**Report - Executive Policy Committee - July 9, 2008**

**Item No. 6 Assessment of Information Security Awareness**
**File FA-2**

EXECUTIVE POLICY COMMITTEE RECOMMENDATION:

On July 9, 2008, the Executive Policy Committee concurred in the recommendation of the Audit Committee and submits the following to Council:

1. That the Assessment of Information Security Awareness dated June 2008 be received as information.

2. That the Proper Officers of the City be authorized to do all things necessary to implement the intent of the foregoing.

**Report - Executive Policy Committee - July 9, 2008**

DECISION MAKING HISTORY:

EXECUTIVE POLICY COMMITTEE RECOMMENDATION:

On July 9, 2008, the Executive Policy Committee concurred in the recommendation of the Audit Committee and submitted the matter to Council.

AUDIT COMMITTEE RECOMMENDATION:

On July 3, 2008, the Audit Committee recommended that the Assessment of Information Security Awareness dated June 2008 be received as information, and submitted the matter to the Executive Policy Committee and Council.

Winnipeg

# Audit Department

## *Assessment of Information Security Awareness*

*June 2008*

*Leaders in building public trust in civic government*

1188

# Table of Contents


MANDATE OF THE CITY AUDITOR ..... 7
AUDIT BACKGROUND ..... 7
AUDIT OBJECTIVES ..... 8
AUDIT APPROACH ..... 8
AUDIT CONCLUSIONS ..... 8
ACKNOWLEDGEMENT ..... 9
KEY RISKS AND IMPACTS ..... 10
OBSERVATIONS AND RECOMMENDATIONS ..... 11
- INFORMATION TECHNOLOGY ADMINISTRATIVE DIRECTIVES ..... 11
- ORGANIZATION ..... 14
- SECURITY AWARENESS PRACTICES ..... 16
- AWARENESS OF STAFF ..... 18

APPENDIX A: INTERVIEW QUESTIONS ..... 21
APPENDIX B: ELECTRONIC SURVEY QUESTIONS ..... 22
APPENDIX C: COMPONENTS OF A SECURITY AWARENESS AND TRAINING PROGRAM ..... 26
- AWARENESS, TRAINING, AND EDUCATION ..... 26
- PROGRAM COMPONENTS ..... 26
- DEVELOP AN AWARENESS AND TRAINING PLAN ..... 27
- STRUCTURE ..... 27
- DEVELOP OR ACQUIRE AWARENESS AND TRAINING MATERIALS ..... 32
- ONGOING AWARENESS, TRAINING, AND MATERIALS MAINTENANCE ..... 35

# Executive Summary

The continued development of information technology (IT) has allowed organizations to increase efficiency but has also brought with it increased risks. Proper management of information security risks from both within the walls of the organization and from external sources that can result in unauthorized access to the computer system is critical. In today's high-tech and interconnected world, every business needs a well planned and implemented IT security framework.

One of the first steps in implementing information security is to formulate a security policy framework. The goal of corporate security policies is to define the procedures, guidelines and practices for configuring and managing security in the environment. The City of Winnipeg has developed and implemented a series of IT directives to assist City employees. While the City workforce has been made aware of the directives and they are easily accessible, there is a need to update the IT governance directive to reflect the present City organization. As technology continues to evolve, additional directives may also be required in areas such as the use of portable storage devices and conducting vulnerability assessments to identify exposure levels and the associated risk.

The role technology plays in supporting the delivery of City services continues to grow. Management recognizes the increased importance and actively supports information security through clear direction and assignment of information security responsibilities. Departmental staff are assisted in performing their responsibilities by a standing corporate level committee, the Information Technology Committee (ITC) and one of its working groups, the Security Committee (SC).

Through *Directive IT-004* responsibility for security has been assigned to the individual; each employee has been directed to operate in a secure and safe manner. While employees have been assigned the responsibility, there is no assurance that they have read or fully understood the requirements of the directive. Developing a process to require employees to sign-off or attest to their understanding is one method to ensure all staff understand their responsibility to be aware and knowledgeable of the IT directives.

The need for this process was supported through a series of interviews and an eSurvey conducted as part of this assessment. Over 25% of all City staff incorrectly indicated that security was the responsibility of IT support staff. Of the 75% of staff who were aware of their responsibility to protect the organization's information, many (nearly 30%) indicated that they only had a poor or fair level of understanding. A lack of understanding means staff do not necessarily know how to fulfill their responsibilities which increases the risk of a breach in the security of confidential information.

Management needs to ensure that staff understands what they need to do and how best to do it—this is an ongoing requirement, not a one-time exercise. As an example, the corporate email team regularly communicates with all email users providing safe computing reminders and updates on the email system and potential threats. This ongoing communication is one example of a proactive effort to improve staff's knowledge of a critical IT system.

In order to improve awareness and understanding on all key systems across the organization, the City needs to invest

additional time and resources in an awareness and training strategy to reinforce the directives and to improve security efforts across City departments and special operating agencies. A variety of security awareness practices have been put in place by various City departments, but since the City operates in a highly-decentralized manner the overall accountability and responsibility for security awareness and training of staff needs to be clarified.

Leveraging a combination of departmental and corporate resources, including the Security Committee, is strongly recommended to increase efficiency in the development of the security awareness and training program and to ensure consistent implementation across the organization.

## Mandate of the City Auditor

The City Auditor is a statutory officer appointed by City Council under the City of Winnipeg Charter Act. The City Auditor reports to Council through the Audit Committee (Executive Policy Committee) and is independent of the City's Public Service. The City Auditor conducts examinations of the operations of the City and its affiliated bodies to assist Council in its governance role of ensuring the Public Service's accountability for the quality of stewardship over public funds and for the achievement of value for money in City operations. Once an audit report has been communicated to Council, it becomes a public document.

## Audit Background

In today's business environment, information security and protection of information assets are vital to the long-term success of all organizations; information is a vital business asset. IT systems connect every internal department, and also connect the organization with myriad suppliers, partners, customers, citizens and others.

Information technology services for the City of Winnipeg are provided and organized on a decentralized basis (within departments and special operating agencies) and also on a centralized basis (through Business Technology Services).

Individual departments and special operating agencies provide their own (decentralized) IT services for systems and technologies that are considered *mission critical* for their particular lines of business.

The centralized Business Technology Services is focused on those services that:

- span multiple departments
- are founded on shared or common IT infrastructure
- are more efficiently provided by one provider than many
- require extensive specialization and are required by more than one department

Business Technology Services provides three major IT and communication service areas:

- Business Solutions (e.g., PeopleSoft system, tax system)
- Managed Hosting (e.g., web sites, databases)
- Connectivity Services (e.g., email, remote access, roaming wireless)

Management and staff of the City of Winnipeg understand the importance of information security and the need to maintain a secure environment for information and information systems across the enterprise. Formal guidance is provided to management and staff through a series of IT security-related directives, including:

- *Administrative Directive No. IT-001 Governance Structure – Information Technology*
- *Administrative Directive No. IT-002 Management of Electronic Mail*
- *Administrative Directive No. IT-003 City-Wide Electronic Data Sharing*
- *Administrative Directive No. IT-004 Individual Responsibility for IT Security*
- *Administrative Directive No. IT-005 City of Winnipeg Web Governance*
- *Administrative Directive No. IT-006 Security of Wireless Computing*

## Audit Objectives

- To assess the awareness of management and staff regarding the City of Winnipeg's IT Security policies
- To assess the understanding of management and staff regarding the City of Winnipeg's IT Security policies
- To identify the key improvement opportunities

## Audit Approach

A planning workshop was conducted with representatives from the City of Winnipeg's Audit Department, IT management from Internal Services Department and the project team from the IT Security consulting firm Securris. Goals and objectives and a project plan were developed.

An assessment team, comprised of staff from Securris, conducted interviews and obtained information and input from all City of Winnipeg departments and selected special operating agencies. Appendix A contains the questions that formed the basis for the interviews. The interviews involved a variety of stakeholder groups including:

- Department heads
- IT management and professionals (mainly IT coordinators)
- Department managers and supervisors
- Corporate managers and professional staff (in Internal Services)

The assessment team reviewed relevant background documentation including the City's administrative directives relating to IT Security and Information Technology.

The assessment team conducted an electronic survey which was made available to almost 50 percent of the City's workforce (all staff with internet access were able to participate). In four days, staff returned over 860 valid responses (20 percent of possible participation) from the following groups:

- Management and supervisory personnel (~35%)
- IT professionals (~11%)
- Everyone else (~54%)

Appendix B contains the questions that made up the electronic survey.

## Audit Conclusions

- Responsibility for security has been assigned to the individual and most City staff are aware of the IT Security directives. The directives are accessible online but some need to be updated to reflect the current organizational structure.
- Results of the eSurvey revealed that nearly 30% of all respondents have only a poor or fair level of understanding of the directives. The development of an IT security training and awareness program combined with employee sign-off of their understanding of the directives would assist staff in improving their overall knowledge of the directives.
- In addition to the above noted opportunities, we made recommendations to create new directives. Evolving technology issues such as the use of portable media devices and the performance of vulnerability assessments require administrative directives to provide guidance to City staff. We also made recommendations to promote the use of the Security Committee in improving security awareness and understanding city-wide.

## ACKNOWLEDGEMENT

The City of Winnipeg's Audit Department would like to acknowledge the assistance provided by the IT Security Consulting firm Seccuris who was engaged to conduct the assessment of the City's Information Security Awareness. In addition, we would like to acknowledge the assistance of staff from all City Departments and special operating agencies who were involved in this project, for their assistance in providing time, information, expertise, co-operation and resources throughout the duration of the project.

| Members of the Audit Team |
| --- |
| Bryan Mansky, MBA, CMA, CIA<br>Audit Manager |
| Kevin Milne, CGA, CIA<br>Senior Auditor |
| Dan Swanson, CIA, CISA, CISSP, CAP, CMA<br>Seccuris, Project Manager |
| David Violago, BA, MA, LLB, CISSP<br>Seccuris |



Shannon Hunt, FCGA, CFE

June 2008

Date

## KEY RISKS AND IMPACTS

With an increased reliance on technology, the security, privacy, and reliability of technology becomes even more critical.

Legislation and good business practice dictates that organizations must safeguard the information entrusted to them. The following are some notable security risks:

- Increased or unknown operational costs due to unavailability of key business applications
- Unauthorized access to, or disclosure of, client records
- Loss of physical assets
- Inadequate or delayed response to information security incidents
- Loss of cash flow
- Damage to reputation

***Increased or Unknown Operational Costs due to Unavailability of Key Business Applications***

There may be an impaired flow of data if an organization's servers or networks are damaged or destroyed, or if they are unable to handle the traffic load imposed by new projects and applications. Delay in obtaining information could delay delivery of services.

***Unauthorized Access to or Disclosure of Client Records***

If information is disclosed to unauthorized persons, then client identities may be stolen. Stolen identities may be used to commit fraud or other criminal offences. In 2006, the personal information (including some credit card and bank account numbers) of about 70,000 people who gave money to Brock University was stolen from the school's computers by a hacker.[1]

***Loss of Physical Assets***

What impact could the theft of a laptop have on an organization? In November, 2007, City University of New York officials urged almost 20,000 students to check their bank accounts, after a broken laptop containing personal information was taken from the school's financial aid office.[2]

***Inadequate or Delayed Response***

An organization may remain unaware that a breach has occurred for months or years. For example, in January, 2007, a large U.S. department store chain announced that it was the victim of an unauthorized computer systems intrusion. It discovered in mid-December, 2006, that its computer systems were compromised and customer data was stolen. Transactions from as early as 2003 were affected.[3] In another example, the private information of thousands of Indianapolis Power and Light customers was inadvertently posted online for up to four years.[4]

---

[1] Source: Hackers steal personal information from Brock University computers, http://www.cbc.ca/technology/story/2006/10/12/tech-brock.html (as of April 14, 2008)

[2] Source: CUNY Urges Students To Check Bank Accounts After Laptop Theft, http://www.ny1.com/ny1/content/index.jsp?stid=8&aid=75183 (as of April 14, 2008)

[3] Source: THE TJX COMPANIES, INC. VICTIMIZED BY COMPUTER SYSTEMS INTRUSION;PROVIDES INFORMATION TO HELP PROTECT CUSTOMERS, http://www.tjx.com/TJX_press_release_Jan_17_%2007.pdf (as of April 14, 2008)

[4] Source: Security Lapse Affects Thousands Of Electric Customers, http://www.theindychannel.com/news/14768281/detail.html (as of April 14, 2008)

***Loss of Cash Flow***

The inability to record charges and bill for services due to a loss of data processing capabilities could disrupt cash flow.

***Damage to Reputation and Public Confidence***

Breaches could erode public confidence in the City of Winnipeg. The result of a general breakdown of trust may reverse several years of confidence-building in the use of City services.

## OBSERVATIONS AND RECOMMENDATIONS

The results of the assessment have been grouped into four categories. For each category positive findings, improvement opportunities, and recommendations are provided. The four categories are as follows:

- Information Technology Administrative Directives – this section focuses on the IT directives developed by the City that form the basis for the IT security framework by defining procedures, guidelines and practices for configuring and managing IT security.
- Organization – this section focuses on the division of roles and responsibilities regarding IT security between corporate and departmental staff.
- Security Awareness Practices – this section deals with the common practices followed city-wide and the unique guidance and practices developed by some departments to support their particular environment...
- Awareness of Staff – this section deals with the analysis of interviews and the eSurvey conducted to gauge City staff's overall awareness of IT security.

## Information Technology Administrative Directives

***Positive Findings***

**City-wide security directives exist**
The City of Winnipeg has issued directives to assist City employees by defining the policies, responsibilities, techniques, and procedures to be used in securing the City's IT environment and information requiring protection.
Security policies are easily available to all City employees, as online access to all directives is in place.

**Departments provide direction to staff on IT security**
Senior management and IT coordinators generally report that they understand their responsibilities.

Some departments and special operating agencies have augmented the City directives with their own policies, practices and procedures, due to their unique business needs. For example, departments whose employees deal with personal health information have PHIA and FIPPA training, and those employees sign off on required pledges of confidentiality. Some departments provide their employees with comprehensive sessions regarding IT security and data confidentiality.

As part of the assessment project approach, the questions used to guide each interview was provided to management ahead of the meeting (these questions are listed in Appendix A). Many departments prepared a response to the assessment questions; a comprehensive view of current practices was prepared by management and the IT coordinator within each Department. All staff involved in the interviews indicated that it was beneficial to review current practices in this manner, as they now have a new baseline of practice information.

**Management works closely with IT**
Management generally relies extensively on IT management and the IT coordinator of many departments drives much of the IT security efforts.

**Anti-Virus Protection**
Departments report that employee workstations run anti-virus software and have available up-to-date sources for anti-virus signatures and security patch updates.

***Improvement Opportunities***

### IT Governance and IT Security-Related Directives Require Updating

**Finding:** Governance of information technology at the City of Winnipeg has recently undergone substantial change. For example, the position of the CIO has been eliminated as a separate position in the organization structure, which is not reflected in Administrative Directive IT-001 (Governance Structure - Information Technology) or in Administrative Directive IT-004 (Individual Responsibility for IT Security).

**Significance:** The directives do not reflect current organizational responsibilities. There should be clear and accurate assignment of specific roles and responsibilities for information security across the organization.

**Recommendation 1:** The Director of Internal Services should update all security-related Administrative Directives to accurately reflect the recent reorganization of IT governance and the resulting adjustment in various roles and responsibilities.

**Management Response:** The Director of Internal Services, together with the Office of the CIO, has committed to a review of all IT Directives over the next 12 months (2008-2009). Besides incorporating additional information and references resulting from the experience of use, the updates will reflect organizational changes and organizational unit (re)naming. IT-004 (Individual Security for IT Security) will take priority, with updates scheduled for completion in 2008, followed by the necessary reviews (Security Committee, Information Technology Committee, Senior Management Team, CAO).

**Recommendation 2:** The Director of Internal Services should give priority to providing resources for the updates to security-related directives. Consideration should be given to using departmental resources and/or other temporary resources to advance the completion of the updates to the security directives.

**Management Response:** The Director of Internal Services will review the priority of Directive updates in relation to other ongoing initiatives, and adjust resourcing accordingly to ensure that timeframes are met. Participation and additional resources from line departments will be sought where advantageous in reviewing the updates.

### Guidance Regarding Technical Vulnerability Assessments (VA) Is Needed

**Finding:** The City of Winnipeg does not conduct technical vulnerability assessments on its technology infrastructure and critical information systems in a systematic manner. Vulnerabilities in the network infrastructure, critical information systems, or both may arise in the environment and not be identified on a timely basis.

**Significance:** Technical vulnerability assessments identify exposure levels and the potential business impact that technical vulnerabilities and operational issues have on an organization. Regularly scheduled and conducted assessments

will support business operations because unknown vulnerabilities and their associated risks will be identified and addressed on a timely and proactive basis.

The City should provide its departments with guidance as to when and how to perform technical vulnerability assessments.

**Recommendation 3:** The Director of Internal Services should consider developing a new Directive regarding technical security assessments. As a minimum, the Director of Internal Services should develop a position statement regarding vulnerability assessments of the various technologies being used.

**Management Response:** A Statement of Direction will be placed on the Office of the CIO Intranet, reflecting a request from the Director of Internal Services' that regular security-related assessments be done. This statement will reference upcoming enhancements to IT-004 (as opposed to a new Directive).

Directive IT-004 has a section on Responsibilities for City IT Staff. That section will be enhanced to require that each department develop and have a plan for assessments – much like a plan for internal procedures for a virus incident – in collaboration with the OCIO and Business Technology Services, and that the plan includes a methodology for presenting the results. As per Recommendation 1, this is scheduled for completion by the end of 2008.

**Recommendation 4:** The Director of Internal Services should develop a vulnerability management plan which would assist the City in scheduling and reviewing the results of the approved vulnerability assessments in a systematic manner.

**Management Response:** Given constraints in budgets and resourcing, it is difficult to commit to a fixed or rigorous schedule for vulnerability assessments. However, at a minimum this will be done every 18 months at (and for) the external Internet-facing infrastructure. Note that such an assessment, done by a third party, is normally priced between ten thousand dollars and twenty thousand dollars, depending on specifications.

A 2008 Vulnerability Assessment has recently been completed, so a similar full assessment would be due in early 2010. This is not to preclude smaller, localized assessments being done in local departmental systems, or on Internet (Web) applications.

The Director will request that in the first half of 2009, the Office of the CIO investigate the availability of zero-cost vulnerability assessment tools for risk mitigation and make a recommendation on their applicability and usage.

### Employee acknowledgment of their understanding of the directives would be beneficial

**Finding:** Employees do not sign off or attest to their understanding of the directives. There is no formal testing of employee knowledge of the directives.

**Significance:** There is no assurance that employees understand and can implement the requirements of the directives. Managing signoff/attestation would require increased time and effort on the part of line managers but would help to ensure employee review and understanding of directives (and the periodic changes to these directives). To reduce the impact to line managers, this type of attestation could be done electronically (e.g., via a web site), reducing paper work and administration effort.

**Recommendation 5:** The Director of Internal Services should consider having employees annually sign off or somehow attest to their understanding of the directives.

**Management Response:** The Director of Internal Services will ask that investigation be done in 2008 into methods by which a periodic reminder can be made available online prior to continuation with network logon, and tracking done on who "accepted" and when.

A regular "I have read and agreed to abide by…" pop-up, together with links to the required resources, is not uncommon in the industry. At the very least, it points out employee obligations, provides an opportunity to review Directives, and fulfills to some degree the employer's obligation to set its expectations. It is expected that this technology will be implemented in 2009.

## Organization

***Positive Findings***

**Information technology reorganization is basically complete**

The IT reorganization that was planned and implemented over the past couple of years has been mostly completed. Individual departments are responsible for delivery of services. Various corporate level entities support the departments and handle corporate-wide solutions (for example, email operations).

**Management demonstrates commitment to information security**

Management actively supports security within the City of Winnipeg through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. These responsibilities are assisted by a standing corporate level committee, the Information Technology Committee (ITC) and one of its working groups, the Security Committee (SC).

The Information Technology Committee identifies opportunities (for both the organization as a whole and departments), prioritizes these opportunities and prepares and puts forth business cases in support of responsible and appropriate courses of action. Its duties include the development and recommendation of policies and directives to maximize the quality and value of information systems and data.

The Security Committee is a working group of the IT Committee. The Security Committee's membership consists of stakeholders from several City departments. The Security Committee is a key vehicle for reviewing various security issues that do arise. Its representation

allows for departmental considerations to be included in new and revised directives and other security guidance that is being issued corporately.

The IT Committee and Security Committee are also useful in the sharing of practices and provide an effective forum for discussion, debate, and resolution.

***Improvement Opportunities***

**A formal Information Security Awareness and Training Strategy is needed**

**Finding:** No formal security awareness and training strategy exists to ensure that all employees have the knowledge and skills required to run systems correctly and fulfill their information security responsibilities.

**Significance:** Without an ongoing awareness and training effort in place, employees may not be aware of the latest security threats to their department or the City organization as a whole, and may be unaware of how to deal with them.

New security issues are emerging regularly. Whether they are highly complex and network-based, or user-oriented operating system-based, these issues should be brought to the attention of the appropriate employees. Security Awareness and Training programs ensure that employees are aware of the newest security issues, ultimately supporting reliable and secure business operations.

Refer to Appendix C for comprehensive detail regarding what an awareness and education program entails. The development of a security awareness and training strategy is recommended to support the operating department's ongoing efforts. Leveraging good Security Awareness and Training Program practices is recommended.

Funding and resourcing of ongoing security awareness and training effort should be reviewed on a regular basis.

**Recommendation 6:** The Director of Internal Services should develop minimum standards regarding awareness and training in security procedures and the correct use of information processing facilities that should be provided to employees, contractors, and third-party users, to minimize possible security risks.

**Management Response:** This can be addressed by ensuring that City processes incorporate the necessary documentation related to IT security. The Director of Internal Services will ensure that:

- Orientation and documentation for new hires, as well as for those moving within and across departments, includes presentation of security-related directives.
- When hiring consultants, Legal and departmental IT Staff review NDAs (Non-Disclosure Agreements) as well as required technical stipulations, as well as. Technical requirements for consultants and "Non-City Staff" will be completed in Q4 2008, reviewed by Security Committee and ITC, and posted on the OCIO site.

For employees and "correct use and conduct", reference will be made in IT-004 to the Employee Code of Ethics, Employee Use of the Internet, and eMail Directive, and these will be included in the regular "pop-up signoff" discussed earlier. A request will be made that the current Internet Usage Guidelines be more visible and accessible, and be made available directly from the Intranet home page.

**Recommendation 7:** The Director of Internal Services should determine overall accountability for security awareness and training of City staff, considering input from the stakeholders.

**Management Response:** Accountability for security awareness and training rests with every department head and supervisor, as it should be part of the day-to-day work mode, much like employee safety. It is not "just an IT Issue", with process, people and policy all as keys to making it work.

The Director will ensure that this is documented in Directive IT-001 (Governance), and reinforced through an ITC Agenda Item regarding IT-001 (Q4 2008).

### Security Awareness and Training should be on the Security Committee's agenda

**Finding:** Security awareness and training has not been a frequent topic of discussion of the Security Committee. Many interviewees indicated that it could be useful to add security awareness and training to the standing agenda of the Security Committee.

**Significance:** Security awareness and training initiatives may not be harmonized across the City's departments and best practices may not be shared on a timely basis.

**Recommendation 8:** The Director of Internal Services should make "Security Awareness and Training" a standing agenda item of the appropriate IT Working Group of the IT Committee (currently, this IT Working Group is the Security Committee), to encourage formal sharing of best practice information on a regular basis.

**Management Response:** Security Committee currently meets three times per year; the Director will ask that Security Awareness be a standing item on the agenda beginning in the fourth quarter of 2008.

**Recommendation 9:** The Director of Internal Services should assign an IT Working Group to provide leadership and support regarding Security Awareness and Training efforts across the City.

**Management Response:** The Security Committee will be the Working Group dealing with Security awareness, with no need for another committee. Minutes will be posted on the Office of the CIO Intranet, with focus to be placed on that area as the primary source of Governance and Awareness materials.

## Security Awareness Practices

***Positive Findings***

**Orientation for new hires**

All departments report that their new staff receive IT security orientation. Departments indicate that, generally, links to the various directives are provided, augmented by any department specific guidance.

**Departmental security policies**

Some departments need access to other secure governmental systems. Such departments have developed their own policies which are harmonized with the policies of the systems they need to access. In some cases for example, firewall rules are made even more restrictive than under City directives.

Some departments dealing with extremely sensitive information limit access to the internet. Employees in such departments require approval to get outside the firewall.

**Departmental review of security topics**

Some departments report that they have annual meetings that specifically review security-related topics. Some departments advise that security-related topics are discussed on an *ad hoc* basis during various team or departmental meetings.

**Sharing of best practices**

Members of the Security Committee use that forum to share best practices with other committee members. The Security Committee has been a key vehicle for reviewing various security issues that do arise, such as inter-departmental virus incident communication procedures.

**Virus outbreak procedure is in place**

New threats may arise at any time, a situation that faces all business organizations. The Information Technology Committee has developed a methodology for inter-departmental communication during a virus incident, as well as recording virus-related information, to minimize the impact on City operations.

***Improvement Opportunities***

**Control over the usage of portable storage mechanisms is needed**

**Finding:** Several departments report that management of portable storage mechanisms, such as USB Data Sticks, is an issue.

Some departments have developed additional policies to guide usage of USB Data Sticks, but there is no standard inter-departmental policy. Some City employees work at home, and may require the use of portable media to transport their work.

**Significance**: Viruses may be introduced into the City's various network environments through malicious, careless, or inadvertent use of such technologies. Additionally, confidential City of Winnipeg information could fall into the wrong hands should a USB data stick be lost by an employee.

There are several possible strategies for mitigating such risks. For example, City issued devices might be encrypted or access ports might be controlled. Specific awareness and training initiatives regarding such devices may also be considered.

**Recommendation 10:** The Director of Internal Services should consider the development of specific procedures governing the control of portable storage mechanisms.

**Management Response:** Considerations are already included in IT-004 that control the devices that can be connected to City computers. The norm is only City-owned and approved storage media. However, within that constraint still lays the potential for data leakage due to "unencrypted" data on removable media (USB hard drives, USB Flash Sticks, SD and CF Cards).

A project is currently underway to evaluate technology applicable to data stored on mobile devices such as laptops and PDAs, and will also encompass means by which encryption can be forced upon any data stored on consumer-type media (USB Flash Drives). The Director will request that as this project evolves, high priority be placed on this aspect of protection.

**Continued support regarding proper email use is needed**

**Finding:** City directives cover employee use of email. However, some departments report that email is still an issue—that email is difficult to control. Up-to-date antivirus definitions (provided by the City

and pushed out to the departments) and robust virus outbreak response procedures (training is now ongoing) are the current final defense against malicious code introduced into City networks via USB drives or email.

**Significance:** Viruses may be introduced into the City's various network environments through malicious, careless, or inadvertent use of such technologies. Email may be used to subject City employees to phishing schemes or other social engineering attacks. Employees should demonstrate their ability to use email and to recognize social engineering attacks. Such demonstrated ability might be measured using tests, but such activity is time and resource dependent.

**Recommendation 11:** The Director of Internal Services should consider having employees annually sign off or somehow attest to their understanding of directives regarding email.

**Management Response:** See Recommendation 5. In regards to email, a separate signoff should not be required, as there is an eMail Directive and it would be referenced along with other relevant Directives in whatever scheme (pop-up or other) is advised.

## Awareness of Staff

The electronic survey (which is reproduced in Appendix B) was sent out under the signature of the Director of Internal Services to the City's entire workforce in late February, 2008. Approximately 4600 members of the workforce who had internet access were able to participate; this was approximately 50 percent of the entire workforce. Of the people who were able to participate in the survey, almost 20 percent (865 responses) actually completed the survey. This level of participation was considered to be excellent. The survey was completed anonymously by those who chose to participate. The survey was made available to City employees for approximately six (6) days.

A quality review of the responses received determined that five responses required purging as the comments provided were not completed in a professional manner. There were no examples of obviously corrupted patterns of response (such as multiples of exactly the same response). Therefore, 860 responses were considered for official assessment analysis.

The most important results are presented below. A detailed summary of the 860 responses has been provided separately to Audit and corporate IT Security staff.

***Positive Findings***

**Respondents answered correctly and/or positively for many questions**

Approximately 70% of respondents have correctly indicated an understanding that everyone is responsible for security. Approximately 82% of respondents felt that important data was regularly backed up to a safe location.

Approximately 82% of respondents felt the City does a good job of keeping staff up-to-date on good IT security practices, while 95% of respondents correctly indicated they would contact their supervisor or IT support staff directly if they detected an IT security problem.

***Improvement Opportunities***

### Develop a Security Awareness and Training Strategy

**Findings:** Approximately 26% of respondents incorrectly indicated that security was the responsibility of IT support staff. Approximately 30% of respondents indicated a poor awareness and/or understanding of the City IT security directives—rating themselves at a 1 or 2 (on a scale of 1 to 5).

Approximately 50% of respondents indicated that they were unsure or did not understand what a compromise of security would entail.

Almost 15% indicated that they were unsure or did not know if important data was regularly backed up.

Almost 18% felt that the City could improve efforts in keeping staff up-to-date on good IT security practices.
Finally, while approximately 88% of respondents understood that permission is required for external parties to connect to the City network, 10% of the respondents indicated that they were unsure or did not know.

**Significance:** Staff misunderstanding of good security practices exposes the City to unnecessary risk such as social engineering or unintentional breaches due to lack of understanding. Training and education is a relatively low-cost activity. By not knowing what a compromise of security entails, an effective response to a security incident is greatly hampered and may be mishandled all together.

Staff should be able to demonstrate their knowledge of information security practices.

Regular outreach to management and staff is very useful in re-enforcing the need for good security practices.

The initial eSurvey completed as part of this assessment project may be used as a baseline for these ongoing efforts.

**Recommendation 12:** The Director of Internal Services should develop a security awareness and training strategy to improve staff's understanding of the security directives.

**Management Response:** In discussion of the standing item on awareness, Security Committee will undertake to build a plan whereby no-cost options are discussed as mechanisms for raising awareness and sparking genuine interest. These include formal presentations at ITC on security topics by line staff and committee members; "Lunch 'n Learns"; security seminars on various aspects of the security landscape, such as anti-phishing, identity theft and "lessons learned"; overviews of corporate-approved security software (anti-spyware, encryption, password keepers and the like); security "tips" in the ISD Connector newsletter; and invited cost-free presentations from consultants and vendors.

Scheduled activities and presentations will be posted as a section on the Course Calendar page, which is quickly accessed through the top-level "Classroom" link on the City Intranet home page.

**Recommendation 13:** The Director of Internal Services should develop a formal security awareness and training calendar, facilitating continued enforcement of security throughout the organization.

**Management Response:** In addition to activities undertaken through Recommendation 12 above, The Director will pursue, through the Office of the CIO and HR Education, re-institution in 2009 of a regular course in the Education Calendar on IT Security generally and at the City specifically, taught by guest lecturers.

**Recommendation 14:** The Director of Internal Services should obtain regular feedback (for example, through use of periodic information security staff surveys) to assess the level of understanding by City employees of the directives, and thus measure the state of security awareness and training needs.

**Management Response:** The Director of Internal Services will request that as part of its regular agenda, the Security Committee decide upon an appropriate methodology – at no cost for software or consulting time – that can be used to carry out a periodic online survey, similar to that done by Seccuris for the initial awareness study. The implementation will be dependent on availability of internal resources to develop a questionnaire, and its priority will be set relative to other ongoing and upcoming IT initiatives. A time frame for the survey will be decided through Security Committee, and after research is done into industry experience on this type of assessment tool.

The results of each survey will be summarized, reviewed at Security Committee, and subsequently presented to ITC.

Considering that an online survey was completed in Spring 2008, the next would be distributed in 2009.

## APPENDIX A: INTERVIEW QUESTIONS

The following questions were used to guide the face-to-face interviews.

1. What are your department's key services and critical information systems?
2. How has the Individual Responsibility for IT Security directive (No. IT - 004) been implemented? Disseminated? Operationalized? Monitored?
3. What efforts have occurred over the past year to keep IT security a priority within your department's operations? What would you consider to be success stories? What challenges are you currently facing?
4. Is your department actively using the web? How useful is the City of Winnipeg's Web Governance Directive (No. IT - 005)? What improvements would you recommend?
5. Security of wireless networks continues to be a challenge; how has the Security of Wireless Computing (No. IT - 006) been implemented in your department? What issues are you struggling with, if any?
6. Email use continues to expand almost exponentially; how has the Management of Electronic Mail (No. IT- 002) been implemented in your department? What improvements to electronic records management are recommended?
7. What formal assessment of technical security in your department has been completed during the past two years? What were the results?
8. What protective measures have been implemented in your department regarding the security of information? Would you consider your information security efforts to be in line with the level of risks and threats to, and importance of, your systems?
9. What other issues should the assessment team consider, if any?
10. In your view, what are the key priorities regarding the improvement of security awareness and understanding within your area of responsibility?

## APPENDIX B: ELECTRONIC SURVEY QUESTIONS

The following questions were provided through an electronic survey instrument. Responses were recorded to a database; the results were tabulated and used to develop the analysis and recommendations.

**1. Please enter your department, or use "undeclared"**

- Assessment and Taxation
- City Clerk's
- Community Services
- Corporate Finance
- Fire Paramedic Service
- Internal Services
- Planning, Property and Development
- Public Works
- Water and Waste
- Winnipeg Police Service
- Winnipeg Transit
- Other
- Undeclared (i.e., prefer to remain anonymous)

**2. Please enter your classification**

Management or supervisory personnel

IT professionals including technical positions

All other positions

**3. Email is a simple, secure and private way to transmit sensitive information.**

Strongly agree

Agree somewhat

Disagree somewhat

Strongly disagree

**4. You find a USB data stick on the ground on your way into work. What do you do?**

Ask IT security what to do with it

Examine it later, when I get home

Leave it where it was

Plug it into my workstation to see what is on it

Put it in the Lost & Found

Throw it in the garbage

**5. On a scale of 1-5 (5 being better), please rate your familiarity with the contents of the City's IT security directives.**

**6. On a scale of 1-5 (5 being better), please rate your understanding with the contents of the City's IT security directives.**

**7. You receive an email which is unexpected and from someone unfamiliar to you. Do you:**

Delete the email, since it's probably spam

Open it up, checking out the attachments if they look interesting

Read the email, but do not open any attachments

Read the email, but don't open any attachments unless you know the sender

**8. Who is responsible for information security in your department?**
Corporate security personnel

Department head

Everyone, including myself

Local IT support staff

**9. When I receive an email, I can rely on the fact that it comes from the person in the "From" address.**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**10. You receive an attachment which doesn't appear related to work and it is received from someone you do not know. Do you:**
Delete the email, since it's probably spam

Open up the email but check out the attachment only if they look interesting

Read the email, but do not open any attachments

Read the email, but don't open any attachments unless you know the sender

**11. The links in emails from unfamiliar sources are generally safe to click on.**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**12. You feel that you would recognize an IT security incident if you saw one.**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**13. What is the largest source of risk to your department's electronic information security?**
Computer viruses and other "malware"

Defective applications

Defective hardware

Human mistakes, malicious or otherwise

**14. I am confident that my/our important data is regularly backed up to a safe location.**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**15. You notice someone in the office you do not know. What do you do?**
Ask them if they're lost, and give them directions if needed

Ask them to identify themselves and escort them to their meeting

Leave them alone if they don't appear lost. If they need help, they will ask

Look to see if they're wearing an access card

**16. It is generally OK to let someone else use my work computer while I'm logged in.**
Strongly agree

Agree somewhat

Disagree somewhat

Strongly disagree

**17. You believe you have detected a security problem in your department. What do you do first?**
Alert the local media

Contact the corporate security team

Tell a co-worker

Contact your supervisor

None of the above

**18. On the whole, the City does a good job of keeping staff up to date on good security practices.**
Strongly agree

Agree somewhat

Disagree somewhat

Strongly disagree

**19. Do you feel that the level of security training you have received is adequate?**
Strongly agree

Agree somewhat

Disagree somewhat

Strongly disagree

**20. I sometimes use my home system to write or revise city documents.**
Strongly agree

Agree somewhat

Disagree somewhat

**21. My home system has up to date security technologies in place to securely work from home.**
Strongly agree

Agree somewhat

Disagree somewhat

Strongly disagree

**22. There an easy method of locking access to your desk top when leaving your desk?**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**23. A consultant wants to plug into the network to access his/her company emails remotely. Are there permissions required before doing so?**
Strongly agree

Agree somewhat

Unsure or don't know

Disagree somewhat

Strongly disagree

**24. Is there something which has been done especially well in your department and/or do you have any suggestions to improve security practices at the City?**

**25. Please let us know if you have any questions or other suggestions.**

# Appendix C: Components of a Security Awareness and Training Program

Every City employee should have adequate knowledge of the various management, operational, and technical controls required and available to protect the information systems resources for which they are responsible.
It is recommended that a formal security awareness and training strategy be developed. This strategy could leverage the best practices cited below. The strategy should help to ensure ongoing information security awareness and training efforts occur within the City of Winnipeg. It would also help to train management and employees on information security goals, policies, and acceptable practices.

## Awareness, Training, and Education

The purpose of awareness presentations is to focus the appropriate attention on security. Awareness presentations are intended to allow individuals to recognize security concerns and to respond in an appropriate fashion.

**Awareness** is the program effort that the organization puts in place to remind employees through repetitive procedures and, at least, an annual update in-person of policy, procedures that support policy, and practices that they need to be aware of to comply with company policy.

Awareness would tend to be both formal and informal. Formal being a 20-minute annual awareness session, informal being excerpts in company newsletters, security awareness emails at appropriate times throughout the year, and reminders of special days (such as Global Security Awareness Week [http://www.globalsecurityweek.com]).

**Training** strives to produce relevant and needed security skills and competencies. The significant difference between training and awareness is that training seeks to teach a skill that allows a person to perform a specific function, while awareness seeks to focus an individual's attention on a particular issue or set of issues. An example of training is the course that a systems administrator might attend to learn how to better apply Microsoft Profiles to controlling changes to the desktop.

**Education** integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge. An example of security education is the formal course. An example of education is a degree program at a college or university.

## Program Components

The following major activities need to be undertaken to establish and maintain a comprehensive Awareness and Training program:

- Develop an Awareness and Training Plan
- Develop or acquire Awareness and Training Materials
- Implement the Awareness and Training Plan
- Complete ongoing Awareness and Training materials maintenance

The following deliverables are expected from this program:

- Needs Assessments
- Training Plans
- Awareness and Training Materials

## Develop an Awareness and Training Plan

In the developmental step of the program, the City of Winnipeg's awareness and training needs are identified, effective organization-wide awareness and training plans are developed, organizational buy-in is sought and secured, and priorities are established.
Priorities may include determining what awareness or training material will be developed first and who will be the first to receive the material.

## Structure

***Partially Decentralized Program Management Model***

In this model, security awareness and training policy and strategy are defined by a central authority, but implementation is delegated to line management in the organization. Awareness and training budget allocation, material development, and scheduling are the responsibilities of these managers.
The needs assessment is conducted by the central authority, because they still determine the strategy for the awareness and training program. Policy, strategy, and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units (i.e., City departments) develop their own training plans. The organizational units develop their awareness and training materials, and determine the method(s) of deploying the materials within their own units.

The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status of unit training plans, and progress reports on the implementation of the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit may be asked to describe lessons learned, so the central authority can provide effective guidance to other units.

***Decentralized Program Management Model (Centralized Policy/Distributed Strategy and Implementation)***

The City of Winnipeg is a relatively large organization and has a very decentralized structure with general responsibilities assigned to the central, corporate level entities and specific businesses and responsibilities assigned to its various departments and special operating agencies. The City's functions are spread over a wide geographical area. The City departments and other similar bodies are quasi-autonomous organizational units with separate and distinct missions. Awareness and training programs may need to differ greatly.

Based upon the City's size, organization and budgetary constraints, Seccuris recommends that the City adopt a fully decentralized program management model.

In this model, the central security awareness and training authority (IT security program manager) disseminates broad policy and expectations regarding security awareness and training requirements, but gives responsibility for executing the entire program to the various City departments.

This model uses the already-existing directives, driven from the central authority.

The needs assessment is conducted by each department, because in this model the department determines the strategy for the awareness and training program. Policy and budget are passed from the central authority to the departments.

Based on the strategy, the departments develop their own training plans. The departments develop their awareness and training material, and determine the method of deploying the material within their own departments.

Communication (between the central authority and each department) travels in both directions in this model. The central authority communicates the City's policy directives regarding IT security awareness and training, and the budget for each department. The central authority may also advise the organizational units that they are responsible for conducting their own needs assessment, developing their strategy, developing training plans, and implementing the program. The central authority may provide guidance or training to the organizational units so that they can carry out their responsibilities.

***Needs Assessment***

A needs assessment should be used to determine each department's awareness and training strategy. In conducting a needs assessment, it is important that key personnel be involved. At a minimum, the following roles should be addressed in terms of any special training needs:

- Executive Management
- Security Officers
- Privacy Officers
- System Administrators, other IT Support Personnel, or both
- Managers/Supervisors
- Users/Front line employees

A variety of sources of information in each department can be used to determine awareness and training needs. There are varying potential methods to collect that information, including:

- Conversations and interviews with management, owners of general support systems and major applications, as well as other organizational staff whose business functions rely on information systems
- Review and assessment of available resource materials, such as any current awareness materials
- Review of security plans for general support systems and major applications to identify system and application owners and appointed security representatives
- Review of system inventory and application user ID databases to determine all who have access
- Review of any findings and/or recommendations from oversight bodies (for example, internal review/audit) or third-party program reviews regarding the security program
- Analysis of events (such as successful virus attacks) might indicate the need for training (or additional training) of specific groups of people
- Review when technical or infrastructure changes are made

Key questions to be answered in the needs assessment include:

- What awareness, training, and/or education is needed—what is required)?
- What is currently being done to meet these needs?
- What is the current status regarding how these needs are being addressed—how well are current efforts working?
- Where are the gaps between the needs and what is being done—what more needs to be done?
- Which needs are most critical?

***Strategy and Plan***

Completion of the needs assessment allows each department to develop a strategy for developing, implementing, and maintaining its awareness and training program. The plan is the working document containing the elements that make up the strategy. The plan should discuss the following elements:

- Policy that requires awareness and training be accomplished
- Scope of the awareness and training program
- Roles and responsibilities of personnel—who should design, develop, implement, and maintain the awareness and training materials, and who should ensure that the appropriate users attend or view the materials
- Goals to be accomplished for each aspect of the program (for example, awareness, training, or education)
- Target audiences for each aspect of the program
- Mandatory (and/or optional) courses or materials for each target audience
- Learning objectives for each aspect of the program
- Topics to be addressed in each session or course
- Deployment methods to be used for each aspect of the program
- Documentation, feedback, and evidence of learning for each aspect of the program
- Evaluation and update of materials for each aspect of the program
- Frequency that each target audience should be exposed to materials

### *Establishing Priorities*

Once the awareness and training strategy and plan have been finalized, an implementation schedule should be established. If this needs to occur in phases (due to budget constraints, resource availability, etc.) then it is important to decide the factors to be used in determining which initiative to schedule first and in what sequence. Some key factors to consider are:

- **Availability of Materials/Resources**—If course materials must be developed and/or instructors must be identified and scheduled, these requirements should be considered when setting priorities.

- **Role and Organizational Impact**—Priority may be addressed in terms of organizational role and risk. General awareness initiatives may receive high priority because the basic rules of good security practices can be delivered to all users quickly. High trust/high impact positions (for example, system administrators) should receive high priority in the rollout strategy.

- **State of Current Compliance**—This involves looking at major gaps in the awareness and training program (gap analysis) and targeting deficient areas for early rollout.

- **Critical Project Dependencies**—If there are projects dependent upon security training (for example, the rollout of a new operating system or an enterprise wide application) then the training schedule needs to ensure that training occurs within the time necessary to address these dependencies.

### *Budget*

Once an awareness and training strategy has been agreed upon and priorities established, funding requirements should be added to the plan. The extent of funding support should be determined based upon existing or anticipated budget and other priorities. The awareness and training plan should be viewed as a set of minimum requirements to be met.

#### One-Time Costs

A portion of the content might be provided by existing resources. There would be one-time costs associated with the purchase of an off-the-shelf solution, and with the creation of new materials and/or revision of the materials to fit each department's context. These costs might include a consultant assisting with creation or revision activities, but there may be internal resources that could perform this work.

#### Ongoing Operating Costs

Operating costs associated would be related to the ongoing management and sustainability of the awareness and training program. The operating budget for materials, equipment, and other supplies should be budgeted.

## Develop or Acquire Awareness and Training Materials

This stage focuses on available training sources, scope, content, and development of training materials, including solicitation of contractor assistance if needed.
Once the awareness and training program has been designed, then supporting materials can be developed or acquired, with the following kept in mind:

- What behavior ought to be reinforced? (Awareness)
- What skills ought the target audience learn and apply? (Training)

The focus should be on specific materials that the participants should integrate into their jobs. Changing attitudes and behavior in terms of security can be challenging. New policies might be seen as conflicting with the way users have done their job for years. One technique that might be used to educate users to necessary changes is to begin an awareness session by discussing security issues in the context of personal experience (for example, the results of inappropriate access to personal information).

***Developing Materials***

The awareness and training plan should identify an audience, or several audiences, that should receive training tailored to address their security responsibilities.
The awareness and training plan should contain a list of topics. Email advisories, online information security websites, periodicals and the City's own policies are all possible sources of ideas and materials. Topics might include:

- Password use and management—creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code
- Policy—implications of noncompliance
- Individual accountability – explain what this means within the City and within each department generally
- Unknown email/attachments
- Web use—allowed versus prohibited; monitoring of user activity
- Incident response—who should be contacted? What steps should be taken?
- Mobile data storage and computing devices (e.g., USB Data Sticks)—address both physical and wireless security issues
- Laptop security while traveling—address both physical and information security issues
- Use of encryption and the transmission of confidential information via the internet
- Access control issues—address least privilege and separation of duties
- Desktop security—discuss use of screensavers, restricting visitors' view of information onscreen (preventing or limiting *shoulder surfing*), and allowed access to systems
- Protect information subject to confidentiality concerns—in systems, archived, on backup media, in hardcopy form, and until destroyed

***Sources of Awareness and Training Materials***

When determining sources of training materials to build courses, it should be decided whether the materials will be developed in-house or contracted out. Each department could leverage in-house expertise and allocate the necessary resources to develop training materials and courses.

If a department decides to outsource its training materials development, there are a number of vendors that offer off-the-shelf solutions that may be suitable or that can be tailored for specific audiences. Prior to selecting a particular vendor, each department should have a thorough understanding of its training needs and be able to determine if a prospective vendor's materials meets those needs.

Alternatively, each department can work with other departments, the Security Committee, or other organizations to develop materials and/or coordinate awareness and training events that meet their needs.

A department can also explore the acquisition of training materials that have been developed by other organizations or governmental bodies; materials that can be edited inexpensively rather than developing completely new courses or materials. Care should be taken that the available materials are applicable to the intended audience, and that the materials address what prospective attendees need to know to satisfy their security responsibilities.

***Implement an Awareness and Training Plan***

This stage addresses effective communication and rollout of the awareness and training program. It also addresses options for delivery of awareness and training materials (for example, web-based courses, and onsite sessions).

The program's implementation must be fully explained to the organization to achieve support for its implementation and commitment of necessary resources. This explanation includes expectations of departmental management and staff, as well as expected results of the program and benefits to the organization.

By the time the program is to be implemented, the department should have conducted the needs assessment, developed the training plan, and developed the awareness and training materials. Executive Management should be briefed on the implementation plan and they would grant approval to communicate it throughout the department.
Once the implementation plan is approved, the plan should be communicated to organizational unit manager/supervisors, providing the schedule for awareness and training offerings. The organizational unit managers/supervisors should then communicate the plan to their staff, identify the awareness and training required, and schedule attendees.

***Techniques for Delivering Awareness and Training Materials***

Many techniques exist to get a message, or a series of messages, spread throughout the organization. The techniques chosen depend upon resources and the complexity of the message.
Techniques that may be considered include, but are not limited to:

- Posters—*do and don't* lists, checklists
- Screensavers and warning banners/messages

- Newsletters
- Desk-to-desk alerts (for example, a hardcopy, brightly-colored, one-page bulletin—either one per desk or routed throughout the office)
- Organization-wide email messages
- Web-based sessions
- Computer-based sessions
- Teleconferencing sessions
- In-person, instructor-led sessions
- *Information Security Day* or similar events
- "Brown bag" lunchtime sessions
- Pop-up calendar with contact information and monthly security or privacy tips
- Awards program (for example, letters of appreciation)

Repeating an awareness message and using a variety of ways of presenting that message can greatly increase users' retention of awareness lessons or issues. For example, discussion in an instructor-led session about avoiding being a victim of a social engineering attack can be reinforced with posters and organization wide email messages.

## Ongoing Awareness, Training, and Materials Maintenance

This stage gives guidance on keeping the program current and monitoring its effectiveness. Effective feedback methods are described (for example, focus groups).

An awareness and training program might become obsolete if attention is not paid to technology advancements, infrastructure changes, and shifts in organizational priorities. Over time, as environmental changes take place, new risks may be introduced into a department's infrastructure. This potential problem should be recognized, and the department should incorporate mechanisms into their strategy to ensure the program continues to be relevant. Continuous improvement should be the theme for awareness and training initiatives.

Formal evaluation and feedback mechanisms are critical components for the awareness and training program. Continuous improvement cannot occur without a sense of how the existing program is working. The feedback mechanism should be designed to address objectives initially established for the program. Once such baseline requirements have been determined, a feedback strategy can be designed and implemented.

A feedback strategy needs to incorporate elements that will address quality, scope, deployment method (for example, web-based, onsite, and offsite), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Several methods can be applied to solicit feedback, including:

- Focus Groups—Bring subjects of the training together in open forums to discuss their perspectives on the training program effectiveness and solicit their ideas for improvement.
- Selective Interviews—This approach first identifies training target groups based on impact, priority, or other established criteria and identifies specific areas for feedback. Conducted using one-on-one interviews or in small groups, this approach is more personalized and private than the focus group approach. It may encourage participants to be more forthcoming in their critique of the program.
- Independent Observation/Analysis—Another approach for soliciting feedback is to incorporate a review of the awareness and training program as a task to an outside contractor or other third party as part of an organization-initiated audit. A department (or the City) could do this to get an unbiased opinion regarding its program effectiveness.
- Formal Status Reports—Another way to keep focus on awareness and training requirements organization wide is to implement a requirement for regular status reporting by functional managers/supervisors.