Confidential Item

CAMPBELLTOWN CITY COUNCIL

Confidential Item

For Council meeting to be held on

Tuesday 17 September 2024 at 7.00 pm

Refer Item 11.13

Confidential Item

11.13 ICT Improvement

Manager Information & Communication Technology, Tarun Sidhwani's Report

Purpose of Report

To consider improvements to Council's ICT network.

Strategic Plan Link

Focus Area 5.3.2 Effective, up-to-date, stable and secure IT systems that meet the needs of our people and the Community

Previous Council/Committee Resolution

Nil.

Background

In June 2024, Staff engaged CyberCX through the Local Government Risk Services (LGRS) Cyber Security Uplift Program to conduct an Essential Eight Maturity Assessment. The assessment was initiated to better understand Council's information security environment and initiate discussions around options and priorities for improvement.

CyberCX assessed Council's information security against the Australia Cyber Security Centre (ACSC) Essential Eight framework, highlighting in their outcomes report the need to implement network segmentation as a key recommendation.

In July 2024, Staff also engaged 3Columns to conduct a comprehensive security assessment of the network to expose any existing vulnerabilities. These assessments use various penetration testing techniques to assist organisations to understand the risks and security posture of the existing information technology environment. Through this assessment and subsequent report, 3Columns reiterated the importance of Council implementing network segmentation to protect its internal network.

These recent assessments by external companies, focused on evaluating the Essential Eight maturity level, have reinforced the importance of implementing network segmentation.

Discussion

This report seeks support from Council to configure and implement a ICT network segmentation.

As part of an ongoing commitment to enhancing Council's cybersecurity position, a recent assessment of the Essential Eight maturity level was conducted by an external cybersecurity firm. The assessment identified several areas for improvement, with the implementation of network segmentation being a key recommendation.

Network segmentation is crucial for strengthening security by isolating sensitive data and critical systems from other areas of the network. For Council, setting up segmentation would help to minimise and contain potential security breaches as it would limit the ability of a malicious attacker to move laterally across the network and access confidential information. By segmenting Council's internal network, Staff can also enforce stricter access controls, ensuring that only authorised Staff can access specific segments, further reducing the risk of unauthorised access and data breaches.

The need for network segmentation has been further underscored by the increasing complexity of cyber threats and the growing regulatory demands for data protection and compliance. In response to these challenges, the proposal to implement network segmentation has been discussed and supported by the Executive Management Team.

Staff recommend that improvements to network security be implemented as soon as practical to align arrangements with broader industry best practice and advance Council's maturity level in cybersecurity.

Social Implications

There are no social implications in relation to this report.

Environmental / Climate Change Implications

There are no environmental / climate change implications in relation to this report.

Asset Management Implications

There are no asset management implications in relation to this report.

Governance / Risk Management

Delaying or not implementing network segmentation poses significant risks to Council's internal network security. Currently Council's network operates as a single entity and lacks the ability to enforce granular access controls across its network, enabling users and devices to have more access to network resources than necessary. This increases the risk of unauthorised access to sensitive data and makes it easier for cyber attackers to gain access, putting Council's data at risk.

In addition, without network segmentation, containing a security incident becomes much more difficult and costly to rectify. This can lead to prolonged downtime, increased recovery costs, and greater overall reputational risk to Council. The absence of network segmentation also hinders compliance with the Essential Eight framework.

Community Engagement

There are no Community engagement implications in relation to this report.

Regional Implications

There are no regional implications in relation to this report.

Economic Development Implications

There are no economic development implications in relation to this report.

Financial Implications

The design and implementation of network segmentation is anticipated to cost $22,000 (exc GST) as it will necessitate hiring external consultants to ensure proper configuration and integration with existing systems. As there are no funds in the budget and due to the importance of this initiative, Staff are recommending that this work be undertaken as soon as practical and the cost be recognised in the First Budget Review for 2024/2025.

Recommendation

That Council:

- **note the implications of cyber security risks and the recommendations from various suppliers and**
- **request Staff to implement the network segmentation necessary to minimise the risk and impact of a cyber attack as soon as practicable and**
- **allocates $22,000 (ex GST) at the First Budget Review 2024/2025 as a New Initiative for the installation of the Network Segmentation.**