How Much Cyber Security is Enough?

Securing mid-sized financial organisations in Australia

Anne Coull
Objective Insight
Australia
email: anne.objectiveinsight@gmail.com

***Abstract*— Cyber security is a risk: the risk that the company's information assets will be compromised in a way that affects their data's integrity, availability, and/or confidentiality. Like any other enterprise risk, cyber risk needs to be managed in a way that balances the cost of risk realisation against the cost of mitigating that risk. Defence in depth is a seemingly simple and logical approach to protecting systems and data, but is defence alone enough, and how much is needed? Local and global standards and guidelines direct companies in where to focus their mitigative efforts, but for the uninitiated, these can be confusing. Cyber security is an expensive exercise, with much at stake. By taking a practical approach that combines people, policies, processes as well as technology, organisations can manage the cyber security risk to protect their critical and sensitive information assets, and comply with government regulations, within a reasonable budget.**

Keywords- cyber security; risk management; penetration testing; threat; vulnerability; control; NIST; ASD; APRA; ISO27001; ISO27002; defence in depth.

I. INTRODUCTION

Cyber security and cyber resilience are business challenges and business risks. An effective cyber security strategy incorporates people, policies, processes, and technology into an over-all risk management plan, and integrates these aspects to implement defence in depth [1][31]-[33]. This way, organisations can protect their critical and sensitive information assets, and be proactive in identifying, preventing, detecting, responding, and recovering from cyber threats and attacks [1][7][28][31]-[33].

Small to medium businesses in Australia are on the front-line of the cyber war, and are easy pickings for cyber criminals, as their lack of cyber expertise and investment in cyber security can leave them open to exploitation.

Implementing an effective Cyber Security Risk Management Plan will enable these smaller organisations to balance their IT security expenditure with government regulation and business outcomes [21]. The Australian Government has recently established a set of standards to which businesses in the financial sector must adhere [2]-[6]. For these smaller businesses to survive, they will need to protect their sensitive and critical information assets and satisfy the government regulations within their limited budgets. But how do they know where to start? And, how much cyber security is enough?

While cyber risk can never be reduced to zero, this paper applies practical risk management to enable an organisation to identify where it should be focusing its efforts. In addition, it analyses the requirements and recommendations of the most visible standards and guidelines and draws from these an effective set of controls that, once applied, will protect the organisation from known threats and attacks, reduce the likelihood and impact of successful exploits, and enable the organisation to meet the Australian government's new pre-requisites to do business.

Section 2 assesses the cyber security standards and guidelines available to businesses in Australia's financial sector. Section 3 discusses a practical approach to managing cyber security risk. Section 4 identifies the controls an organisation should apply, within this risk management framework, to mitigate their cyber security risk and reduce the residual risk to an acceptable level.

II. CYBER SECURITY STANDARDS AND GUIDELINES

The following cyber security standards and guidelines were assessed:

1. The Australian Prudential Regulation Authority (APRA):
   a. CPG 234 Management of Security Risk in Information and Information Technology [2];
   b. CPS 234 Information Cyber Security [6];
2. The Australian Signals Directorate (ASD):
   a. Top 4 [7];
   b. Essential 8 [7][8]; and
   c. Top 37 controls [9];
3. AS ISO/IEC 27001:2015 Information technology – Security Techniques – Information security management systems – Requirements [15];
4. AS ISO/IEC 27002:2015 Information technology – Security techniques – Code of practice for information security controls [16];
5. NIST:

 ISBN: 978-1-61208-743-6

a. Cyber Security Framework [19];
b. 800-53 & 800-53A: Security Controls and Objectives [27];
c. 800-53R4 Security and Privacy Controls for Federal Information Systems and Organisations [26];
d. 800-167 Guide to application whitelisting [30];
e. IR 7621: Small business fundamentals [23].

A. AS ISO/IEC 27001:2015 and AS ISO/IEC 27002:2015

The ISO 2700X standards define the objectives and techniques for implementing information security management in an organisation [15][16]. This is the standard applied by the larger banks and financial organisations operating in Australia. It is also the standard used for measuring the security posture of their third-party suppliers. ISO 2700X require that an information security policy will be documented, communicated, and available; Persons will be assigned responsibility for implementing an information security management system that meets the stated objectives and identifies, assesses, and treats the risks associated with the loss of confidentiality, integrity, and/or availability of information by implementing suitable controls to meet the information security objectives [15][16]. ISO 27001 standard specifically identifies the need for competent people to oversee its information security performance, and for all people working in the organisation to be aware of the information security policy and how their individual roles contribute to its effectiveness [15][16].

B. APRA CPS 234

The APRA prudential standard set is aimed at the financial sector in Australia. CPS 234 covers the fundamentals of cyber security, such as the need to have an information security policy and security controls in-place to protect information assets as well as the need for third-party suppliers who hold an organisation's information on their behalf meet these same obligations. CPS 234 requires an organisation to identify and classify its information assets by criticality and sensitivity. Criticality and sensitivity indicate the degree to which the organisation would be impacted by an incident that affects availability, integrity, and/or confidentiality of that asset [2][6]. An asset's classification acts as a guide for selecting controls suitable to protect that asset. The effectiveness of these controls needs to be tested regularly, relative to the rate of systems change within the organisation, and externally in the broader threat landscape [2][6].

APRA requires that an organisation be able to detect and respond to potential cyber incidents and that incidents and vulnerability test results need to be reported to the appropriate Information Security executive(s) and the board. The design and effectiveness of the information security controls need to be internally audited [2][6]. APRA must be notified within 5 days of any material information security incidents and/or when the organisation identifies a material vulnerability in its information security controls that cannot be remediated in a timely manner [6].

Leadership and board commitment are key requirements spelled out in both the APRA CPS 234 and the ISO2700X standards. Ownership and visible support from the top is critical to the success of information security management in an organisation as this assures the necessary resources are made available to establish, implement, maintain and continually improve the security management system [6][16].

C. Australian Signals Directorate Top 4 and Essential 8

The Australian Signals Directorate (ASD) offers a comprehensive list of 37 mitigating cyber security controls that they have classified as essential, excellent, very good, good, and limited [7][8]. ASD claims that their Top 4 cyber mitigations will reduce the risk of a successful cyber exploit by 85% by decreasing the likelihood of a successful intrusion, and then limiting the impact of that intrusion, should it succeed [7]. The essential 8 includes the top 4 plus 4 more essential mitigations [7][8]. The ASD essential 8 mitigations are:

1. Application whitelisting of approved programs to prevent the execution of malicious programs including .exe, DLL, scripts, and installers.
2. Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours (e.g., Remote code execution in Microsoft windows operating system). Always run the latest version of the operating system, and don't use unsupported versions.
3. Patch applications such as Flash, web browsers, Microsoft Office, Java and PDF viewers. Use the latest version of applications and patch or mitigate extreme risk vulnerabilities within 48 hours.
4. Restrict administrative privileges to operating systems and applications based on user duties. The need for privileged access should be regularly revalidated and confirmed by the person's manager. Privileged accounts must not be used for reading email and web browsing.
5. Harden user applications by configuring web browsers to block Flash, ads, and Java on the internet. Disable any features in MS Office, web browsers, and PDF viewers that are not needed, such as OLE.
6. Important and changed data, software, and configuration settings need to be backed-up daily and stored off site and disconnected from the source network for at least 3 months. Restoration

 ISBN: 978-1-61208-743-6

should be tested at least annually and when the IT infrastructure changes.

7. Use multi-factor authentication for VPNs, RDP, SSH, and other remote access, and for all users performing privileged actions or when accessing sensitive information.
8. Microsoft Office macro settings should be configured to block macros from the internet, and only allow permitted macros from trusted locations or those with a trusted certificate, with limited write access [7][8].

D. NIST 800-53 and NISTIR 7621 for Small Business

NIST 800-53 provides a comprehensive framework of guidelines for managing risks – from vulnerability identification and risk assessment through to identifying and implementing mitigative controls. NIST 800-53 divides the cyber security management into 5 phases: identify, protect, detect, respond and recover [19].

NISTIR 7621 for small business offers 25 mitigating cyber security controls. There is natural overlap between the NIST and the ASD essential 8 controls. Both NIST and ASD recommend patching operations systems and applications, whitelisting applications and controlling internet access, ensuring redundancy of systems and data by taking regular backups, limiting access to data, and controlling systems administration privileges. NISTIR 7621 for small business also recommends: the use of both hardware and software firewalls between the organisation's network and the internet; anti-virus and anti-spyware on every device that connects to the organisation's network, encrypting data at rest and in transit. In addition, the NIST guideline extends beyond managing the technology to include mandatory data breach reporting requirements, for example. It also includes controls identified in the ISO 27002 standard, such as restricting physical access to the workspace and data centre [15][16][19][23][26][27][30].

III. Practical Risk Management

Proactive management of cyber security risks within an organisation is best achieved by combining aspects of the standards and guidelines discussed to establish an effective cyber security risk management process that identifies the cyber risks, evaluates the level of the risks for that organisation and implements an appropriate set of mitigating controls to reduce the residual risk to an acceptable level [21][29]. This can be achieved by combining appropriate aspects of the standards and guidelines discussed, within the context of the organisation under consideration.

Risk management is a continuous process. The risk management plan is the basis for effectively identifying, managing, and monitoring its cyber security-related risks [21][29]. An organisation's objective in performing risk management is to enable it to achieve its mission by:

1. More effectively securing the IT systems that store, process, or transmit the company's information;
2. Providing the information needed to make well-informed risk decisions that justify security-related IT expenditure;
3. Facilitating and enabling accreditation, by providing supporting documentation as a result of this risk management plan [21][29].

A. Cyber Security Risk Management Process Activities

1) System characterisation and Scope determination

Managing cyber risk needs to be done within the context of the organisation, its purpose, scope, and the environment in which it operates. The first step is to understand the business context by defining the mission and operational characteristics of the system: what the system does and how it operates in the organisation's environment, and what is the scope and boundary of the risk management plan [21][29].

2) Asset identification and analysis

Within the agreed boundary and scope, identify critical and sensitive information assets and significant and critical systems and activities that need to be protected, and assess their value [6][21][29] in terms of:

i. the functions they perform, as they relate to confidentiality, integrity, and availability;
ii. the value to the business in terms of reputational damage and market-share loss if they were compromised;
iii. their replacement value (if applicable);

3) Threat identification and analysis

Perform threat modelling to identify and evaluate relevant threats to confidentiality, integrity, and/or availability of these assets, or the information pertaining to these assets, by considering common, known threats, emerging threats, and threats that relate to the local environment. Threats may be natural events, or man-made: man-made threats can be intentional or accidental; and intentional threats can be external or internal. Intentional threats can be better understood by considering the potential motives driving these behaviours, ability to execute the attack, and opportunities available for the attackers to exploit vulnerabilities to execute these attacks. Commonly known potential threats include social engineering, phishing, hacking, and worms [18][21][24][25][29][31]-[33].

4) Vulnerability identification and analysis

Assess the vulnerabilities, or weaknesses in the protection measures for the assets identified that may be exploited by these threats, such as people clicking on links in phishing emails or malicious websites, downloading

 ISBN: 978-1-61208-743-6

malware infected files and software, out of date patching on operating systems and applications, and/or lack of whitelisting [21][29][30]. This is an ongoing exercise as new vulnerabilities are identified. Intelligence services can assist with providing updates on recent/current vulnerabilities and exploits.

5) Risk identification

Risks are identified where threats may exploit the vulnerabilities in these assets [21][29].

6) Risk analysis

The level of risk is determined by the likelihood these vulnerabilities will be exploited by these threats, and the impact if this were to happen [21][29]:

Level of Risk Exposure = Likelihood x Impact.

Impact includes the estimated direct and indirect costs to the business, if this were to happen. The NIST Risk Analysis process provides a comprehensive model for risk analysis [27][29] as illustrated in Figure 1. The process starts with the threat source, their intent, and the likelihood they will initiate a threat event to attempt to exploit a vulnerability in the target organisation. The degree to which the attacker is successful in exploiting these vulnerabilities will depend on the effectiveness of the mitigative security controls. The residual risk is the combination of likelihood that the exploit will succeed and the degree of the adverse impact if it does.

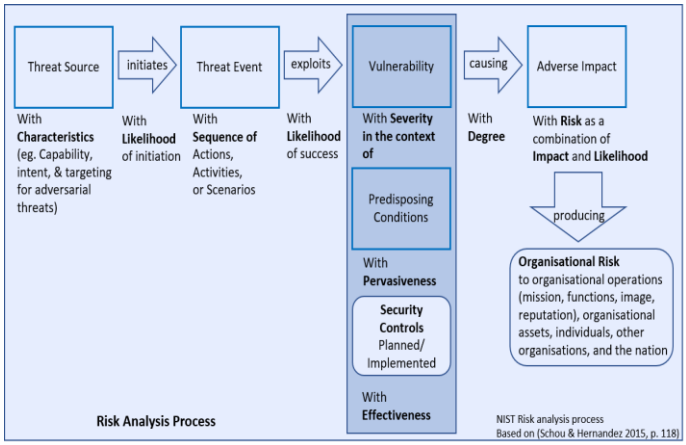

Figure 1. NIST Risk Analysis Process

7) Risk treatment

Prioritise the risks based on business impact. Identify and evaluate countermeasures, or controls that can be applied to reduce the residual risk. Calculate the cost of these controls. The types of controls need to be appropriate for the criticality and sensitivity of the assets, the vulnerabilities and threats to these assets, where they are in the lifecycle, and the potential consequences of a security incident [6][15]-[17].

Controls are selected to:

i. protect critical and sensitive information assets;
ii. mitigate risks and avoid unnecessary operational, financial, and customer losses.
iii. ensure compliance with regulatory and legislation requirements;
iv. gain competitive edge.

8) Monitoring Risk

Following the implementation of the recommended controls, the organisation should monitor, measure and validate the effectiveness of controls and the extent to which they are meeting their objectives [15]-[17].

IV. RECOMMENDED CONTROLS

These controls have been identified from the sources discussed [1]-[16][19][20][22][23][26]-[28][30]-[32] and tested in the Australian cyber landscape for their effectiveness in maintaining cyber security and resilience for a mid-sized Australian organisation with 300-500 employees. These controls apply in both physical (and virtual) data centres and cloud computing architectures, and can be implemented within a reasonable budget and timeframe.

TABLE I. RECOMMENDED CYBER SECURITY CONTROLS

Ownership, accountability, and resourcing	
Objective	***Control***
Information Security Policy	The Information Security Policy is owned and endorsed by the board. It defines how the organisation will mitigate specific elements of its cyber risk, including the behavior it expects from its people. The Information Security Policy is accessible and communicated to all staff on a regular basis, and staff are held to account.
Appropriately staffed & resourced	The cyber security strategy and day-to-day responsibility for implementing and maintaining security protection, detection, response and recovery sits with the CIO, CTO, and/or CISO. This person must have appropriate cyber knowledge.
Trusted staff	Background checks should be conducted on all internal employees. Administration-level privileges should only be provided to trusted staff, for the systems and periods they are required.
Develop a security culture by teaching employees how to protect their data	Induction training to include security policies on use of computers and devices, networks, and internet connections; and expectations of the employee in protecting sensitive and critical information.
	Train employees in appropriate use of corporate devices and resources, such as phones & printers.
	Have all new employees sign a statement that they comprehend these policies, that they will comply with these policies, and that they understand the consequences of non-compliance.
Protection and Prevention	
Objective	***Control***
Protect networks, systems and	Install and regularly update anti-virus and anti-spyware software on every computer and device on the network, and all that will connect to the network.

information from damage by viruses, spyware, and malicious code.	This includes within the office, remote access, and any third-party supplier devices that connect to the organisation's network. Set the anti-virus to automatically update and scan at a regular time.
Provide security for the internet connection: hardware firewall	Install, use, and keep operational a hardware firewall between the internal corporate network and the internet
	Install, use, and keep operational a hardware firewall between internal employee's home network and the internet if employees work from home
	Change the administrator's name and regularly change the administrator's password on the hardware firewall
Provide security for the internet connection: software firewall	Install, configure, use, and keep operational a software firewall between the internal corporate network and the internet. Enable and configure the firewall on Microsoft and IOS systems.
	Install, configure, use, and keep operational a software firewall between internal employee's home network and the internet. Enable and configure the firewall on Microsoft systems.
Patch operating systems and applications	Test and install application and operating system patches. Critical patches should be installed within 48 hours. Use automated scans to identify unpatched vulnerabilities, and determine temporary workarounds until patches are made available.
Control physical access to all computers and network components	Only allow authorised people to have physical access to and use of corporate devices.
	Position computer screens and displays so people walking past cannot read them.
	Know and monitor who has access to the systems, networks, and office space, including cleaners & maintenance, and network repair personnel.
	Store servers and communication hardware in a secure server room, and limit access to those who need it.
	Implement a policy to challenge all unknown personnel.
Secure the wireless access point and network	Set the wireless access point so it doesn't broadcast its SSID (Service Set Identifier).
	Change the default administrative login id and password on the device.
	Use strong encryption for transmitted data so it cannot be easily intercepted and read by electronic eavesdroppers. (WPS-2) (Don't use WEP)
Data storage: Static encryption	Classify, label, and encrypt all sensitive data in storage.
Data storage: Data loss prevention	Establish and train employees on 'rules' in relation to handling and protecting customer data, both at work, and offsite. (e.g., Don't put customer data on home computers)
	Disable USB drive connections
	Monitor data transfer through all channels (email, file copy, print etc.) IDS can assist with this.
	Secure hardware destruction prior to decommissioning
	Utilise the ability to remotely wipe all mobile devices
Encryption in transit	Encrypt data in transit within the network and when shared externally. Options include TLS 1.3 (at the transport layer), WinZip AES 256 for email attachments, and SFTP for external file transfer.
Encryption key management	Securely store the encryption keys and restrict and monitor who accesses these. Tools are available for this purpose but they are only as secure as their own access controls.

Individual user accounts	Each must have a separate, individual user account for each application, computer, and device.
	Passwords need to be a random series of letters, numbers, and special characters, and be at least 8 characters long. Use passphrases.
	Passwords should be changed every 3 months.
	All users should have accounts that DO NOT have administrative privileges.
	Prevent users from installing unauthorised software.
	Administrative rights should only be used by systems administrators for the time and the purpose for which they are needed. Never surf the web from an admin account. It may allow malicious software to be downloaded and installed.
Limit data access to needs to know	Employees should have only access to the specific data and systems they need to do their job. This access should be verified every 3 months
Separation of duties	Protect the business from insider threat by not allowing a single individual to both initiate and approve a financial or other transaction.
Multi-factor authentication	Utilise multi-factor authentication (MFA) on all systems and accounts holding and accessing sensitive and critical data.
Disable macros	Disable macros except in specific, identified circumstances.
Whitelisting	Only download software from trusted sites. Only allow known, listed apps to be installed and run on corporate computers.
Hardware disposal	When disposing of business computers, remove and destroy the hard drives. When disposing of storage media: drives, USB's, paper copies, containing sensitive information, destroy using a cross-cut shredder.
Application development and testing	Have separate build, test, staging, and production environments. Apply security measures to build and test environments. For example: firewall protection; encryption & data masking to protect sensitive information.
	Build security into every phase of the development lifecycle: design, build, test, and implementation
	Perform exploit testing to identify vulnerabilities in applications, prioritise resolution into maintenance schedule.
Secure services and data	Harden Applications. Applications should be developed and implemented to separate the user interface, processing, and data storage layers. Limit communications and data transfer between application layers with subnets, port hardening, and security groups.
Continuous hosting critical systems	Redundant Servers: failover monitoring of critical servers.
	In virtual cloud, pre-image servers for DR redundancy
Harden DNS	Configure DNS server to alternative third-party DNS, such as OpenDNS, Norton DNS, or DNS Resolvers.
Uninterrupted data store	Establish redundant data store (e. Raid5 failover for data, or secondary data store in cloud)
Uninterrupted power	Establish Uninterrupted Power Supply (UPS), with redundant power source
Uninterrupted LAN-to-WAN comms	Redundant LAN-to-WAN connection: ADSL, wireless mobile with alternate ISP
	LAN-to-WAN Domain Router selects alternative connection: ADSL, wireless mobile with alternate ISP & automatically switches over
Uninterrupted LAN	Redundant LAN (cloud or redundant wireless Lan router)
Uninterrupted phone & VoIP	Redundant phone number, VoIP alternative or diversion.

comms	
Identify and track vulnerabilities	Utilise vulnerability scanning tools to identify vulnerabilities relating to patching and OWASP Top 10.
Penetration testing to identify vulnerabilities	Perform penetration testing pre and post release. Perform both internal and external black box and white box penetration testing.
Manage and close vulnerabilities	Prioritise vulnerabilities for resolution and retest based on criticality and sensitivity of assets at risk.
Detection	
Objective	***Control***
Log and analyse activities and events	Define and implement systems and security activity and event logging for all levels, systems, and networks.
	Monitor attempts to access closed and unused ports.
Inbound email authentication	DMARC, DKIM, SPF protocols for inbound DNS authentication, to prevent email spoofing
Email scanning	Incoming emails should be scanned for SPAM and malicious links and content.
Intrusion Detection	Utilise IDS to identify anomalous behaviours and review event logs regularly.
Identify intrusions early	Implement Security Information and Event Management (SIEM) to collate and analyse all log data. Utilise machine learning / artificial intelligence to identify anomalous behaviours across multiple systems as early warning indicators of compromise
Response and Recovery	
Objective	***Control***
Backup important business information	Don't store sensitive information on desktop C: drives Implement a comprehensive backup policy, to backup business information (data), including word processing documents, spreadsheets, configuration information & paper files The 'grandfather' principle has 3 cycles of backup – 1. a snapshot or drive for each day of the week: gets overwritten the same day the following week; 2. a snapshot or drive for each week of the month: gets overwritten the following month; 3. snapshot or drive for each month of the year: gets overwritten the same month the following year Retain the last snapshot or drive for the year, for 8 years. Backup onto separate, removable media or long-term cloud storage. Store backups offsite segregated from primary data. Redundancy for all servers running critical applications Redundancy for critical database(s) O/S & apps should be able to be reinstalled from CD, USB, or snapshot.
	Test the backed-up data to ensure it can be reliably read and restored successfully, at least every 3 months.
Denial of Service Protection	Processes & agreements in place to gain assistance from ISP and/or cloud provider DDoS protection capabilities to identify and block traffic from attacker's IP address(s) (in DoS or DDoS attack)
	Implement & monitor Web Application Firewall (WAF) on all web facing servers.
Cyber security incident management	Plan and implement Cyber Incident Response Process
	Plan for and implement threat awareness and critical incident communications.
Comply with the Australian Privacy Act	Incorporate appropriate data breach notifications into the Incident Management Process.
Business continuity planning (BCP) and testing	Pre-arrange alternative office facilities or secure remote access. For infrastructure housed in a physical data centre, redundant systems in an alternative location will be required. In a cloud computing architecture, terminal servers may be used to facilitate remote access (via secure VPN). Remote systems monitoring to allow system administrators to work remotely or from home
Outsourcing and Supplier Management	
Objective	***Control***
Assure third party security	Assess cyber security capability of third parties interfacing into the organisation systems, and/or storing or processing sensitive or critical data to assure they have at least the same cyber security.

A. Compliance

As a result of effectively implementing this Risk Management Plan, with the recommended controls, the organisation will satisfy the requirements for:

- ASD Security certification and accreditation;
- ISO 27001, and ISO 27002 compliance;
- Australian Privacy Standard;
- APRA CPS 234.

V. CONCLUSION

Defence in depth can be an expensive process. It is critical for businesses of all sizes to focus on the real risks that may impact their sensitive and critical data, and to mitigate these in priority order. An effective Risk Management Plan provides a robust framework within which to manage cyber security and cyber resilience. There are many sources of truth when it comes to identifying the right controls for a particular organisation. Taking a structured risk-based approach, based on the information available from NIST, ISO, and ASD will enable an organisation to balance IT security expenditure with business outcomes, and assure the company's survivability in the face of increasing cyber security concerns.

REFERENCES

[1] J. Andress and S. Winterfeld, "Cyber Warfare: Techniques, tactics and tools for security practitioners", second edition, Elsevier, Inc, United States of America, 2014.

[2] APRA, "Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology", 2013, Available from: https://www.apra.gov.au /sites/default/files/Prudential-Practice-Guide-CPG-234-Management-of-Security-Risk-May-2013_1.pdf, accessed August 2019

[3] APRA, "Prudential Practice Guide CPG 235 – Managing Data Risk", 2013, Available from: https://www.apra.gov.au /sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_0.pdf, accessed August 2019

[4] APRA, Prudential Standard CPS 232 Business Continuity Management", 2017, Available from: https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-232-Business-Continuity-Management-%28July-2017%29.pdf, accessed August 2019
[5] APRA, "Prudential Standard CPS 231 Outsourcing", 2017, Available from: https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf, accessed August 2019
[6] APRA, "Prudential Standard CPS 234 - Information Security (Draft)", 2018, Available from: https://www.apra.gov.au /sites/default/files/Draft-CPS-234.pdf, accessed August 2019
[7] ASD, "Strategies to Mitigate Cyber Security Incidents", Australian Cybersecurity Centre (ACSC), Australian Government, 2017, Available from: https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents, accessed August 2019
[8] ASD, "The Essential 8 Explained", ACSC, Australian Government 2017, Available from: https://www.acsc.gov.au/publications/protect/essential-eight-explained.htm, accessed August 2019
[9] ASD, "Australian Government Information Security Manual", ACSC, Australian Government, 2019, Available from: https://www.cyber.gov.au/node/237, accessed August 2019
[10] ASD 2019, "Preparing for and Responding to Denial-of-Service Attacks", ACSC, Australian Government, Available from: https://www.cyber.gov.au/node/166, accessed August 2019
[11] ASD, "Cloud computing security", ACSC, Australian Government, 2019, Available from: https://www.cyber.gov.au/node/55, accessed August 2019
[12] ASD, "Risk management of enterprise mobility including bring your own device", ACSC, Australian Government, 2019, Available from: https://www.cyber.gov.au/node/171
[13] R. Bejtlich, "The tao of network monitoring: beyond intrusion detection", Addison-Wesley 2005.
[14] R. Bejtlich, "The practice of Network Security Monitoring: Understanding Incident Detection and Response", San Francisco: No Starch Press, 2013.
[15] ISO AS ISO/IEC 27001:2015 "Information technology – Security Techniques – Information security management systems – Requirements"
[16] AS ISO/IEC 27002:2015 "Information technology – Security techniques – Code of practice for information security controls"
[17] A. Calder and S. Watkins, "IT Governance: a manager's guide to data security and ISO 27001/ISO 27002", Kogan Page, 2008.
[18] A. Shostack, Threat modelling: designing for security, John Wiley & Sons, Inc. 10475 Crosspoint, BoulevardIndianapolis, IN 46256., 2014
[19] Department of Homeland Security (DHS), "NIST Cyber Security Framework", 2014, Available from: https://www.nist.gov/cyberframework/online-learning/components-framework.
[20] Federal Communications Commission (FCC), "Cyber Security Planning Guide", October 2012, Available from: https://transition.fcc.gov/cyber/cyberplanner.pdf, accessed August 2019
[21] D. Gibson, "Managing risk in information systems", Jones Bartlett Learning, Burlington MA 01803, 2015.
[22] K. Joiner et al., "Four testing types core to informed ICT governance for cyber-resilient systems", IARIA 2018, International journal on advances in security, issn1942-2636 vol.11,no.3&4,year2018, pp.313-327, Available from: http://www.iariajournals.org/security/, accessed August 2019
[23] R. Kissel, NISTIR 7621: "Small Business Information Security: The Fundamentals", 2009, Available from: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf, accessed August 2019
[24] Malwaretech, 2017, "How to Accidentally Stop a Global Cyber Attacks", MalwareTech,13 May 2017, Available from: https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
[25] Mandiant 2013, "APT1: exposing one of china's cyber espionage units", Mandiant, Available from: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, accessed August 2019
[26] NIST 2013, Security and Privacy Controls for Federal Information Systems and Organizations, "National Institute of Standards and Technology Special Publication 800-53", Revision 4 462 pages (April 2013) CODEN: NSPUE2 Available from: http://dx.doi.org/10.6028/NIST.SP.800-53r4, accessed August 2019
[27] NIST, "NIST special publication 800-31, National Institute of Standards and Technology Special Publication 800-53", 2019, Available from: https://nvd.nist.gov/800-53, accessed August 2019
[28] OWASP, Top 10-2017 Top 10, "Open Web Application Security Project", 2017, Available from: https://www.owasp.oeg/index.php/top_10-2017_Top_10, accessed August 2019
[29] C. Schou and S. Hernandez, "Information Assurance handbook: Effective computer security and risk management strategies", McGraw Hill Education. United States of America, 2015.
[30] A. Sedgewick, M. Souppaya, and K. Scarfone, "NIST Special Publication 800-167: Guide to Application Whitelisting", U.S Dept Commerce 2015, Available from: http://dx.doi.org/10.6028/NIST.SP.800-167, accessed August 2019
[31] Verizon Enterprise Solutions 2018, 2018 "Data Breach Investigations Report", Available from: https://enterprise.verizon.com/resources/reports/dbir/, accessed August 2019
[32] Verizon Enterprise Solutions 2019, 2019 "Data Breach Investigations Report", Available from: https://enterprise.verizon.com/resources/reports/dbir/, accessed August 2019
[33] S. Winterfeld and J. Andress, "The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice", Elsevier, Inc, United States of America, 2013.

 ISBN: 978-1-61208-743-6