Item #6.9
ISC: UNRESTRICTED
AC2018-0410

City Auditor's Report to
Audit Committee
2018 April 17

CYBER SECURITY INCIDENT RESPONSE AUDIT

EXECUTIVE SUMMARY

The City Auditor's Office issued the Cyber Security Incident Response Audit Report to Administration on April 9, 2018. The report includes Administration's response to recommendations raised by the City Auditor's Office to Information Security and Information Technology. Administration accepted all recommendations and has committed to the implementation of action plans no later than December 31, 2018. The City Auditor's Office will track the implementation of these commitments as part of our on-going follow-up process.

RECOMMENDATIONS

1. That Audit Committee receive this report for information; and
2. That Audit Committee recommend that Council receive this report for information.
3. That Audit Committee recommend that Attachment to Report AC2018-0410 remain confidential pursuant to Sections 20(1)(k) and (m) of the *Freedom of Information and Protection of Privacy Act* until the year 2033.

PREVIOUS COUNCIL DIRECTION / POLICY

Bylaw 30M2004 (as amended) established the position of City Auditor and the powers, duties and functions of the position. Under the City Auditor's Office Charter, the City Auditor presents an annual risk-based audit plan to Audit Committee for approval. The City Auditor's Office 2017 Annual Audit Plan was approved on November 10, 2016. The City Auditor is accountable to Council and subject to the oversight of Audit Committee under Bylaw 48M2012 (as amended).

BACKGROUND

This audit was undertaken as part of the approved City Auditor's Office 2017 Annual Audit Plan. The objective of this audit was to determine if The City has an incident response process that will reduce the impact of a non-routine cybersecurity incident.

Approval: Katharine Palmer, City Auditor Author: Ross Visscher

CYBER SECURITY INCIDENT RESPONSE AUDIT

The incident response lifecycle (Figure 1), consists of four phases[1]:

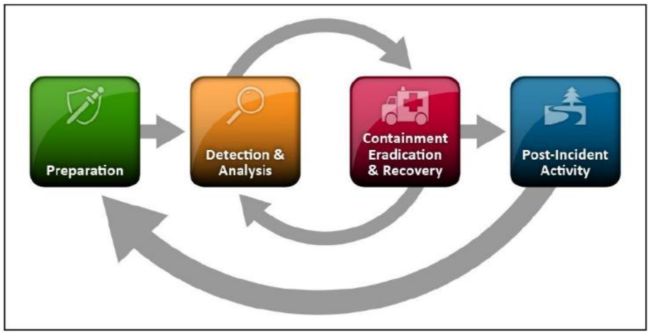

Figure 1: Incident Response Lifecycle (Source: NIST SP 800-61)

1. Preparation: Establishing an incident response capability so the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
2. Detection and Analysis: Determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.
3. Containment, Eradication, and Recovery:
   a. Containment - provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g. shut down a system, disconnect it from a network, or disable certain functions).
   b. Eradication - may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts.
   c. Recovery - restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, and rebuilding systems from scratch.
4. Post-Incident Activity: Learning from the incident by reviewing what happened and how staff and management performed in dealing with the incident. Lessons learned meetings improve future responses; a post-mortem analysis of the way an incident was handled can expose missing steps or inaccuracies in procedures. The reports gathered from these meetings provide a reference when handling similar events in the future.

INVESTIGATION: ALTERNATIVES AND ANALYSIS

The audit objective was achieved by evaluating controls across each of the four phases of the incident response cycle. Furthermore, commentary was provided on the relationship between incident response processes, and investments in people and technology. Information Security has agreed to all recommendations and committed to implementing no later than December 31, 2018.

Stakeholder Engagement, Research and Communication

This audit was conducted with Information Security and Information Technology business units acting as the principal audit contact(s) within Administration.

[1] As defined by the National Institute of Standards and Technology's Special Publication 800-61 - Computer Security Incident Handling Guide

CYBER SECURITY INCIDENT RESPONSE AUDIT

Strategic Alignment

Audit reports assist Council in its oversight of the City Manager's administration and accountability for stewardship over public funds and achievement on value for money in City operations.

Social, Environmental, Economic (External)

N/A

Financial Capacity

Current and Future Operating Budget

N/A

Current and Future Capital Budget

N/A

Risk Assessment

The activities of the City Auditor's Office serve to promote accountability, mitigate risk, and support an effective governance structure.

Cybersecurity events could result in a high impact on The City's finances, reputation and operations if not managed effectively. Financial risks associated with stolen records can be high, estimated at $190[2] per record. Unavailable systems can prevent The City delivering critical services to citizens.

REASONS FOR RECOMMENDATIONS

Bylaw 48M2012 (as amended) states: "Audit Committee receives directly from the City Auditor any individual audit report and forwards these to Council for information."

The Freedom of Information and Protection of Privacy Act states:
20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to:
(k) facilitate the commission of an unlawful act or hamper the control of crime,
(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

ATTACHMENT

AC2018-0410 Cyber Security Incident Response - CONFIDENTIAL

[2] Ponemon Institute - 2017 Cost of Data Breach Study