Cyber 2 / CSIRW: The Challenges of Implementing Cyber in the Real World

Chair: Anne Coull

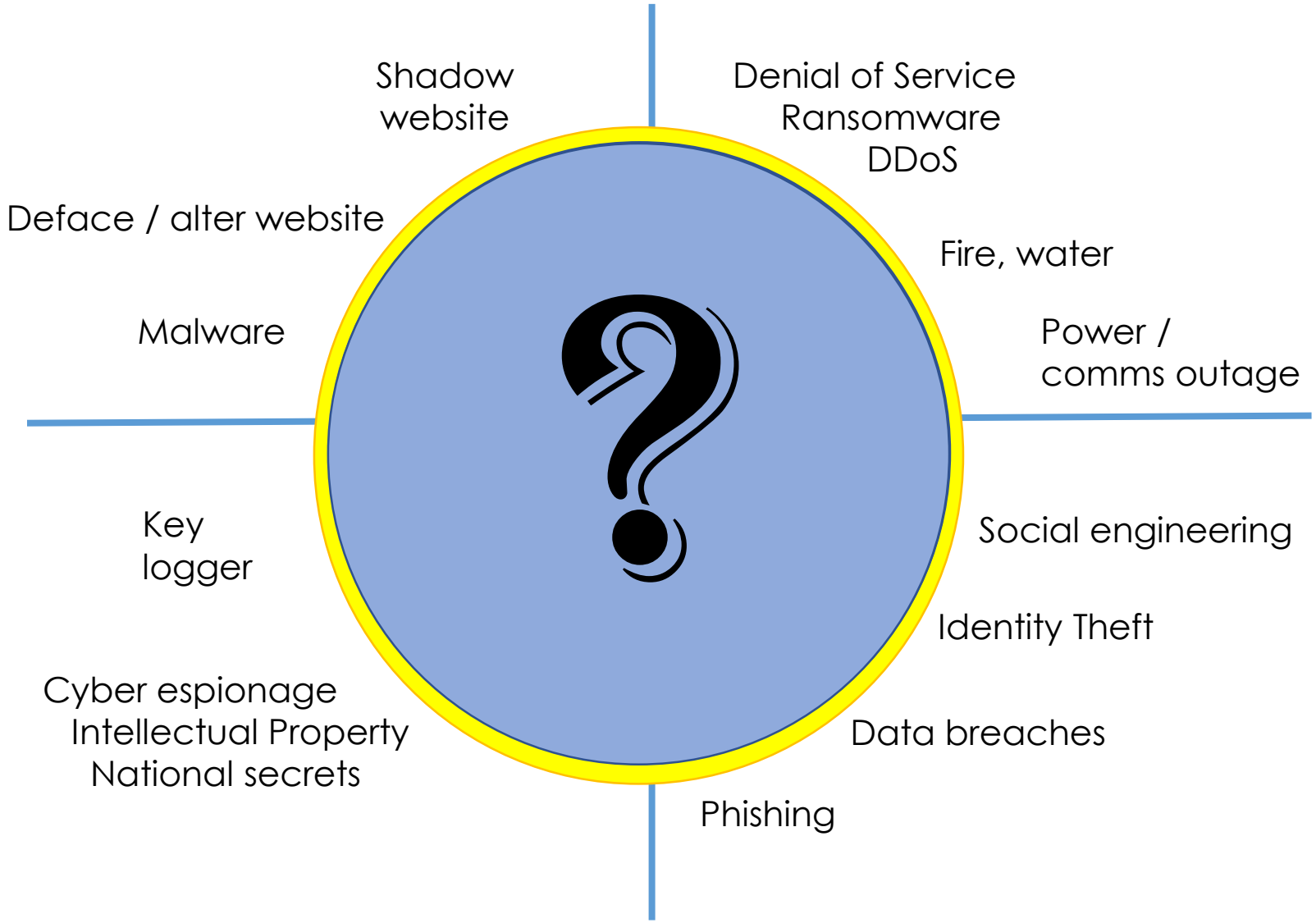
September 2019

How Much Cyber Security is Enough?

Anne Coull

September 2019

How much cyber security is enough?



Standards and Guidelines

Australian Prudential Regulation Authority
CPS 234

AS ISO/IEC 27001
AS ISO/IEC 27002

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Australian Signals Directorate

ISO 27001:2015 & ISO 27002:2015

AS ISO/IEC 27001:2015 Information technology – Security Techniques – Information security management systems – Requirements	**AS ISO/IEC 27002:2015** Information technology – Security techniques – Code of practice for information security controls
Organisational context & scope	Policies & procedures
Leadership, policy, roles & responsibilities	Organisation
Planning & Objectives	People – screening
Resourcing & Awareness	Asset management – ownership, classification
Operational planning & control (incl. risk assessment)	Access control
Performance evaluation: monitoring, measuring (audit)	Cryptographic controls
Improvement	Physical security
	Operations controls: malware, backups, vulnerability mgt, Audit
	Network security & information transfer
	System acquisition, SDLC
	Supplier Mgt
	Incident Mgt
	BCP & redundancies
	Legal & compliance

APRA CPS 234 & CPG 234

Australian Prudential Regulation Authority

CPG 234 Management of Security Risk in Information and Information Technology

CPS 234 Information Cybersecurity

- Policy
- User awareness
- Access control
- Lifecycle, SDLC
- Physical security
- Monitoring and incident management
- Assurance

Australian Signals Directorate (ASD)

Australian Signals Directorate

Top 4

- patching operating systems
- patching applications
- restricting administrative privileges
- application whitelisting

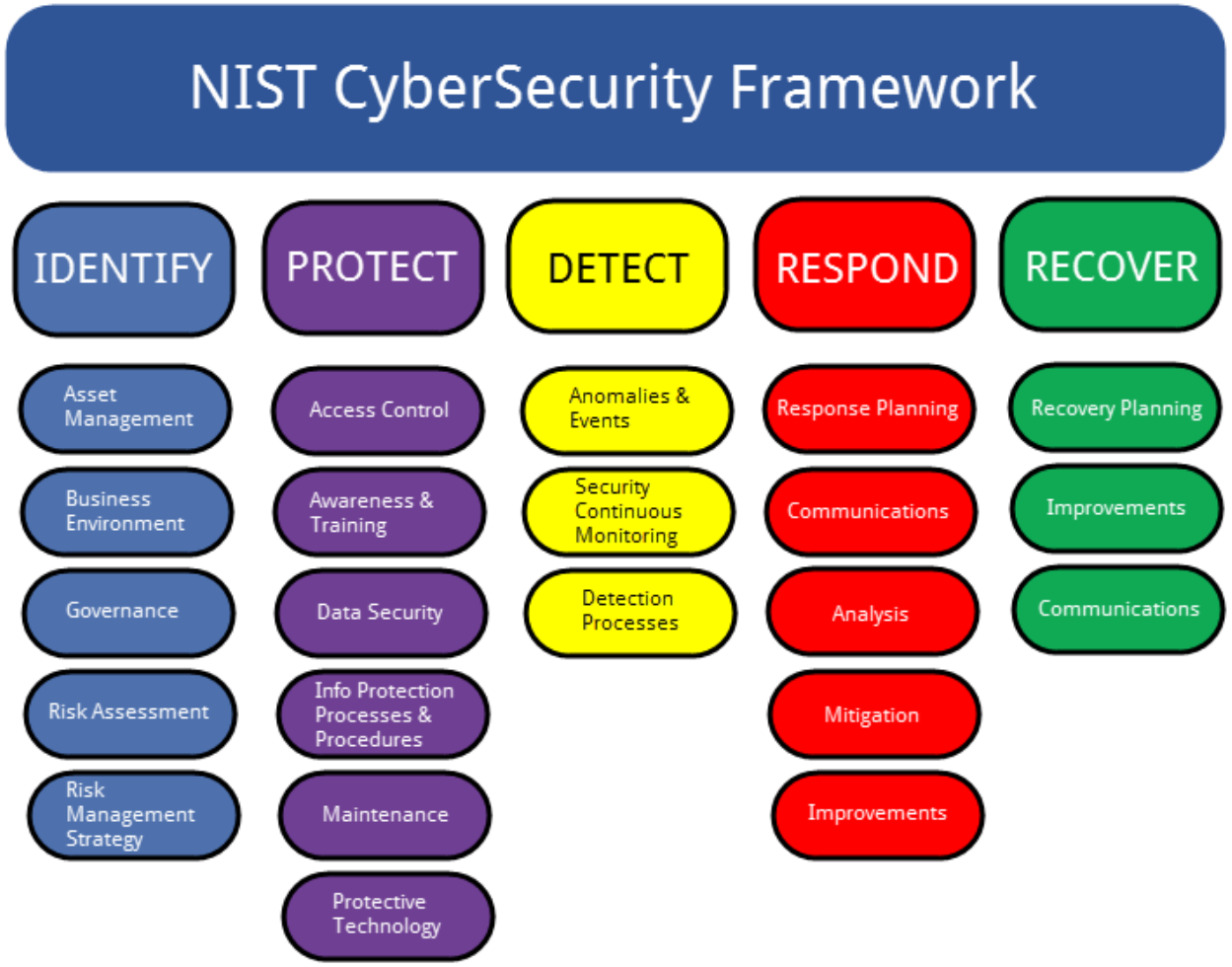
… Essential 8

- configuring Microsoft Office macro settings
- application hardening
- multi-factor authentication
- daily backups

… Top 37

NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Cyber Security Framework

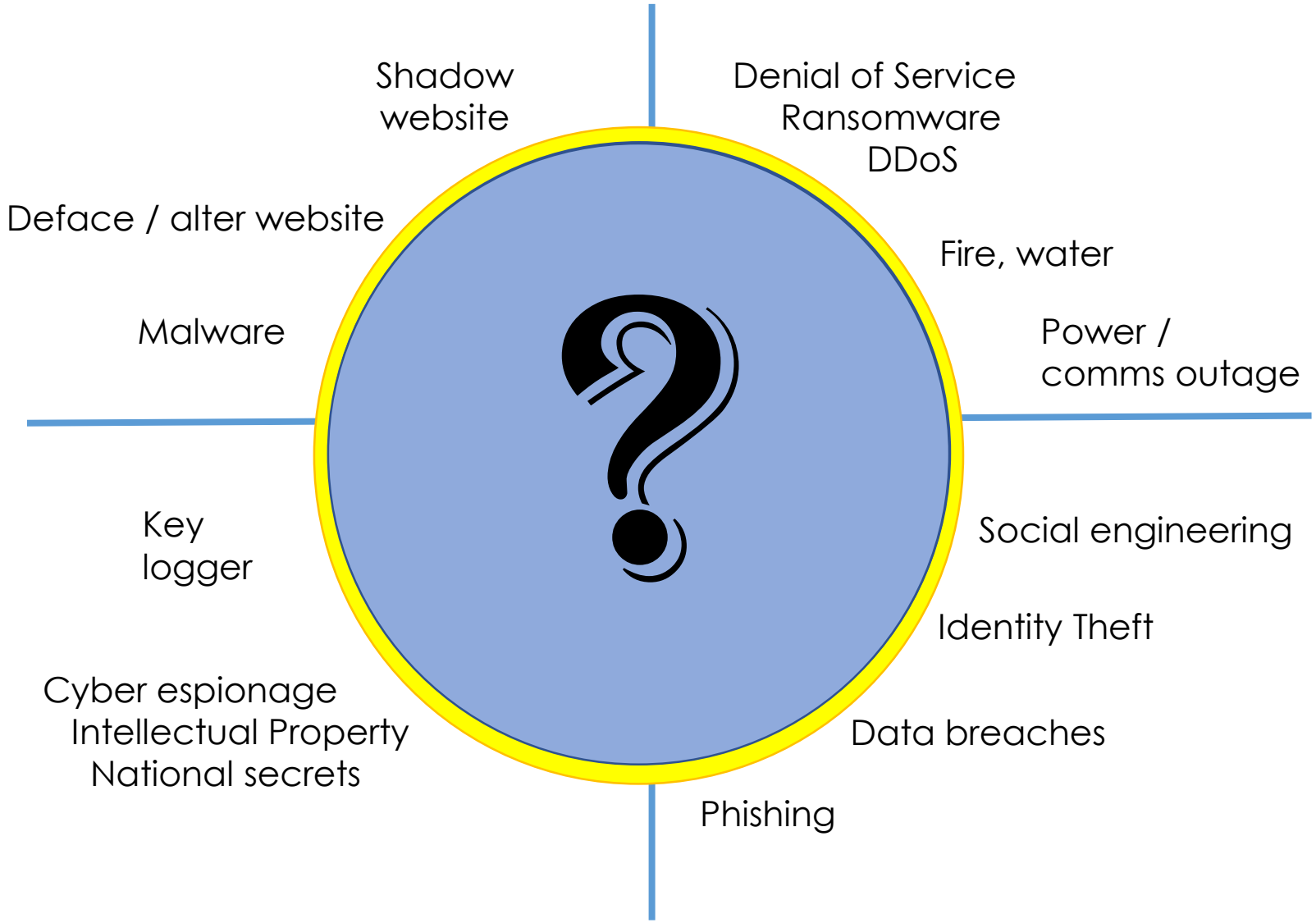
800-53 & 800-53A Security Controls and Objectives

800-53R4 Security and Privacy Controls for Federal Information Systems and Organisations

IR 7621 Small business fundamentals

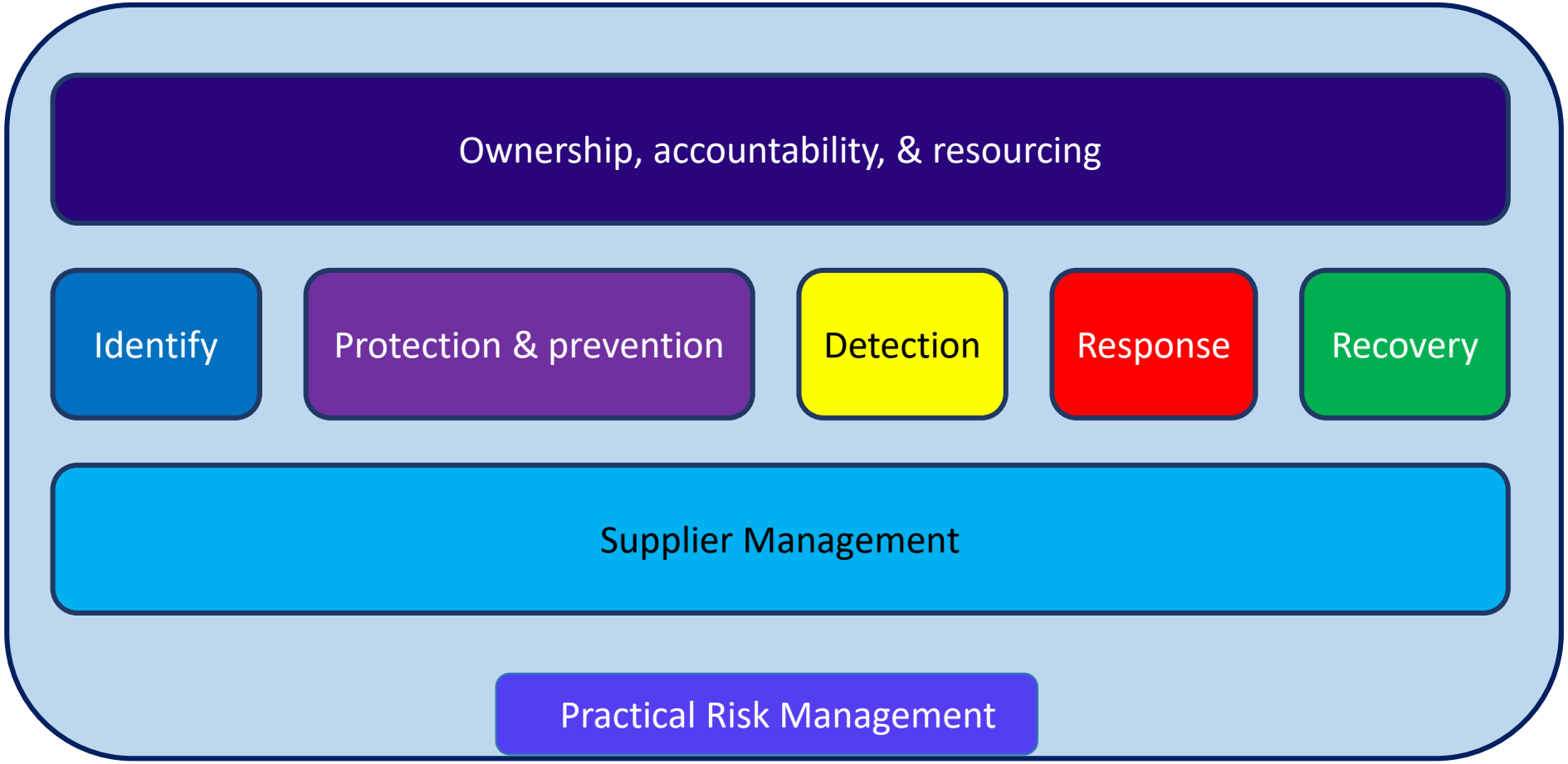
[19][23][26][27][30]

How much cyber security is enough?

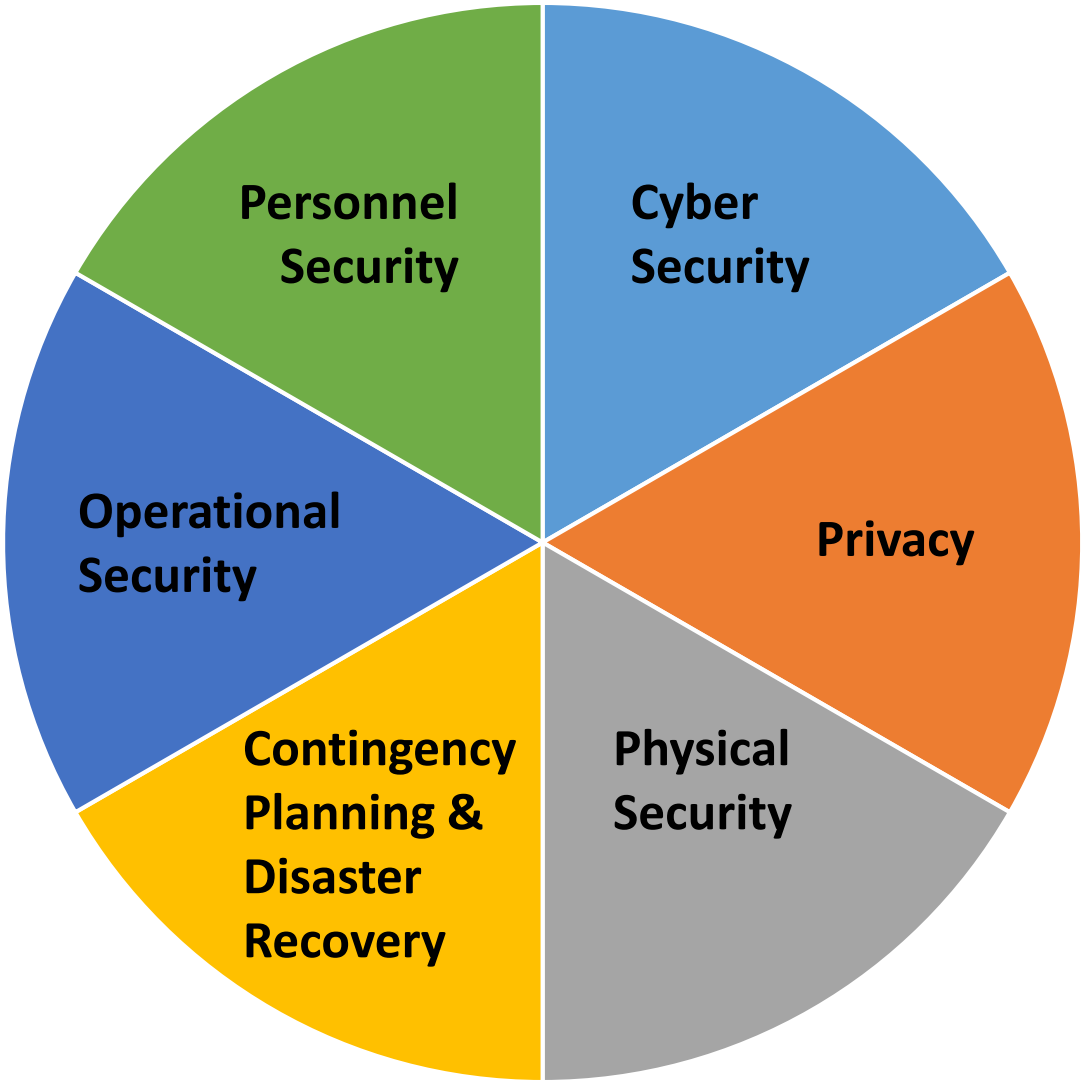


Cyber Security Strategy

People Policies Processes Technology



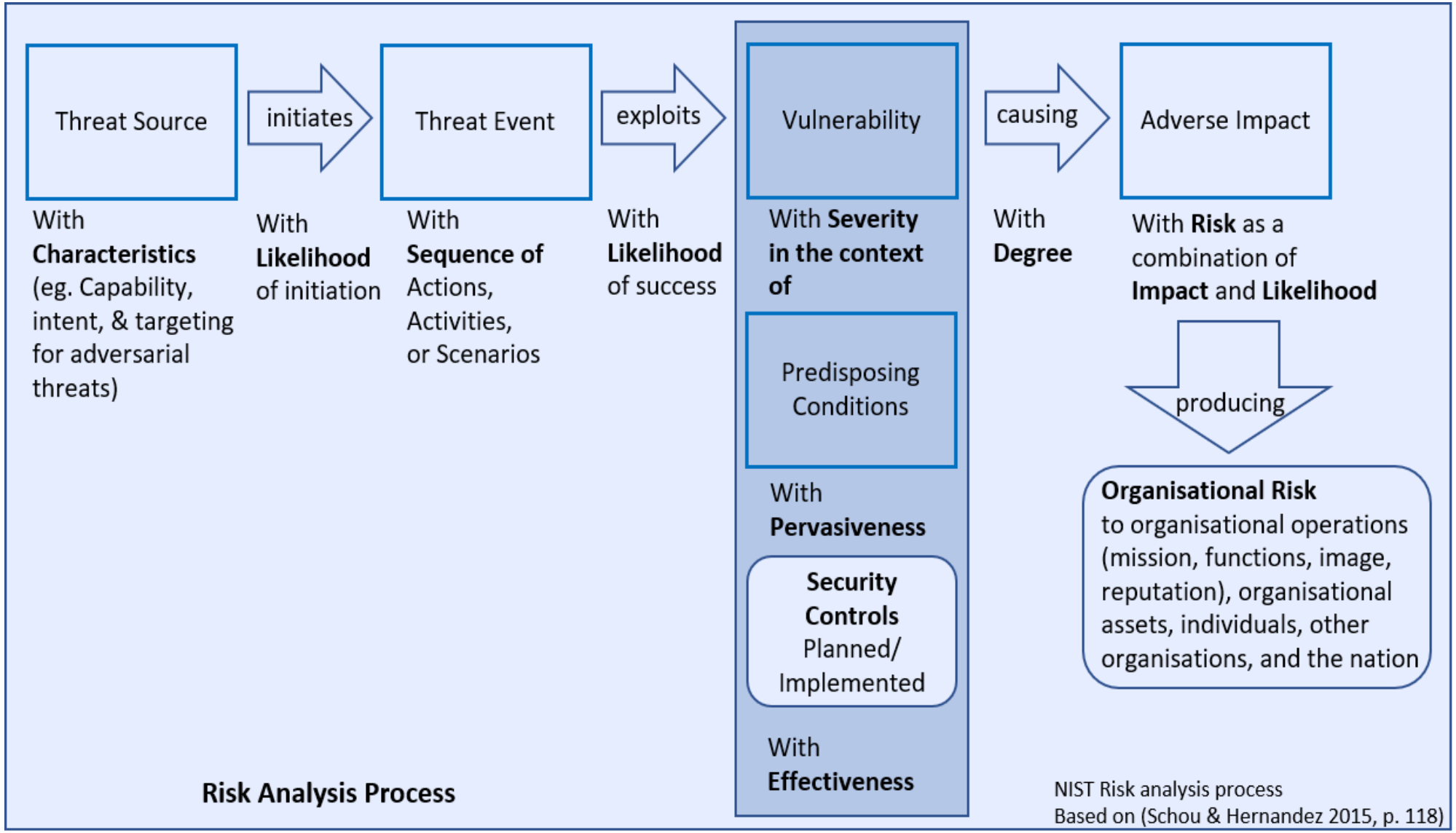
Cyber Security is an Enterprise Risk



...within the organizational context

Practical Cyber Risk Management

Within the organizational context:



Recommended Controls

Ownership, Accountability and Resourcing

Information Security Policy
Security team appropriately resourced
Trusted staff (background checks)
Develop a security culture by teaching employees how to protect their data

Protection and Prevention

Security for internet connection: hardware & software firewalls (configured!)
Control physical access to all computers and network components (subnets, security groups, monitor)
Secure the wireless access point and network
Harden DNS

Data storage: data loss prevention (disable USB, monitor)
Data storage: static encryption (classify)
Encrypt in transit
Encryption key management

Individual user accounts (passwords, privileges)
Data access - Needs to know
Multi-factor authentication
Separation of duties (SOD)

Anti-virus, malware, spyware
Disable macros
Application and IP/URL whitelisting
Patch operating systems and applications

Secure hardware disposal
Secure SDLC/ Application development

Continuous hosting of critical systems / uninterrupted data store (failover)
Uninterupted power, LAN, LAN-to-WAN comms, phone/VoIP/mobile

Identify and track vulnerabilities (scan, pen test)
Manage, prioritise, and close vulnerabilities

[1]-[16][19][20][22][23][26]-[28][30]-[32]

Recommended Controls

Detection

Log and analyse activities and events
Inbound email DNS authentication (DMARC, DKIM, SPF protocols)
Email scanning for SPAM, malicious links and attachments
Identify intrusions early
- Intrusion detection
- Security Information and Event Management (SIEM)

Response and Recovery

Backup important business information, test restore
DoS protection
Incident Management
Aust Privacy Act
Business Continuity

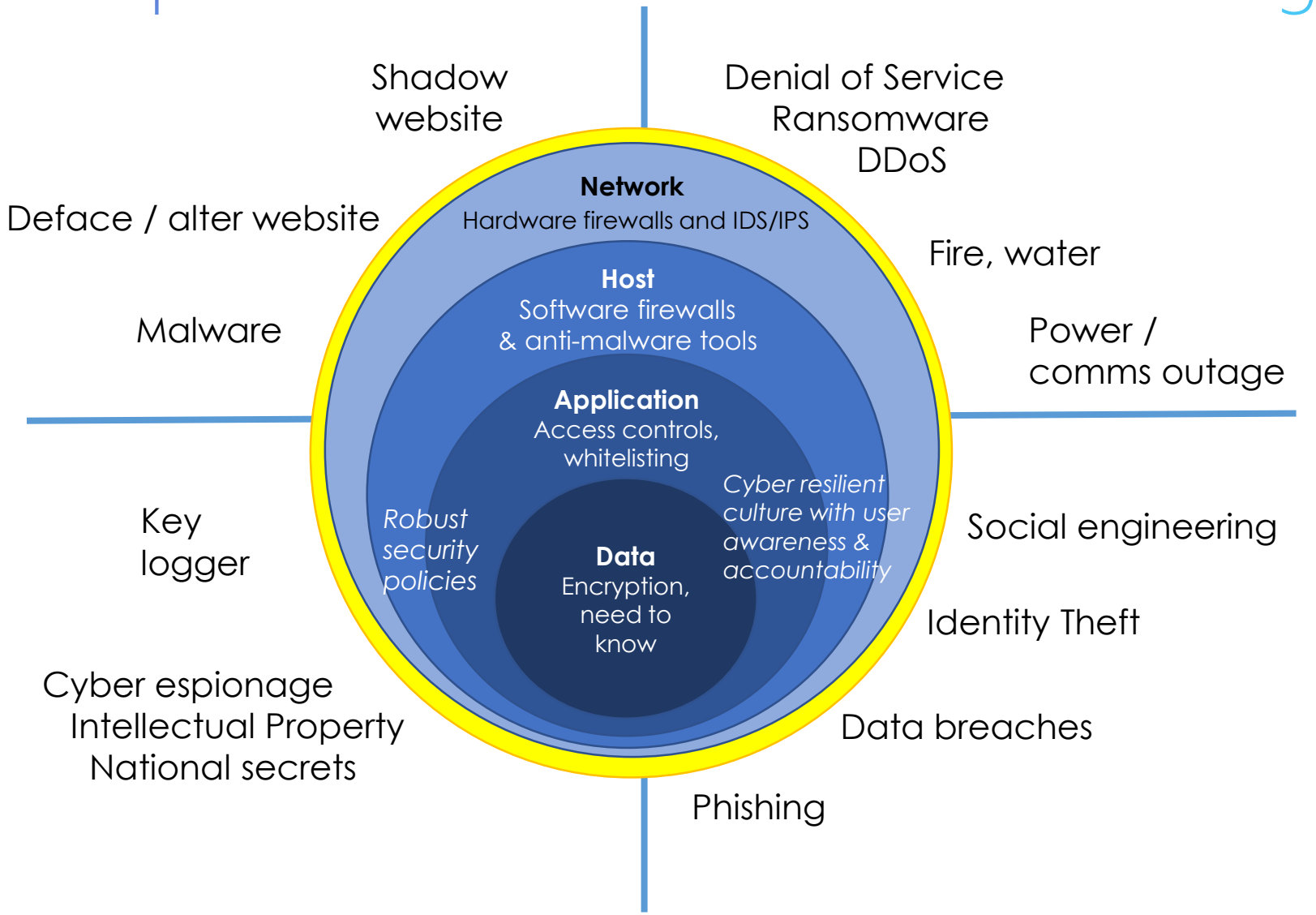
Outsourcing

Assure third party security

[1]-[16][19][20][22][23][26]-[28][30]-[32]

Attacks on Confidentiality, Integrity, Availability

People Policies Processes Technology



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. Australia Prudential Regulation Authority (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

Questions ???