City of Westminster Enterprise Cyber Security Training – Executive Summary

Updated 2018

Purpose

The purpose for this executive overview is to provide a high-level view of the City's Enterprise-Wide End User Security Awareness Training Program

SANS End User Security Training Program

Cybersecurity awareness training is an important piece of the City of Westminster's overall cybersecurity program. In 2010, the Information Technology Department initiated an optional in-house training class for employees to learn how to protect City networks and data from those who might use social engineering techniques to gain unauthorized access. Those classes helped to expand the knowledge of attendees and lowered the risk of security breaches.

In order to gauge the City's potential risk of social engineering attacks, the City added an end user social engineering test component to the annual security audit conducted by an outside security firm. Results from the social engineering test showed positive results in 2011 and 2012, but in 2013 several employees provided information and physical access to the security firm's undercover representative. The information and access provided could have led to a potential security breach event in the City if used by an unauthorized individual.

Following the 2013 test, the Information Technology Department investigated strategies to broaden the depth of security training for the end users throughout the organization. In a presentation to the executive management team, full agreement was achieved in support of initiating a mandatory end user cybersecurity training program.

As opposed to using a significant amount of IT Department staff hours to train every permanent employee in the City, staff evaluated more cost-effective options and acquired the SANS ACLP (Advanced Cybersecurity Learning Platform).

All fulltime benefitted employees were required to complete the training in 2018. To date, more than 950 employees have successfully completed the training. All new employees are required to complete the program within 90 days after their start date. This program provides the training modules as shown below. Depending on the department, employees are required to complete between 12 and 18 specific training modules, with others made available as optional. The results of the 2018 security audit social engineering test will be used to determine the success of this program, but feedback from many employees has been very positive in terms of content and knowledge gained.

Awareness Training Modules

- You Are the Shield
- Social Engineering
- Email & Phishing

- Browsing Safely
- Social Networks
- Mobile Devices
- Passwords
- Encryption
- Data Security
- Working Remotely
- Physical Security
- Creating a Cyber Secure Home
- Protecting Your Home Network
- Protecting Your Kids Online
- Hacked
- Ethics
- Senior Leadership
- Targeted Attacks
- Cloud Services
- International Travel
- Malware
- Privacy

Compliance Training Modules

- PCI-DSS
- FERPA
- HIPAA
- Personality Identifiable Information
- Criminal Justice
- Federal Tax Information
- Gramm-Leach-Bliley Act: Educational
- Gramm-Leach-Bliley Act: Financial
- International Traffic in Arms Regulations
- Data Retention
- Social Security Numbers
- Foreign Corrupt Practices Act
- Federal PII
- EU Data Protection
- Client Confidentiality in Law Offices