Cybersecurity Update

Strategic Alignment - Enabling Priorities

Public

Tuesday, 21 March 2023

City Finance and Governance Committee

Program Contact:
Sonjoy Ghosh, Manager Information Management

Approving Officer:
Steve Zaluski, Acting Chief Operating Officer

EXECUTIVE SUMMARY

At the meeting of 28 October 2022, the Audit and Risk Committee discussed the importance of matters relating to data breaches and recognised that cyber security is an emerging key risk for Council.

Council has identified cybersecurity and related matters as a strategic risk to Council prior to 2020 and reports against key performance indicators regularly through the Strategic Risk and Internal Audit group. Since 2020 Council has progressively increased its resilience to cyber threats through the introduction of mitigating controls such as mandatory cyber security training for all system users, regular audits, incident management processes, and alignment to cybersecurity best practice.

Council has also worked closely with the Local Government Information Technology of South Australia (LGITSA) to help elevate the local government sector in cyber security awareness and capability.

This report provides an update on our approach to mitigate cyber security risk, and our plans to further improve our resilience to cyber threats. The Audit and Risk Committee have endorsed the four-year plan in Attachment A.

RECOMMENDATION

THAT THE CITY FINANCE & GOVERNANCE COMMITTEE RECOMMENDS TO COUNCIL:

That Council

1. Notes the cyber security principles that provide strategic guidance on how we protect our systems and data from cyber threats.
2. Notes Council's current baseline achievement against the Essential Eight maturity model.
3. Endorses the four-year plan in Attachment A to Item 6.3 on the Agenda for the meeting of the City Finance and Governance Committee held on 21 March 2023.

IMPLICATIONS AND FINANCIALS

City of Adelaide 2020-2024 Strategic Plan	Strategic Alignment – Enabling Priorities To support the Council's delivery of strategic objectives by securely enabling its initiatives and operations while protecting it from threats to the availability, integrity, and confidentiality of systems and data from ongoing cyber threats.
Policy	Not as a result of this report.
Consultation	Not as a result of this report.
Resource	Not as a result of this report.
Risk / Legal / Legislative	The regular monitoring and reporting of the Council's cyber security is a key step in mitigating risks events that could impact the delivery of the Strategic Plan and Business Plan and Budget.
Opportunities	The proposed annual reporting of the Council's cyber security is a key step in maturing the organisation's overall understanding and mitigation of cyber threats.
22/23 Budget Allocation	Not as a result of this report.
Proposed 23/24 Budget Allocation	Not as a result of this report.
Life of Project, Service, Initiative or (Expectancy of) Asset	Not as a result of this report.
22/23 Budget Reconsideration (if applicable)	Not as a result of this report.
Ongoing Costs (eg maintenance cost)	Not as a result of this report.
Other Funding Sources	Not as a result of this report.

DISCUSSION

Background

1. Council has been improving its cyber security resilience for over 3 years, which was driven by our requirement to meet certain conditions of our transactional banking contract. Under our transactional banking contract, Council must be compliant with the Payment Card Industry (PCI) Data Security Standard (DSS). PCI-DSS introduced several new controls, both technical and non-technical to ensure, the protection of credit card details.
2. Cyber threats are increasing every year and we must create a strong organisational culture of cybersecurity. Cybersecurity is no longer just an IT issue. Everyone has a role to play to prevent a cyber incident from occurring.

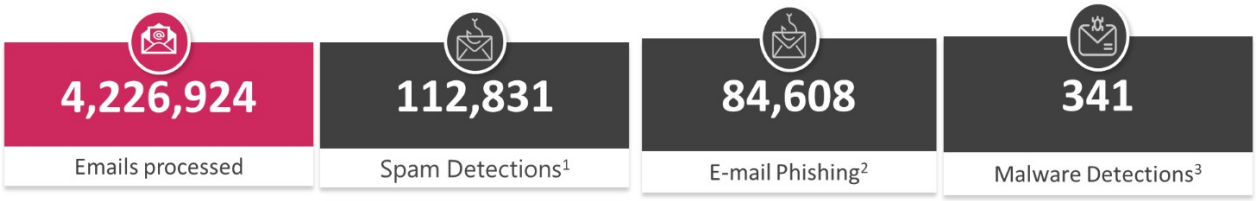
Cyber Security Risk Landscape

3. There are six key risks associated with cyber security:
   - 3.1. Disruption to service, in which criminals seek to deny access, disrupt, deface, or gain access to our systems and resources.
   - 3.2. Reputational risks which can be caused by cyber incidents being highly visible in the media and/or broadly reported and discussed.
   - 3.3. Criminals obtain valuable data that can be used for ransom, threatening to divulge information unless we pay.
   - 3.4. Potential for substantial financial impact through loss of productivity or penalties and fines.
   - 3.5. Third-party risk as we partner and collaborate with more organizations that may not be as mature in their cyber security practices.
   - 3.6. Regulatory and compliance risks if we fail to meet contractual and/or legal obligations.

Cyber threat statistics

4. The statistics in Figure 1 below demonstrate the volume of potential cyber threats observed by the Council in the past six months.

Figure 1: Cyber threats in the past 6 months



Four Pillars of Cyber Security Principles

5. As Council matures in its approach to cyber security, we must align to cyber security principles. The principles are to provide strategic guidance on how we can protect our systems and data from cyber threats. These cyber security principles are grouped into four key pillars:
   - 5.1. **Govern**: Identifying and managing security risks.
   - 5.2. **Protect**: Implementing controls to reduce security risks.
   - 5.3. **Detect**: Detecting and understanding cyber security events to identify cyber security incidents.
   - 5.4. **Respond and Recover**: Responding to and recovering from cyber security incidents.

Controls that are in place now

6. Council has already implemented several controls over the past 3 years driven by the requirements of PCI-DSS.
7. A summary of the controls in place are outlined below:
   - 7.1. Mandatory cybersecurity training for all system users – 'Be Security Smart'.
   - 7.2. Developed cybersecurity incident management operating guideline.
   - 7.3. Multi-factor authentication process

7.4. Ongoing implementation of server, desktop, and application hardening based on industry standards.

7.5. Ongoing monthly patching of all servers, network equipment, and desktop environments

7.6. Annual upgrades to corporate applications to ensure they are up-to-date and supported by the vendor.

7.7. Updated contractual terms to ensure adequate cyber and data security obligations by suppliers and vendors.

7.8. Established a cybersecurity analyst role within Information Management

7.9. Implemented quarterly vulnerability scans.

7.10. Implemented annual cybersecurity penetration tests.

Essential Eight Control Strategies

8. Council has aligned its approach to cyber security with the Australian Cyber Security Centre (ACSC) Essential Eight. The Essential Eight are a set of technical control strategies targeted at preventing cyber intrusions, ransomware, and other malicious events, limiting their damage, and enabling organisations to recover if they occur.

8.1. The Essential Eight is a cybersecurity self-assessment maturity tool "to help organisations mitigate cyber security incidents caused by various cyber threats" and has been designed to protect Microsoft Windows-based internet-connected networks. The controls are focused on eight key mitigation areas.

8.2. To assist organisations in protecting themselves from cyber threats, the ACSC developed a three-tier maturity model for the Essential Eight.

8.2.1. Maturity Level Zero: Not yet aligned with the intent of the mitigation strategy.

8.2.2. Maturity Level One: Partly aligned with the intent of the mitigation strategy.

8.2.3. Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.

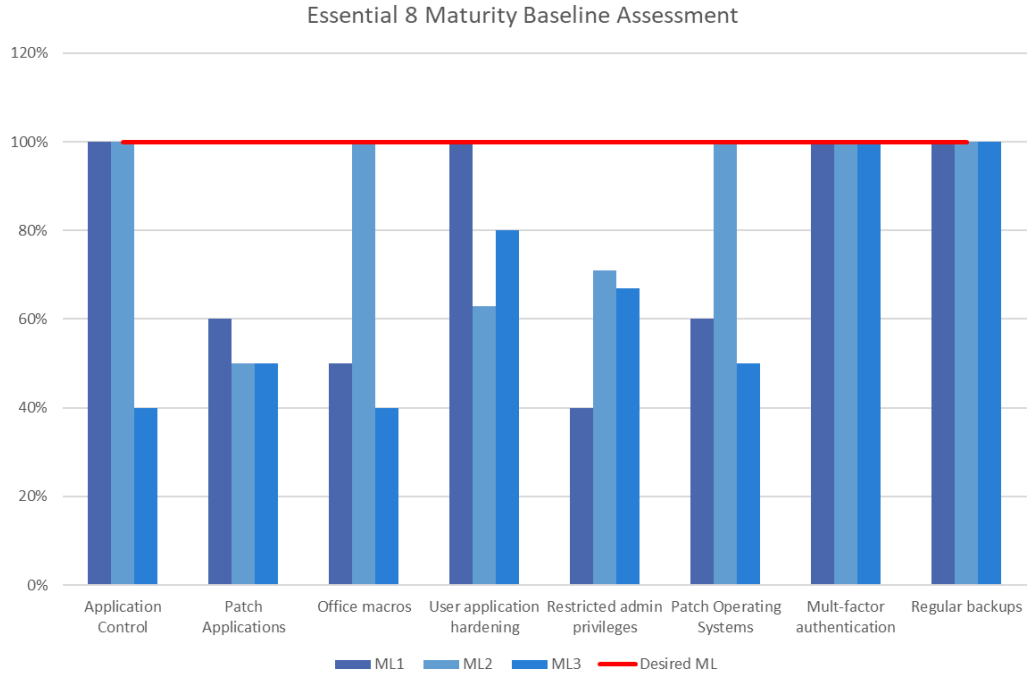
8.2.4. Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

8.3. Each of these Maturity Levels must be achieved individually.

8.4. The Essential Eight is seen as the baseline of cyber security maturity and is just one part of a wider framework that agencies need to have in place.

8.5. In 2022, Council conducted an external assessment against the Essential Eight model. The result of the initial assessment is provided in Figure 2 below. We are currently faring well with the target being to have all bars reached the desired Maturity Level (red bar), this will take 2 to 3 years to achieve.

Figure 2: Essential Eight assessment results



Audit and Risk Committee Advice

9. On the 3 February 2023, the Audit and Risk Committee (ARC) met and considered this item.
10. ARC noted the cyber security principles that provide strategic guidance on how we protect our systems and data from cyber threats.
11. ARC also noted Council's current baseline achievement against the Essential Eight maturity model.
12. ARC recommended Council endorse the four-year plan which is contained in **Attachment A**.

Next Steps

13. To improve our cyber security resilience, we have developed a four-year plan of activities in **Attachment A** that will improve our cyber security across all four pillars. Key activities include:
    - 13.1. Assessment against the recently released LGITSA cyber security framework. This is planned to be completed by April 2023.
    - 13.2. Development of an annual independent cyber security testing and auditing program.
    - 13.3. Review current capacity and capability and ensure efficient and effective resources are in place.
14. Continue to partner with the Government of South Australia and SA Police in improving our cyber resilience and work with the local government sector to increase cyber maturity.

ATTACHMENTS

Attachment A – Cybersecurity four-year plan

- END OF REPORT -