OFFICE OF THE
City Auditor

Information Technology Security Review

April 16, 2012

THE CITY OF Edmonton

The Office of the City Auditor conducted this project in accordance with the *International Standards for the Professional Practice of Internal Auditing*

Information Technology Security Review

1. Introduction

For many organizations, information and the technology that supports it represent their most valuable assets. Capturing, processing, transmitting, storing, and reporting information are fundamental to organizational operations. With the rapidly increasing complexity of systems and sharing of system access and data with outside parties, the risk of compromising information integrity, confidentiality and availability is a growing risk to an organization's reputation and ability to maintain operations.

The Office of the City Auditor (OCA) included a review of the City's Information Technology (IT) Security in its 2011 and 2012 Annual Work Plans. The overall objective of this review was to perform a comprehensive information security assessment of the City's IT environment from the perspective of an external attacker.

2. The Challenge

Organizations face the risk of unauthorized external as well as internal access to their sensitive and vital information. Our research shows that globally and across industries there is an increase in security breaches, electronic frauds and cyber attacks launched from the outside via the Internet, dial-up modems, wireless access devices, etc. For example, credit card details and personal information are often targets of cyber criminals who are seeking to commit fraud.

In addition to increasingly frequent and complex cyber attacks, intruders are using social engineering techniques to gain access to organizations' internal information systems. A recent Time Magazine article defined social engineering as "using deception, manipulation and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail." The user's action may then execute unauthorized code allowing the attacker to remotely access and exploit vulnerable applications and data. In addition to external threats, organizations also face the risk of employees or contractors with network access gaining access to unauthorized information and/or applications due to inadequate security and access controls.

There are a number of software tools, technologies, methodologies, processes and controls that organizations use to prevent, detect and address the risk of unauthorized external and internal access to their IT environment in order to protect their critical information and technology assets. Some common methods include conducting security threat and risk assessments to safeguard the IT environment. These provide assurance that sufficient controls are in place to reduce the risk of information loss, error, misuse, damage, and service interruption to an acceptable level. Regular vulnerability

assessments that complement threat and risk assessments are also undertaken to test systems for particular weaknesses that could compromise security. Penetration tests that determine whether the identified vulnerabilities can be exploited, both externally and internally, provide organizations a pulse on their security efforts, and facilitate prioritization of their efforts to correct confirmed weaknesses. In addition, organizations implement effective access administration policies and procedures, monitor staff activities, and enhance security awareness and training of users. The chosen level of risk establishes the technical environment in place to support security measures, the types and levels of controls required, and consequently, the resources devoted to an organization's response to suspected and actual security incidents.

It should be noted that organizations that perform regular security and vulnerability assessments as well as penetration tests often find deficiencies in parts of their IT environments that had previously been considered secure. This is a result of new risks and vulnerabilities being introduced or uncovered in view of new complexities, changes in staff habits and more intrusive cyber attacks.

3. The City's Environment

The IT Branch provides core IT services to all Branches and Departments across the City. The Branch is led by the Chief Information Officer (CIO), who is also the Branch Manager reporting to the General Manager of Corporate Services Department. The CIO is both the Chief Architect for the future use of the City's information and technology and the Chief Information Security Officer, responsible for the overall security of the City's information and the technology that supports it.

The City of Edmonton maintains numerous business applications (including web applications), servers, and network systems, and uses the Internet to meet internal and external objectives. It maintains large databases of personal information on its employees and processes millions of dollars in credit card transactions each year.

4. Objectives

Our objectives were to determine whether:

1. The City's IT environment incorporates appropriate safeguards to defeat, or detect and mitigate unauthorized external access and cyber attacks.

2. The City has implemented the procedures and controls necessary to minimize the risk of social engineering techniques being used to compromise its IT environment.

5. Scope and Methodology

Our review focussed on the IT environment managed by the City of Edmonton. It did not include IT systems and environments that are independently managed by Edmonton Public Library, Edmonton Police Service, and other Boards and Authorities. Our scope was limited to assessment and testing to identify vulnerabilities. The Administration is responsible for the development and implementation of strategies and action plans to address any identified weaknesses.

We used the following methodology to meet our objectives:

- Conducted research and a literature search to determine what other organizations, particularly government organizations, are doing to assess and protect their IT environments.
- Met with the CIO and IT Branch staff members to determine the extent of previous security assessments, discuss the City's IT Governance and environment, and assess available IT security evaluation approaches to determine the scope of our review.
- Reviewed the City's policies, directives and processes for managing its IT environment.
- Issued a Request for Proposal with the assistance of Materials Management, IT and Customer Information Services staff, and hired external expertise to conduct the required testing and evaluation.

The selected security consultant's specialized tools, technologies and methodologies were used to perform the following:

1. External network vulnerability assessment and penetration testing
2. Web application vulnerability assessment and penetration testing
3. Remote access system security testing
4. Wireless network vulnerability assessment and penetration testing
5. Mobile device and associated infrastructure vulnerability assessment and testing
6. Social engineering assessment and testing.

Steps were taken to ensure that the assessments, tools, and methodology used were not destructive and did not disrupt the City's operations. We managed the work of the selected consultant and executed an appropriate agreement that formalized the deliverables and other City requirements in order to minimize the City's risks.

6. Summary of Findings

In view of the security risks associated with publicly releasing details on potential and validated vulnerabilities in the City's IT environment, as well as the consultant's proprietary information, the detailed testing, assessment results and recommendations were only shared with authorized representatives of the Administration. We have

provided a summary of the findings, conclusions, recommendations, and the action plans prepared by the Administration in this report.

Comprehensive IT security reviews, which include vulnerability assessments and penetration tests, are considered best practice, both for audit and IT. These reviews provide specific areas for improvement in the overall IT security program.

Based on the tests and assessments performed, the consultant provided overall security risk ratings for the six areas in scope. These are based on the number of security issues found, the ease of exploitation, and the type of information obtained to further exploit other systems.

Table 1 outlines the security risk ratings and the definitions used by the consultant to rate the City's IT environment.

Table 1
Definitions of Security Ratings

RATING	DEFINITION
HIGH RISK	Serious vulnerabilities that have been exploited or are highly likely to be exploited and/or significant deficiencies in design, implementation or management identified.
MEDIUM-HIGH RISK	Vulnerabilities discovered with moderate likelihood of exploitation and/or at least one significant deficiency in design, implementation or management identified.
MODERATE RISK	Vulnerabilities discovered with moderate likelihood of exploitation and/or multiple deficiencies in design, implementation or management identified.
ELEVATED RISK	Vulnerabilities discovered with low likelihood of exploitation and/or minor deficiencies in design, implementation or management identified.
LOW RISK	No vulnerabilities or deficiencies in design, implementation or management. All patches and service packs have been applied.

In addition, the consultant has provided benchmark and comparative information on other organizations based on assessments they have performed over the past three years. This comparative information provides a perspective on how the City of Edmonton fairs compared to other organizations and can be used to prioritize security enhancements.

Table 2 summarizes the overall security and benchmark ratings provided by the consultant for the six areas in scope in the City's IT environment.

Table 2
Overall Security and Benchmark Ratings by Scope Area

SECTION	AREAS IN SCOPE	SECURITY RATING	BENCHMARK RATING
6.1	External Network	MODERATE RISK	AVERAGE 127/300 tests
6.2	Web Application	MODERATE RISK	AVERAGE 116/300 tests
6.3	Remote Access	MEDIUM-HIGH RISK	BELOW AVERAGE 44/300 tests
6.4	Wireless Network	LOW RISK	ABOVE AVERAGE 91/300 tests
6.5	Mobile Device and Associated Infrastructure	LOW RISK	AVERAGE 6/10 tests
6.6	Social Engineering	HIGH RISK	AVERAGE 284/300 tests

Based on the comparative information provided by the consultant, the City is considered average in its security efforts around the external network, web applications, mobile devices and social engineering attacks, above average in its efforts in wireless network, and below average in its efforts in remote access systems. It should be noted that although the City received a high risk security rating in social engineering, 95% of the organizations assessed by the consultant over the past three years face similar challenges and received the same security rating.

The following sections describe the assessments and testing performed by the consultant, the overall results and the comparative information. We have made three recommendations in Section 7 to address the findings.

6.1. External Network

External penetration testing is the process of assessing a network from the perspective of an external attacker for potential vulnerabilities, and if found, performing a controlled attack to verify the results. This type of test is valuable in determining an organization's overall security posture.

A vulnerability assessment was initiated by the consultant's assessment team against the Internet-facing applications[1] identified by the OCA. Various deficiencies were discovered pertaining to the web server and firewall configurations. The consultant was able to gather pertinent information during this phase which was used to exploit the City's remote access systems as outlined in section 6.3. A portion of the information gathered was also used to perform a social engineering attack as outlined in section 6.6.

[1] Web applications that are designed and delivered with the intent of access by individuals or organizations over the public internet

Based on the consultant's security rating matrix, the City of Edmonton is considered to be at moderate risk of external unauthorized network access from exploitation of known system vulnerabilities. In the 300 most recent external network penetration tests conducted by the consultant, 127 (42%) received the same risk rating. There were 11% at lower risk and 47% at higher risk compared to the City's rating. Procedural and configuration changes as well as security awareness training for the City's IT professionals have been recommended by the consultant. The IT Branch has initiated remediation efforts to address these as part of their action plans for Recommendation 2.

6.2. Web Application

A web application penetration test uses specialized tools to gather data and determine if potential vulnerabilities exist in the web servers, application servers, database servers and any intermediary devices such as firewalls. Controlled attacks are performed for all reported vulnerabilities. Exploitation of a web application can expose sensitive information and may result in gaining remote access to an organization's network. Tests are also performed to evaluate user access controls, the strength of authentication and session management, as well as other web-related areas.

During the planning phase of this review, we determined that the City has a number of Internet-facing applications in its web environment that are hosted by third parties. However, the City does not have a complete and accurate inventory of such applications. We were only able to include the applications hosted by one third party in the scope of our review. The other applications had to be excluded in view of the incomplete information and the lack of easy access to the agreements that are in place between the City and the third parties. A complete and accurate inventory of third party hosted applications and its ongoing maintenance will allow the City to have better corporate control over future decisions on vulnerability and penetration tests. It will also assist in determining whether the City is adequately protected in its agreements that various City Departments have with the third parties. The Corporate Services Department has initiated remediation efforts to address this as part of their action plans for Recommendation 1.

The consultant's testing indicated that the City's web processes and procedures need to be strengthened to enhance overall adherence to industry and vendor best practices. Based on the consultant's security rating matrix, the City of Edmonton is considered to be at moderate risk of unauthorized access to its web-based applications. In the 300 most recent remote access tests conducted by the consultant, 116 (39%) received the same risk rating. There were 13% at lower risk and 48% at higher risk compared to the City's rating. Procedural and configuration changes have been recommended by the consultant. The IT Branch has initiated remediation efforts to address these as part of their action plans for Recommendation 2.

6.3. Remote Access

Remote access systems provide access to applications and network services to users when they are away from their office. Vulnerabilities in a remote access system could result in unauthorized access to applications or the entire network. The remote access system security scanning was included as part of the external vulnerability assessment and the web application assessment. In addition, the assessment team performed targeted tests on several remote access systems in order to assess the possibility of unauthorized external access. Since the City no longer has a dial-up remote access service, no dial-up phone numbers were tested.

The consultant's scanning and testing resulted in unauthorized access to the City's Internet-facing applications. This led to their gaining access to the internal City systems and applications. The major causes for this level of penetration relate to the use of inadequate procedures, and poor adherence to industry and vendor best practices around remote access. Based on the consultant's security rating matrix, the City of Edmonton is considered to be at medium-high risk of external unauthorized access to its remote access systems. In the 300 most recent remote access tests conducted by the consultant, 44 (15%) received the same risk rating. There were 80% at lower risk and 5% at higher risk compared to the City's rating. Procedural and configuration changes have been recommended by the consultant. The IT Branch has initiated remediation efforts to address these as part of their action plans to address Recommendation 2.

6.4. Wireless Network

A wireless network vulnerability assessment includes a review of the wireless network infrastructure, discovery of access points, and a review of the security devices that make up the wireless network. It also includes a review of the authentication mechanisms that control access to the wireless network, access control mechanisms, encryption of data as well as the overall design of the wireless network against industry and vendor best practices. A wireless penetration test is also performed to determine if the wireless network can be breached.

The assessment team performed a wireless assessment and penetration test at four City of Edmonton locations selected by the OCA; three in downtown as well as one remote location. They found both, the City's free public wireless network and the private wireless network to be sufficiently secured, and were unable to gain access to the City's internal systems or networks.

Based on the consultant's security rating matrix, the City of Edmonton is considered to be at low risk of external unauthorized access. In the previous 300 wireless network penetration tests conducted by the consultant, 91 (30%) received the same risk rating. The remaining 70% were at higher risk compared to the City's rating. The City's configuration of wireless networks is currently adequate to ensure confidentiality and integrity of data, and the City has implemented fairly well-defined access controls to prevent unauthorized external access. In view of this, we have not made any recommendations in this area.

6.5. Mobile Device and Associated Infrastructure

A mobile device and associated infrastructure vulnerability assessment and testing from an external attacker's perspective includes attempts to locate employer-owned devices such as smartphones and tablets, and access them through the use of automated tools and social engineering techniques.

A number of City mobile devices were discovered during the consultant's assessment and testing, including BlackBerrys, iPhones and iPads. These were subjected to remote attacks by the assessment team. However, they were not successful in obtaining unauthorized access to these devices through remote methods.

Based on the consultant's security rating matrix, the City of Edmonton's mobile devices are currently considered to be at low risk of external unauthorized access. In the ten most recent mobile device security assessments conducted by the consultant, six (60%) received the same risk rating. The remaining 40% were at higher risk compared to the City's rating. Based on the tests performed, the current configurations of the City's mobile devices identified are adequately secured to ensure confidentiality and integrity of the data from a remotely accessible standpoint. In view of this, we have not made any recommendations in this area.

6.6. Social Engineering

Social engineering assessment and testing includes remote and physical methods of gathering key information and attempts to penetrate an organization's physical and IT environment. During the remote phase, pertinent information such as e-mail addresses, phone numbers and other employee information is gathered from various public sources. This information is then used to develop an email attack against selected targets with the objective of obtaining and utilizing employee credentials to penetrate the corporate network. The physical phase includes site surveillance of selected locations to gather key information in order to determine potential entry points. This information is then used in attempting to gain access to the physical locations, and in turn, gain access to the corporate network through the use of automated tools. Other methods can also be used such as enticing employees to pick up or receive planted memory sticks and plugging them into their computers, which in turn connects them to the tester's devices.

Four City locations were selected for the social engineering test by the OCA; three in downtown as well as one remote location. The assessment team used two forms of social engineering; physical and electronic. As part of the physical social engineering test, the assessment team performed surveillance of the selected locations and attempted to break-in. They were able to bypass existing physical security controls in all four locations and gain access to the City's internal network. This ultimately allowed them access to the City's systems and applications. The assessment team also physically passed on memory sticks to three City employees in the locations they were able to access. All three employees plugged them into City-owned computers, which in turn connected them to the consultant's devices.

An electronic social engineering attack was initiated by the assessment team against 49 e-mail users of which six responded and provided their credentials. This provided access to the City's internal network and eventually allowed the assessment team to gain control over the City's network infrastructure. A second test was initiated in which a secondary group of 589 potential e-mail users was targeted with a hyperlink to a site controlled by the assessment team. Of these, 233 (40%) responded to the e-mail attack within a 24–hour period. Further testing of how many of these employees would provide their credentials to the consultant was not pursued as the required evidence from the first test of 49 e-mail users was considered adequate.

Based on the consultant's security rating matrix, the City of Edmonton's ability to identify and deter both physical and electronic social engineering attack methods is considered to be at high risk of unauthorized access. It is interesting to note that in the 300 most recent social engineering assessments conducted by the consultant, 284 (95%) received the same risk rating. The remaining 5% were at lower risk compared to the City's rating. This shows that since manual controls are common and employees are involved, organizations face a bigger challenge of reinforcing preventative methods and monitoring the application of existing controls. Procedural changes, security training, as well as ongoing and effective end user education and awareness have been recommended by the consultant. The Corporate Services Department has initiated remediation efforts to address these as part of Recommendation 3.

7. Conclusion and Recommendations

The OCA has completed vulnerability assessments and penetration testing of the City's IT environment from the perspective of an external attacker, with the assistance of third party expertise and automated tools. Our objectives were to determine whether the City's IT environment incorporates appropriate safeguards to defeat, or detect and mitigate unauthorized external access and cyber attacks; and whether the City has implemented the procedures and controls necessary to minimize the risk of social engineering techniques being used to compromise its IT environment.

During the planning phase of this review, we determined that the City has a number of Internet-facing applications that are hosted by third parties. However, the City does not have a complete and accurate inventory of such applications. Such an inventory and its ongoing maintenance will allow the City to have better corporate control over future decisions on vulnerability assessments and penetration tests and in determining whether the City is adequately protected in its agreements that various City Departments have with the third parties.

Based on the consultant's security rating matrix, the City received a moderate risk rating for its external network and web applications; a medium-high risk rating for its remote access system security; a low risk rating for its wireless network and mobile devices; and a high risk rating for its ability to identify and deter both physical and electronic social engineering.

The consultant has also provided a benchmark rating to indicate a typical rate of success for each of the areas tested in comparison to assessments they have performed for other organizations. These benchmarks and security risk ratings will facilitate the prioritization of the City's efforts to implement security measures and controls required to correct confirmed weaknesses. They will also provide an IT security baseline for measuring the City's progress in enhancing its security measures between assessment cycles.

The consultant has provided detailed recommendations pertaining to procedural and configuration changes, effective security training as well as end user education and awareness of City staff. The Corporate Services Department has initiated remediation efforts to address these. A follow-up external vulnerability scan will be conducted by the consultant at a mutually convenient time to provide effective feedback on the City's remediation efforts. There are plans to provide appropriate tools and training to City staff to assist them in conducting their own periodic assessments in order to enhance security of the City's IT environment.

Our overall conclusion is that the City needs to continue to enhance its IT environment and incorporate appropriate safeguards to minimize the risk of unauthorized external access, as well as physical and electronic social engineering attacks.

We have made the following three recommendations to strengthen controls, which have been accepted by the Administration:

Recommendation 1 – Inventory of third party hosted applications
The OCA recommends that the General Manager of Corporate Services, on behalf of the Corporate Leadership Team, ensure that an accurate and complete inventory of third party hosted applications is maintained to facilitate decision-making and to protect the City's interests.
Management Response and Action Plan
Accepted Action Plan: As part of the Application and Software Rationalization initiative, the IT Branch has initiated a process to develop a comprehensive list of the different applications being used across the City. A list of externally hosted applications that handle private City information will be delivered as part of this project to support risk mitigation activities for the corporation. Planned Implementation Date: Q2, 2012 Responsible Party: Chief Information Officer

Recommendation 2 – Enhance City's IT environment & incorporate safeguards
The OCA recommends that the Chief Information Officer and Manager of Information Technology Branch continue to enhance the City's IT environment and incorporate appropriate safeguards to defeat, detect and mitigate unauthorized access and cyber attacks.
Management Response and Action Plan
Accepted Action Plan: The City is committed to being responsible stewards for the information and data entrusted to us by the public. The IT Branch has reviewed and prioritized the specific technical recommendations; high priority issues have been remediated and a plan to respond to all other items has been implemented. The IT Branch will develop a broader Information Security Strategy that incorporates the themes from the audit; this will establish a roadmap for the next 5 years to enhance information security across the organization. Planned Implementation Date: Q1, 2013 Responsible Party: Chief Information Officer

Recommendation 3 – Minimize risk of physical and electronic social engineering
The OCA recommends that the General Manger of Corporate Services take reasonable steps to strengthen the application of procedures and controls to minimize the risk of physical social engineering attacks; and enhance the procedures and controls to minimize the risk of electronic social engineering attacks, including ongoing and effective end user education and awareness.
Management Response and Action Plan
Accepted Action Plan: The responsibility for corporate information management is shared across the organization. The City has taken immediate steps in response to areas where vulnerabilities were identified; these will serve as parameters for a corporate implementation plan to enhance information and physical security. The Corporate and IT Security sections will collaborate to develop an ongoing education and awareness program to enhance the culture of security across the corporation. Planned Implementation Date: Q4, 2012 Responsible Party: General Manager, Corporate Services

We thank the consultant's staff, the City's General Manager of Corporate Services, and IT leadership and staff for their assistance and support during this foundational review.