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?

Denial of Service
Ransomware
DDoS
Identity Theft
Data breaches
Cyber espionage
Intellectual Property
National secrets
Shadow website
Deface / alter website
Malware
Key logger
Cyber espionage
Intellectual Property
National secrets
Phishing
Fire, water
Power / comms outage
Social engineering
Identity Theft
Data breaches
Confidentiality
Network
Host
Application
Data
People
Standards and Guidelines

Australian Prudential Regulation Authority
CPS 234

Australian Signals Directorate

AS ISO/IEC 27001
AS ISO/IEC 27002

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

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational context &amp; scope</td>
<td>Policies &amp; procedures</td>
</tr>
<tr>
<td>Leadership, policy, roles &amp; responsibilities</td>
<td>Organisation</td>
</tr>
<tr>
<td>Planning &amp; Objectives</td>
<td>People – screening</td>
</tr>
<tr>
<td>Resourcing &amp; Awareness</td>
<td>Asset management – ownership, classification</td>
</tr>
<tr>
<td>Operational planning &amp; control (incl. risk assessment)</td>
<td>Access control</td>
</tr>
<tr>
<td>Performance evaluation: monitoring, measuring (audit)</td>
<td>Cryptographic controls</td>
</tr>
<tr>
<td>Improvement</td>
<td>Physical security</td>
</tr>
<tr>
<td></td>
<td>Operations controls: malware, backups, vulnerability mgt, Audit</td>
</tr>
<tr>
<td></td>
<td>Network security &amp; information transfer</td>
</tr>
<tr>
<td></td>
<td>System acquisition, SDLC</td>
</tr>
<tr>
<td></td>
<td>Supplier Mgt</td>
</tr>
<tr>
<td></td>
<td>Incident Mgt</td>
</tr>
<tr>
<td></td>
<td>BCP &amp; redundancies</td>
</tr>
<tr>
<td></td>
<td>Legal &amp; compliance</td>
</tr>
</tbody>
</table>
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
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
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
How much cyber security is enough?

Shadow website

Denial of Service
Ransomware
DDoS

Fire, water
Power / comms outage

Social engineering
Identity Theft
Data breaches
Phishing

Cyber espionage
Intellectual Property
National secrets

Key logger
Malware
Deface / alter website
Cyber Security Strategy

People  Policies  Processes  Technology

Ownership, accountability, & resourcing

Identify  Protection & prevention  Detection  Response  Recovery

Supplier Management

Practical Risk Management
Cyber Security is an Enterprise Risk

Personnel Security

Operational Security

Contingency Planning & Disaster Recovery

Cyber Security

Privacy

Physical Security

...within the organizational context
Practical Cyber Risk Management

Within the organizational context:

**Risk Analysis Process**

- **Threat Source**: With Characteristics (e.g., Capability, intent, & targeting for adversarial threats)
- **Threat Event**: With Likelihood of initiation
- **Vulnerability**: With Sequence of Actions, Activities, or Scenarios, Likelihood of success
- **Adverse Impact**: Causing with Risk as a combination of Impact and Likelihood

**Organisational Risk**

to organisational operations (mission, functions, image, reputation), organisation assets, individuals, other organisations, and the nation

NIST Risk analysis process
Based on (Schou & Hernandez 2015, p. 118)
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)
Uninterrupted power, LAN, LAN-to-WAN comms, phone/VoIP/mobile

Identify and track vulnerabilities (scan, pen test)
Manage, prioritise, and close vulnerabilities
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
Attacks on Confidentiality, Integrity, Availability
People Policies Processes Technology

Network
- Shadow website
  - Denial of Service
  - Ransomware
  - DDoS

Host
- Malware
  - Deface / alter website
  - Fire, water
  - Power / comms outage

Application
- Key logger
  - Social engineering
  - Data breaches
  - Identity Theft

Data
- Cyber espionage
  - Intellectual Property
  - National secrets
  - Data breaches

Robust security policies
- Cyber resilient culture with user awareness & accountability
- Encryption, need to know

Access controls, whitelisting
- Hardware firewalls and IDS/IPS
- Software firewalls & anti-malware tools

Software firewalls & anti-malware tools
- Application
- Access controls, whitelisting
- Hardware firewalls and IDS/IPS

Hardware firewalls and IDS/IPS
- Network
- Shadow website
- Deface / alter website
- Malware
- Key logger
- Cyber espionage
- Intellectual Property
- National secrets

Encryption, need to know
- Data
- Cyber resilient culture with user awareness & accountability
- Application
- Access controls, whitelisting
- Hardware firewalls and IDS/IPS

Application
- Access controls, whitelisting
- Hardware firewalls and IDS/IPS
- Software firewalls & anti-malware tools

Software firewalls & anti-malware tools
- Application
- Access controls, whitelisting
- Hardware firewalls and IDS/IPS

Host
- Malware
  - Deface / alter website
  - Fire, water
  - Power / comms outage

Network
- Shadow website
  - Denial of Service
  - Ransomware
  - DDoS
Questions ???