Enabling Priorities

Cyber Security

May 2022

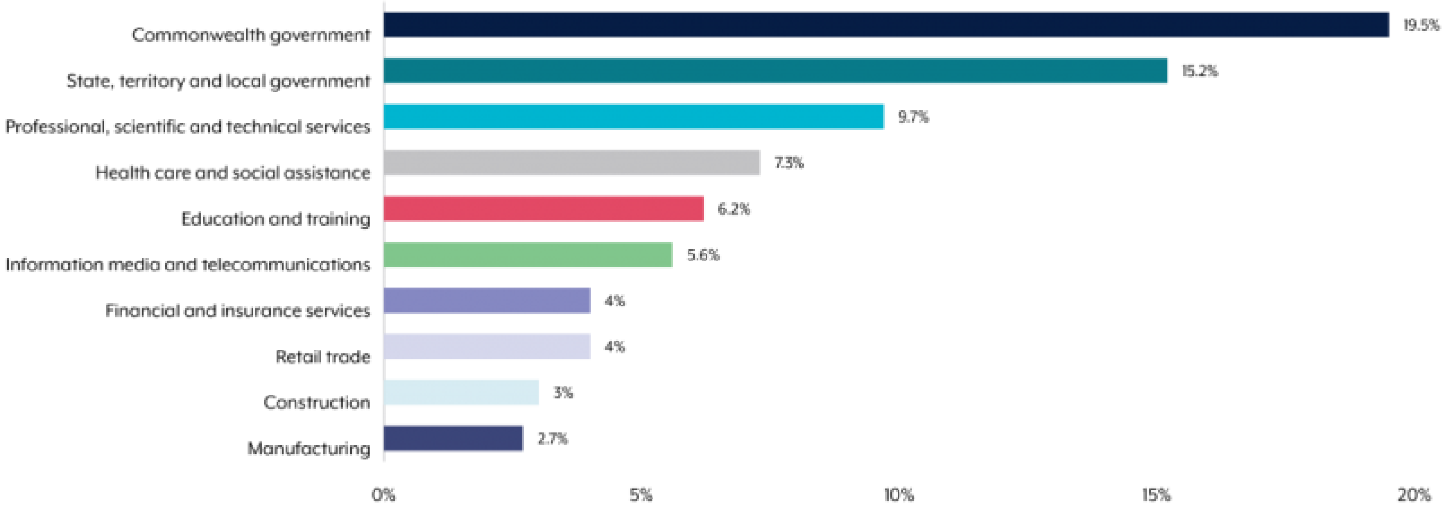
Information Management

CITY OF ADELAIDE

Cyber Security April 2022

Background

- Over **67,500** cybercrime reports received, an increase of nearly **13 %**
- Over **1,500** cybercrime reports of malicious cyber activity related to the coronavirus pandemic (approximately four per day).
- Nearly **500** ransomware cybercrime reports, an increase of nearly **15 %**



Reference: ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au

Top Cyber Threats in 2020-21

- Exploitation of the pandemic environment
- Disruption of essential services and critical infrastructure
- Ransomware
- Rapid exploitation of security vulnerabilities
- Supply chains
- Business email compromise (BEC)

Cyber Security April 2022

What’s next for Frontier

Short Term

- Build brand new corporate network
- Extend the requirement for
and usage of MFA
- Review and enhance where required Remote Access methods
- Review and enhance where required Software updates and patching policy

Medium Term

- Dedicated CISO
- Review and enhance where required Password change policy
- BYOD policy
- Network Monitoring & centralised logging
- Accelerate phase out unsupported O/S
- Implementation of Managed Security Services
- Windows hardening to servers

Long Term

- Review business and data security processes
- Regularly scan corporate servers and other end points
- Enhance ongoing internal educations regarding data security and tie into KPI
- Review all corporate restored servers for client data and action appropriately

Cyber Security April 2022

What have we done

CoA has significantly improved our cyber security posture thanks to our Payment Card Industry (PCI) obligation

CoA has applied PCI best practices across much of our Information and Communication Technologies (ICT) infrastructure and assets

Improved our contracts to cover data security obligations

What are we doing

CoA is working through its implementation of the ACSC Essential Eight Maturity Framework

> “The Essential Eight is a series of baseline prioritized mitigation strategies taken from the Strategies to Mitigate Cybersecurity Incidents recommendations for organizations.”

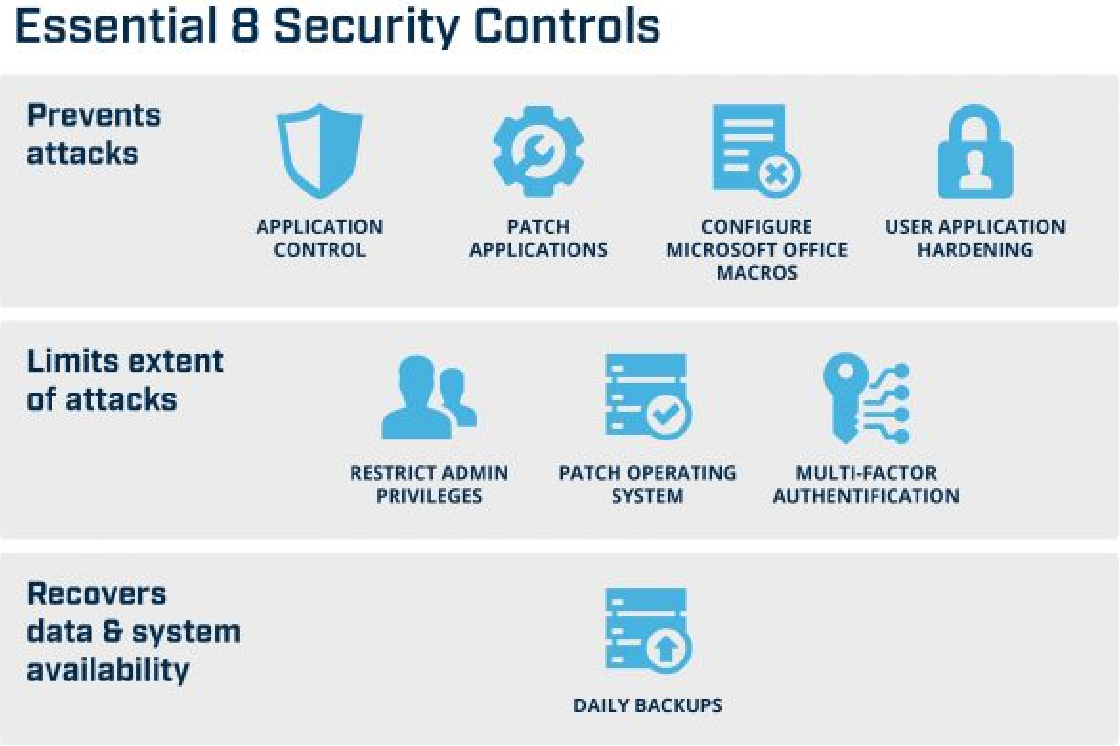
Australian Government

Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Security April 2022

How do we stack up



Essential 8 Security Controls

Prevents attacks

APPLICATION CONTROL

PATCH APPLICATIONS

CONFIGURE MICROSOFT OFFICE MACROS

USER APPLICATION HARDENING

Limits extent of attacks

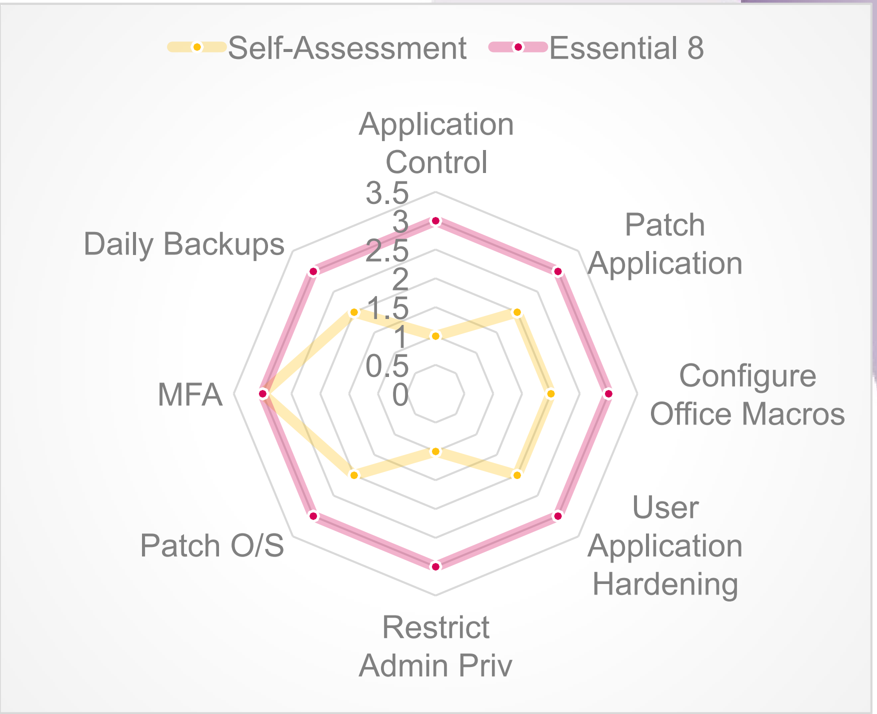
RESTRICT ADMIN PRIVILEGES

PATCH OPERATING SYSTEM

MULTI-FACTOR AUTHENTIFICATION

Recovers data & system availability

DAILY BACKUPS



What are the ongoing risks / challenges

Our people

- Our people are our biggest risk and opportunity…must have a cyber security culture
- Cyber security is not just for IM to do, security is everyone’s business
  - The Frontier example is technically a data breach, not a cybersecurity incident…

Legacy Application

- CoA still has several legacy applications that are holding us back
- Business Systems Roadmap is helping to mitigate these risks

Suppliers

- We are at the mercy of some of our suppliers, we need to ensure that we select suppliers that meet or exceed our cyber and data security requirements and needs, this may at times come at a higher cost.

Cyber Security April 2022

What are we planning

- Improving organisational awareness of cyber security
- Audit our current controls against the Essential Eight
- Test our users and systems against potential threats (real world exercise)
- Continue to work with LG Sector to improve cyber security as a whole