

9 Confidential Items**9.1 2020-21 ACSC Annual Cyber Threat Report****Report Reference** FAC211012F9.1**Moved Ms Rantanen****Seconded Mr Papa**

That pursuant to Section 90(2) and (3)(e) of the *Local Government Act 1999*, the Council orders that all persons present, with the exception of the following persons: Chief Executive Officer, General Manager City Development, General Manager Corporate Services, General Manager City Services, Manager Office of the CEO, Chief Financial Officer, Manager IT Operations, Unit Manager Governance and Council Support and Governance Officer, be excluded from the meeting as the Council receives and considers information relating to 2020-21 ACSC Annual Cyber Threat Report, upon the basis that the Council is satisfied that the requirement for the meeting to be conducted in a place open to the public has been outweighed by the need to keep consideration of the matter confidential given the information relates to internal and external security assessments.

Carried Unanimously

3.40pm the meeting went into confidence.

Moved Ms Rantanen**Seconded Mr Papa**

The Manager IT Operations introduced the item and provided the following summary:

- Solutions will be automated through the newly appointed cyber security lead
- The report identified actions and processes that had not been completed, however this has been acknowledged and staff are attending to this and undertaking remediation work. The risk was identified, and staff are actively working through the solutions.
- One of the immediate actions is to replace the firewalls and wi-fi which will provide a clean slate for one third of the infrastructure.
- The organisation is aiming for all systems to be cloud based which will reduce the liability to Council as these third parties have a higher level of security.
- The removal of redundant hardware will also go a long way to reducing any threat.
- A further in-depth assessment will be carried out to identify vulnerabilities (not yet started)

The Committee provided the following comments:

- The report was alarming. The Committee had concerns over the level of insurance being \$ 500k only, identifying that this may never be enough.
- The Committee also raised concerns around the significant number of items to be addressed by December 2021 and whether this was realistic with current IT resources. Management was comfortable with the timeframes, noting the capabilities of staff coming on board enabling the team to stand up systems quickly, removing redundant hardware and installing only necessary new equipment.
- Suggested a regular update be provided to each committee meeting.

- It is good to have externals review the report and processes, however if they do not have the expertise or understanding on how to remedy the issues and provide realistic recommendations, this could be problematic.
- Queried how this ties-in with the internal audit plan and tracking of the cyber security recommendations.
- The Committee suggested going above the essential eight standards. Management confirmed they are aiming for an ISO27001 assessment; however this could not be contemplated until the essential eight had been completed by the December 2021 timeframe.
- Raised concerns that processes were not effectively being managed against the framework and questioned the controls that were in place to monitor this. Staff confirmed the work they were doing with the software would go towards addressing the reporting vulnerabilities. Insights and mandated reporting would be provided on a regular basis with defined timeframes to those who are not undertaking the work.

Moved Ms Rantanen

Seconded Mr Papa

That the Finance and Audit Committee:

1. Notes the report
2. Notes that IT services are working to implement security practices and structures
3. Notes that an update will be brought to each Finance and Audit Committee meeting which will include the tracking and progress of recommendations.
4. In accordance with Section 91(7) and (9) of the *Local Government Act 1999* the Council orders that this report, 2020-21 ACSC Annual Cyber Threat Report, any appendices and the minutes arising from this report having been considered in confidence under Section 90(2) and (3)(e) of the Act, except when required to effect or comply with Council's resolution(s) regarding this matter, be kept confidential and not available for public inspection for a period of 12 months from the date of this meeting. This confidentiality order will be reviewed at the General Council Meeting in December 2021.

Carried Unanimously

4.01pm the meeting came out of confidence.