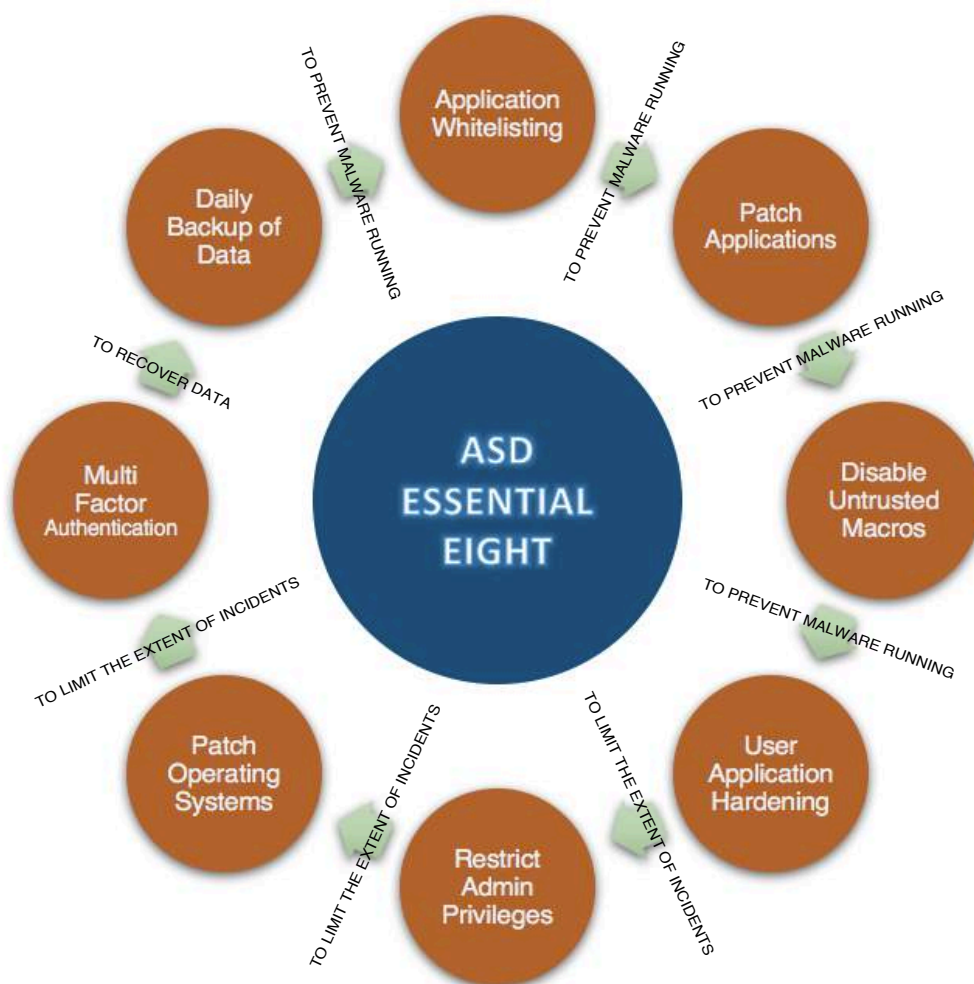
Step Two: Secure Your Devices, Network and Electronic Infrastructure

There is broad acceptance of the value of physical security systems such as locks, fences, alarms, access control systems and cameras to protect from intruders and burglars. Your organisation has very likely invested significantly in these protective systems. Information security is based on the same principles in order to protect your virtual assets.

As with physical security, it is never entirely possible to guarantee that your organisation will not be compromised. However, by making it as difficult as possible for a would-be attacker to break in, an organisation can significantly reduce the risk of a cyber breach.

There is no one-size-fits-all approach to securing your devices, networks and infrastructure. Different organisations have different needs. To mitigate cyber security incidents, organisations should refer to the Federal Government Australian Signals Directorate "Essential Eight", listed below, to ensure that:

- o an advanced / unified threat management firewall is deployed to protect from external cyber threats.
- o leading endpoint security software is deployed for computers and mobile devices.
- o the appropriate network and domain security services are installed, enabled and configured.
- o strong email security systems such as spam filters, message control systems and email-based threat detection systems are in place.
- o the appropriate security is configured and installed on appliances such as wireless networks, IP telephony, video conferencing equipment and IoT devices.
- o privileged access to electronic infrastructure and services is restricted to necessary personnel only and that access is managed proactively, constantly monitored and regularly reviewed.



Step Three: Keep Software and Applications Up To Date

Ongoing maintenance is essential to ensure that IT systems are as secure as possible. Operating systems, applications and even device firmware will occasionally require updates and patches to address any discovered bugs and faults. This applies particularly to IT infrastructure such as network switches and routers.

Most operating systems such as Windows and Mac allow for automatic updates, however, many applications will require manual updates. Adobe Flash and Java, for example, are particularly vulnerable to security threats and these applications should be updated frequently.

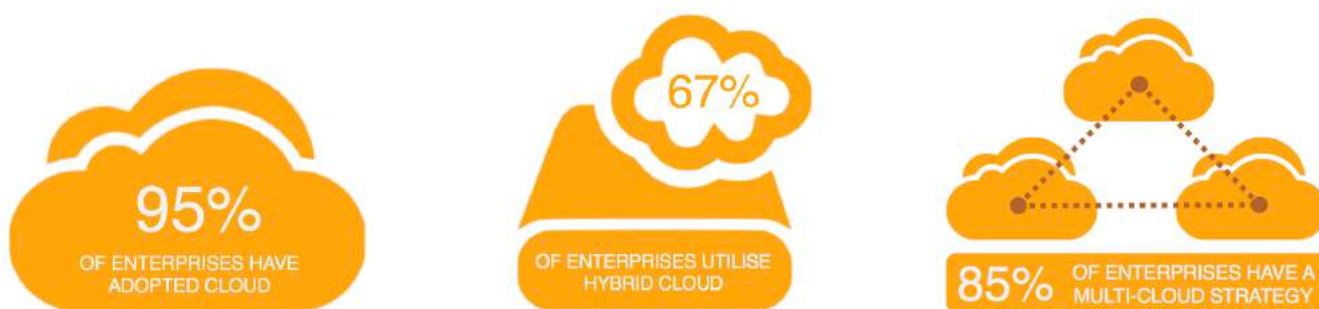
Many organisations use hardware and software that is no longer supported by the manufacturer. This "end-of-life" equipment is particularly vulnerable to being breached as any security flaws that exist will no longer be rectified. It is critical to refresh this equipment with current technology.



Step Four: Secure Your Cloud Environment

The majority of organisations have moved applications, data and processes to the cloud. Whilst there can be considerable cost savings in transitioning to cloud computing services, the principles of information security are different in the cloud as they are for on-premises infrastructure and often this will present different categories of risk to an organisation.

While it is certainly possible to secure data in the cloud, a risk assessment prior to implementation is prudent. Enforcement of appropriate security measures during implementation followed by a cyber security assessment post-implementation is always the recommended course of action for any data that is kept off-site. This includes cloud services regardless of whether they are hosted in a public, private or hybrid cloud environment.



Source: Rightscale - Cloud Computing Trends, 2017

Step Five: Have a Backup of Your Organisations Data

Complete, verifiable and well-managed information backups are critical for any size organisation. Disaster events such as fires, floods, storms, power surges, power outages and theft of equipment happen far more frequently than most organisations prepare for. Other events that can affect an organisations IT environment include equipment failure, a severe cyber breach or simple human error.

The "3-2-1" rule of backup is essential for all organisations to follow. This means:

- o have at least three complete copies of your data.
- o have copies of your data on at least two different types of media.
- o have one copy of your data stored off-site or in a secure cloud location.



Ransomware incidents caused by malware such as Cryptolocker continue to cause issues for many organisations. When a computer has been hijacked by ransomware, the most effective course of action is to wipe the computer clean and restore it from a recent, complete and easily accessible backup. This minimises downtimes but most importantly avoids the payment of any ransom to a cyber criminal. Many organisations cut corners when backing up data, presenting a significant business continuity risk.

Step Six: Implement a Data Loss Prevention Strategy

Over 30% of all cyber security breaches occur when a trusted insider within an organisation either accidentally or deliberately shares confidential data to external parties. Often, the insider had privileged access to data they had no business justification to have in the first place, usually due to poor or mismanaged user permission settings.

Most organisations have no mechanism in place to prevent the loss of important files through their transfer to a portable hard drive or USB key connected to a workstation. Email is another transferral method. There are countless examples of disgruntled employees taking confidential data such as intellectual property, customer databases and financial data with them upon exiting an organisation. These cases often end up in court, however, by that point, the damage to that organisation has almost certainly been done.



A strong and well-enforced data loss prevention strategy will help organisations keep sensitive and confidential data protected helping to ensure that data loss events detrimental to your organisation are minimised.

Step Seven: Educate Your Staff, Suppliers and Customers

An organisation can spend significant time and money to purchase the best information security systems available. These systems are then rendered useless when organisations allow staff to use easily guessed dictionary-based passwords. Poor user education with regards to information security is a major contributor to successful cyber breaches.

It is vital for organisations to place strong emphasis on frequent education of staff on cyber risk. In addition, customers, suppliers and stakeholders of that organisation can and should be educated to minimise cyber risk and exposure.



Step Eight: Undertake a Regular Cyber Security Assessment

The best way for an organisation to confirm that it has a strong cyber security defences is to work with a third-party provider such as Sententia to undertake thorough and regular assessments of information security systems, processes and policies.

Cyber security assessments are particularly crucial for an organisation's executive team. Assessments help management establish that all legal and regulatory requirements relevant to that organisation are being met. The executive can confirm that the organisation is protecting itself from undue harm, risk and potential reputational damage. Where deficiencies are detected, an assessment will recommend the appropriate course of action to address and remediate these.



Step Nine: Consider Purchasing a Good Cyber Breach Insurance Policy

Every day, new cyber threats emerge. Whilst organisations can take every possible step to protect themselves from a technical and awareness perspective, it is impossible to entirely guarantee that an organisation will not suffer a breach. In fact, organisations are well advised to prepare and plan for a cyber breach to occur at some point.

It is always recommended that organisations purchase cyber breach insurance to address the considerable risk associated with any potential cyber breaches or data loss incidents. Through our Cyber Security Threat Assessment Services, Sententia can assist your organisation in preparing you to obtain a cyber insurance policy by reducing your risk profile and your premium.



Step Ten: Consider a Cyber Security Managed Service

Information Security is rapidly changing. New threats constantly emerge. To master the field requires continual focus and dedication. Even large organisations with dedicated information security teams struggle to keep on top of their cyber security defences. For smaller organisations who often employ a generalist IT manager with little to no specialisation in information security, they grapple with maintaining the necessary protections required to prevent breaches as well as managing the organisations IT operations. For this reason, many organisations seek to outsource this risk to a specialised and certified information security partner that can offer operational peace of mind.

Since 1989, organisations across Australia have relied on Sententia to provide strong cyber security protection. Sententia is a recognised leader in information security and has attained some of the highest levels of industry and vendor certifications available. Sententia is the only provider able to offer the expertise, knowledge, dedication, focus and passion your organisation needs to protect its information.



Industry Certifications

Organisations rely on Information Security solutions to provide protection from external intrusion, insider threats and accidental loss of data. Sententia acknowledges the enormous responsibility placed on us by you, our valued client. Cognisant of this, Sententia's greatest priority is to ensure that our teams are the most experienced, most knowledgeable, most qualified and most skilled people in the information security business. We seek to ensure that your organisation operates at peak security whilst optimising efficiency and productivity. Our formal industry certifications include:



Sententia experts hold Certified Information Systems Security Professional (CISSP) accreditation, awarded by ISC², an independent accreditation body. CISSP certified personnel possess extensive experience in information security, having demonstrated at least seven years of hands on experience.



Sententia experts hold the highly coveted Certified Information Systems Manager (CISM) accreditation, awarded by ISACA, an independent accreditation body. CISM ensures that a certified professional approaches IT security in accordance with established frameworks and principles.



Sententia experts hold the highly coveted Certified in Risk and Information Systems Control (CRISC) accreditation, awarded by ISACA, an independent accreditation body. CRISC ensures that a certified professional approaches IT from a risk management perspective.



Sententia experts hold ISO 27001 Lead Auditor accreditation, demonstrating our capability to assess an organisations cyber security readiness. ISO 27001 is the de-facto standard framework for information security readiness and management worldwide.



Sententia experts are active members of the Australian Information Security Association (AISA). AISA is the peak professional body for Australian information security professionals, working with government and industry peers to drive education and policy to protect information.



Sententia experts are ITIL certified. ITIL certification demonstrates Sententia's competence in providing best practice IT service management to ensure alignment of IT services with an organisations needs and overall strategy.



Sententia experts are PRINCE2 certified. PRINCE2 is a structured project management methodology and framework and Sententia professionals consistently use elements of PRINCE2 as part of our managed service and solutions offerings.



Sententia experts are PMP certified. The Project Management Professional certification is an internationally recognised designation that demonstrates competence in delivering complex projects. With the sensitive and mission critical nature of projects Sententia works on daily, being PMP certified is crucial for our clients.

Cyber Security Threat Assessments

Methodology and Analysis

WHY IS CYBER SECURITY SO IMPORTANT?

The cyber security landscape is changing every single day.

The number of cyber breaches occurring is increasing exponentially.

Organisations can no longer afford to hope they will not be breached. There is a direct link between the loss of confidential data and the long term viability of organisations. There are significant financial and legal penalties that also apply.

In addition, the cost to the organisation due to reputational damage and business disruption is immeasurable.

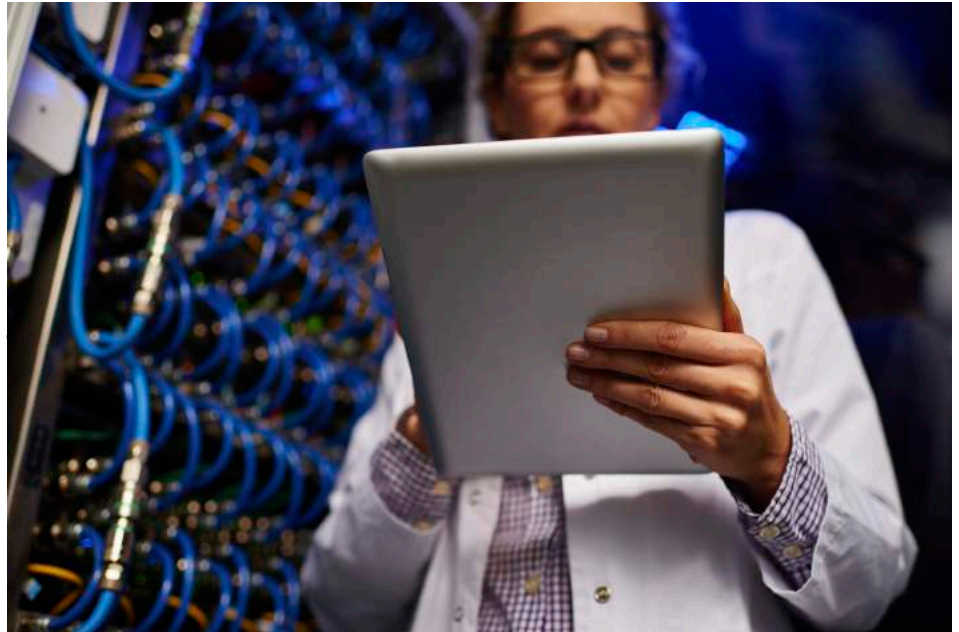
WHY REVIEW YOUR CYBER SECURITY?

A cyber security threat assessment is the first step in determining an organisation's cyber security posture.

Once completed, the assessment allows an organisation to address areas of concern such as regulatory compliance, risk mitigation and business continuity strategies.

A Cyber Security Threat Assessment is the first step in ensuring that your organisation is protected from cyber criminals.

Information security is a major concern for senior managers and boards in all organisations. Cyber security threat assessments allow your organisation to gain insight into its information security posture. Any deficiencies can be addressed, offering your organisation protection from previously unseen risks.



Assessment Service Offering

Cyber Security Threat Assessments are undertaken by Sententia's skilled and qualified network and information security engineers. Our team forensically review all aspects of your organisation's cyber security posture including:

- conducting an **initial cyber security health check** which monitors network and traffic flows and connected devices for any vulnerabilities such as data leakage, bots, ransomware and advanced threats.
- conducting a **comprehensive cyber security assessment** including a network assessment, firewall rule assessment, endpoint protection assessment, patching and update policy assessment and backup / disaster recovery policy assessment.
- performing an **external vulnerability assessment** to determine the organisation's external cyber security posture. This can include formal penetration testing if required.
- conducting a **social media threat assessment** helps identify exposure and risk an organisation has to social engineering and social media based threats.
- performing a **user awareness assessment** helps organisations determine how risk aware individuals in the organisation are to information security principles.

Cyber Security Threat Assessments are held in high esteem by executives and boards, cyber insurance providers, legal practitioners as well as organisational stakeholders, who increasingly seek assurances their personal information is safe.

Cyber Assessment Focus Areas

Initial Cyber Security Health Check

The initial cyber security health check is a low cost, low impact service carried out by conducting an analysis of traffic flows in and out of the organisations network. This analysis is conducted with a network security check-up appliance which will determine threats such as bots, malware, attempted exploits, data loss incidents, high-risk web applications and access to high-risk websites.

An initial health check will also indicate your organisations information security compliance to frameworks such as PCI-DSS, ISO27001, NIST and others.

Comprehensive Cyber Security Assessment

Upon completion of the initial assessment, any recommendations made should be actioned as appropriate. Following this, it is recommended that a comprehensive cyber security assessment is carried out. This assessment involves:

- A vulnerability assessment that evaluates network connected devices for any application, patching, configuration or setup vulnerabilities and recommends remediation recommendations.
- A review of the organisation's patching and update policy to ensure that device patching takes place within an acceptable timeframe.
- A network assessment that inspects the overall network architecture to ensure that the network (including wired and wireless networking) is configured and managed in the most secure manner possible.
- A firewall rule assessment that reviews the existing firewall rules and policy configuration to ensure that the most secure and appropriate settings have been configured on the firewall.
- A backup and disaster recovery policy assessment reviews the organisation's data backup policy to determine if business critical data is being managed in the most fault-tolerant and business resilient method possible.
- A review of cloud applications and platforms being used by the organisation, with an emphasis on whether the appropriate security settings are in place.



OVER
80%

OF COMPANIES
HAVE BEEN
SUCCESSFULLY
HACKED¹

\$2.82m

THE AVERAGE
COST PER CYBER
BREACH TO AN
AUSTRALIAN
BUSINESS²

48%

OF BUSINESS
LEADERS ARE VERY
CONCERNED ABOUT
CYBER SECURITY³

OVER
254k

KNOWN
CYBERCRIME
INFECTIONS IN
AUSTRALIA IN ONE
SINGLE MONTH⁴

Sources:

1 - Duke University / CFO Magazine Global Business Outlook Survey

2 - IBM / Ponemon - 2015 Cost of Data Breach Study - Australia

3 - Cisco Systems, 2016 - Presentation to the Australian Cyber Security Centre, Canberra, April 2016

4 - Australian Crime Commission 2016 - Presentation to the Australian Cyber Security Centre, Canberra, April 2016

86%
OF ORGANISATIONS
CURRENTLY LACK
ADEQUATE CYBER
SECURITY
CAPABILITIES⁵

146 DAYS
THE MEDIAN TIME
CYBER CRIMINALS
WERE ON A VICTIMS
NETWORK BEFORE
BEING DISCOVERED⁶

95%
OF INCIDENTS
INVESTIGATED FOUND
HUMAN ERROR AS A
FACTOR TO A CYBER
BREACH⁷

44%
OF ORGANISATIONS
CONSIDER A STRONG
CYBER SECURITY
POSTURE AS A
COMPETITIVE
ADVANTAGE⁸

Sources:

5 - HPE - Cyber Risk Report 2016

6 - Mandiant Consulting - M-Trends Report - February 2016

7 - IBM - 2014

8 - Cisco Systems, 2016 - Presentation to the Australian Cyber Security Centre, Canberra, April 2016

External Vulnerability Assessment

Upon completion of a comprehensive assessment, a list of recommendations is produced. Once these recommendations have been actioned, an external vulnerability assessment can be carried out by conducting:

- o vulnerability scans which assess potentially misconfigured externally-facing systems, unnecessary administrator access to externally-facing systems and the possible use of default, weak or dictionary-based passwords.
- o inspection of an organisations off-site or cloud deployments to ensure that the necessary security is deployed and implemented.
- o optional penetration tests can be conducted through the employment of registered ethical hackers. Penetration tests are only recommended if a comprehensive assessment has been completed and cyber security issues continue to persist.



Social Media Threat Assessment

Threats from social media engineering are becoming more prevalent, usually because inappropriate information about an organisation is available through social media.

A unique offering available through Sententia is a social media threat assessment. This assessment allows an organisation extensive visibility relevant information available through social media channels including Facebook, Twitter, LinkedIn and Instagram. The assessment assists organisations in formulating a solid social media strategy to ensure that it can best control publically available information pertaining to that organisation.



User Awareness Assessment

One of the most critical areas of information security is user awareness and training. The desire for convenience often means that users make inadequate security-related decisions. This can include simple passwords on their user accounts, offering their credentials to others for use, inadvertently "volunteering" information to third parties and opening email attachments without first making an informed and security conscious assessment of the email.

Over 30% of all cyber breaches occur simply because of a lack of user awareness. Surprisingly, very little effort is placed on assessing, educating and incentivising an organisations users into adopting good information security behaviour.

Another unique Sententia offering is a user awareness assessment. This assessment seeks to establish the cyber security readiness of an organisations users to determine how educated users are in information security readiness. The assessment will recommend any improvements needed to minimise an organisations chances of a cyber incident due to human error.



VICTIM CASE STUDY: CODAN LIMITED

Codan is an ASX-listed and Adelaide based manufacturer of sophisticated metal detectors for military and mining applications.

In 2011, Codan started to receive returns of faulty metal detectors. These returns had unrecognisable parts in them. Codan was of the impression that customers were repairing or modifying the equipment, thus voiding the warranty. Soon, ASIO alerted Codan's senior management of a far more serious problem - one of their employees notebooks had been hacked whilst on a business trip to China. The notebook was compromised through the hotels wi-fi connection. The notebook contained the blueprints to all of Codans products. The hacker stole these blueprints and sold them to the highest bidder, who subsequently started to manufacture counterfeit Codan metal detectors at one-third of the price of a regular Codan unit.

Soon, Codans share price plummeted, and within a 10 month period, Codan's profitability fell by 80%. Five years later, Codans share price is still yet to recover.



\$575

BILLION

THE GLOBAL COST
OF CYBERCRIME
PER YEAR⁹

23 DAYS

THE AVERAGE TIME
TAKEN FOR AN
AUSTRALIAN
BUSINESS TO
RESOLVE AN
ATTACK¹⁰

430 MILLION

THE NUMBER OF
UNIQUE PIECES OF
MALWARE THAT
EXISTED IN 2015¹¹

\$200 THOUSAND

THE REWARD APPLE
PAYS RESEACHERS
PER VULNERABILITY
DISCOVERED¹²

Sources:

9 - Intel Security - Net Losses: Estimating the Global Cost of Cybercrime, June 2014

10 - Stay Smart Online - Australian Government, October 2015

11 - Symantec - Internet Security Threat Report 2016

12 - Macrumors.com - Apple Launches Bug Bounty Program, August 2016

Cyber Security Managed Services

Sententia Deploy, Monitor and Respond

The SententiaGuardian™ suite of Cyber Security Managed Services can proactively monitor and rapidly respond to cyber security incidents in your organisation - 24 hours a day, 7 days a week and 365 days a year.

Cyber Security has become a critical concern for business owners, boards and senior managers in all organisations. There is significant risk that shortcomings in an organisations cyber security posture can and will threaten its survival.

Many organisations are grappling with the issue of cyber security and often allocate responsibility to the IT manager. However, even diligent IT managers struggle to keep up with the ever-changing face of cyber security, an area that is increasingly becoming more specialised and complicated.

This is where Sententia can assist. As a specialised and recognised cyber security provider, Sententia helps provide your organisation with cyber security solutions design, deployment, management, proactive monitoring and incident response, helping you stay ahead of cyber criminals whilst mitigating risk and maximising business resiliency.



Managed Security Service Offering

Sententia understands that not all organisations are the same. The **SententiaGuardian™ CSOC** service can cater for the requirements and budgets of all organisations.

The standard CSOC service is available in Silver, Gold and Platinum. In addition, the SententiaGuardian CSOC can be customised to your organisations needs.



Providing a basic level of monitored security services, the **SententiaGuardian™ CSOC Silver** service protects your organisation by monitoring and advising you of key external cyber threats.






Offering a good level of managed and monitored security with leading visibility and reporting, the **SententiaGuardian™ CSOC Gold** service protects your organisation from both internal and external cyber security threats.



With the very best managed and monitored security protection possible, the **SententiaGuardian™ CSOC Platinum** service offers your organisation complete peace of mind from internal, external and insider threats.

Managed Security Focus Areas

	 Silver	 Gold	 Platinum
External Services			
Anti-Virus	✓	✓	✓
Anti-Bot	✓	✓	✓
Anti-Malware	✓	✓	✓
Anti-Spam	✓	✓	✓
URL Filtering			✓
DNS	Optional	Optional	✓
Intrusion Prevention System		✓	✓
Intrusion Detection System		✓	✓
WAN Link Monitoring		Optional	✓
Sandboxing and Threat Extraction			✓
Encrypted Traffic (SSL and TLS)			✓
DDoS		Optional	✓
Vulnerability Scanning	Annual Scan	Continuous Passive	Continuous Active
Internal Services			
Server		✓	✓
Endpoints		✓	✓
Network and WAN		✓	✓
Firewall Rules		Optional	✓
Mobile Devices		Optional	✓
Identity Awareness			✓
Disk Encryption			✓
Sandboxing			✓
Application Monitoring			✓
Disaster Recovery Monitoring			✓
Data Loss Prevention			Optional
Vulnerability Scanning	Annual	Continuous Passive	Continuous Active
Cloud Services			
Servers		✓	✓
Application			✓
Disaster Recovery / Backup			✓
Vulnerability Scanning	Annual	Continuous Passive	Continuous Active
Maintenance			
Hardware Firmware Updates	Optional	Optional	✓
Software Updates / Patching	Optional	Optional	✓
Vulnerability Management	Optional	Optional	✓
Reporting and Readiness			
Monthly Security Reporting	Optional	✓	✓
Customised Security Reporting		✓	✓
PCI-DSS / ISO-27001 Readiness			✓
Incident Response	Ad-hoc Billable per incident	Ad-hoc Billable per incident	Included
Service Hours	8AM to 6PM Business Days	8AM to 6PM Business Days	24 Hours a Day 7 Days a Week
Advisory Services			
Legal Advisory Service (Operated by External Provider)	Optional	Optional	Optional
Insurance Advisory Service (Operated by External Provider)	Optional	Optional	Optional
ISO27001 / PCI-DSS Compliance (Operated by External Provider)	Optional	Optional	Optional

WHY CHOOSE SENTENTIA TO MANAGE YOUR CYBER SECURITY?

Sententia's team of cyber security experts hold some of the highest industry and vendor certifications available. You can rest assured that when Sententia monitor your IT security, you are being protected by the safest pair of hands in the industry.

Sententia has been successfully operating a Cyber Security Operations Centre for NSW Government for over 10 years and has managed the security for some of the largest financial service providers in Australia.

Sententia will help protect your organisation from cyber criminals.

About Sententia

Sententia is a leading managed cyber security services provider, IT solutions provider and trusted business consultant and advisor. Sententia works with local, state and federal government departments, media organisations, finance, insurance and banking providers and corporate, enterprise and not-for-profit customers to safeguard them from the unknown.

Sententia has been helping organisations across Australia, New Zealand and South East Asia secure their information technology infrastructure since 1989 and is a recognised leader in information security. Sententia possesses some of the highest levels of accreditation and certification available today. Offering preventative services, proactive monitoring and support as well as breach remediation, incident response services and information security consulting services, Sententia can offer your organisation the best cyber security solutions available today.

HACKER PROFILE: OLGA KOMOVA

Olga Komova is a 25 year old Uzbek national living in Thailand. In August 2016 while working as a hotel guest relations officer, Komova was arrested by Thai authorities at the request of US law enforcement officials.

Komova is accused of being the mastermind behind \$38 million worth of cyber crime. The operation allegedly targeted customers of financial institutions in the USA, the UK, Australia, Germany, Italy and Japan with phishing emails in order to obtain their banking credentials to wire funds into the syndicates possession.



Komova, who maintained an active social media presence during the time when the alleged crimes were said to have occurred, is accused of using her position at the hotel as cover for her alleged cyber crime activities. The United States successfully applied for her extradition to face criminal charges and if convicted, Olga Komova will face a lengthy jail term.

About this guide

The content provided in this guide is for general information purposes only. This guide should not be used as a substitute for professional advice. This guide should not be used as a basis for any decision or action that may affect your organisation. Before making any decision or taking any course of action that may affect your organisation, you should consult a qualified professional adviser.



SYDNEY - MELBOURNE - BRISBANE

ADELAIDE - CANBERRA - PERTH

Phone: 1800 333 867
www.sententia.com.au

Copyright 2017 - Sententia Pty Ltd