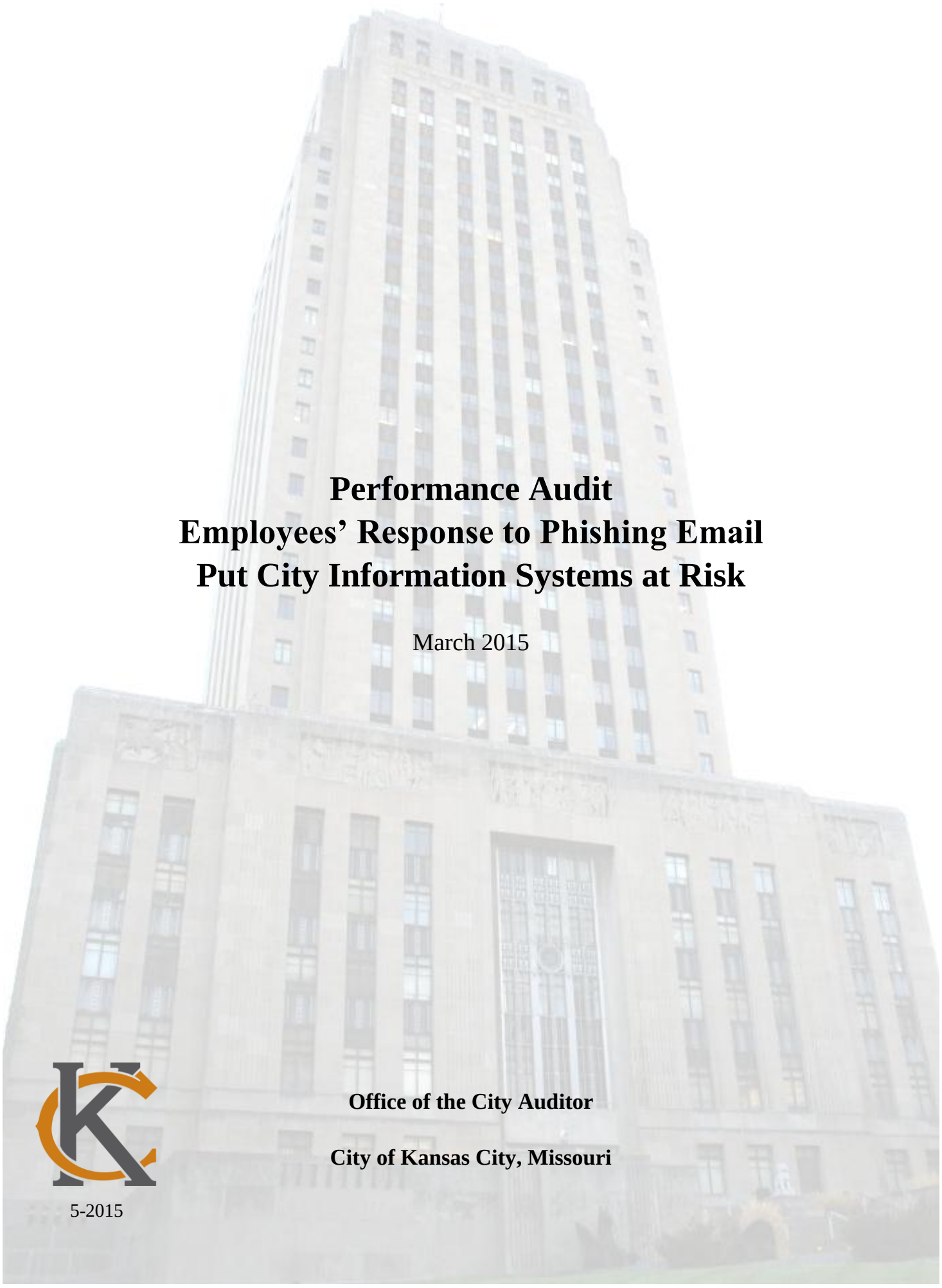


Performance Audit
Employees' Response to Phishing Email Put City Information Systems at Risk

March 2015

Office of the City Auditor

City of Kansas City, Missouri

5-2015

CITY OF FOUNTAINS
HEART OF THE NATION
KANSAS CITY
MISSOURI

Office of the City Auditor

21st Floor, City Hall
414 East 12th Street
Kansas City, Missouri 64106

(816) 513-3300
Fax: (816) 513-3305

March 25, 2015

Honorable Mayor and Members of the City Council:

This performance audit focuses on whether city employees are prepared to respond appropriately to phishing emails. Phishing is a social engineering attack that uses email or malicious websites to solicit personal information or system credentials by posing as a trustworthy organization.

Cyber attacks, such as phishing emails, have become not only more numerous and diverse but also more damaging and disruptive. Because cyber attacks frequently compromise personal and business data, it is critical to identify the attacks early and respond quickly and effectively when breaches occur. Employees must be vigilant in order to protect the information the city collects from taxpayers, citizens, vendors, employees, and the public.

To test how employees would respond, we sent phishing emails to all city employees with city email addresses enticing them to click on a link and provide their network login information. Some employees put the city's information systems at risk by clicking on the link of a fake website in our phishing email; providing valid login credentials that could be used to hack the city's system; and not changing their passwords after they were alerted. Hackers can take advantage of employees' actions to harm the integrity, confidentiality, and availability of the city's information systems.

The Information Technology Division (ITD) has detection tools in place to limit phishing and other cyber attacks, but it cannot prevent all attacks. During our phishing test, ITD took appropriate steps to respond to our phishing email. Although ITD has practices in place to respond to phishing emails, they are not written. In addition, ITD does not have a comprehensive cyber security incident response plan. A cyber attack can happen at any time. It is important to have a comprehensive response plan in place so the response will be quick, consistent, and effective.

We make recommendations to ensure that employees respond to phishing emails and other social engineering attacks appropriately and that cyber incidents are promptly identified, exploited weaknesses are mitigated, loss and destruction are minimized, and IT services are restored.

The draft report was made available to director of general services on February 24, 2015 for review and comment. His response is appended. We would like to thank General Services Department's Information Technology Division staff for their assistance and cooperation during this audit. The audit team for this project was Sue Polys and Vivien Zhi.

Douglas Jones
City Auditor

Employees' Response to Phishing Email Put City Information Systems at Risk

Table of Contents

List of Exhibits

Introduction

Objectives

We conducted this audit of how city employees respond to phishing emails under the authority of Article II, Section 216 of the Charter of Kansas City, Missouri, which establishes the Office of the City Auditor and outlines the city auditor's primary duties.

A performance audit provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making, and contribute to public accountability.[1]

This report is designed to answer the following question:

- Are city employees prepared to respond appropriately to phishing emails?

Scope and Methodology

Our review focuses on whether city employees are prepared to respond appropriately to phishing emails. Our audit methods included:

- Setting up a fake website and conducting a phishing test to determine how employees responded.
- Analyzing the phishing test results to determine the proportion of employees who responded to the phishing email.
- Interviewing Information Technology Division (ITD) staff to determine how ITD responded to the phishing email and to employees' help desk calls and emails about the phishing email.

[1] Comptroller General of the United States, *Government Auditing Standards* (Washington, DC: U.S. Government Printing Office, 2011), p. 17.

- Reviewing the National Institute of Standards and Technology's (NIST) *Building an Information Technology Security Awareness and Training Program*; Verizon's *2014 Data Breach Investigations Report*; and the State of Oregon's Information Security Resource Center's *18 Best Practices in Security Awareness Training* to identify criteria and recommended practices related to security awareness training.

- Reviewing the NIST's *Computer Security Incident Handling Guide* and Multi-State Information Sharing and Analysis Center's *Cyber Incident Response Guide* to identify criteria and recommended practices related to cyber security incident response planning.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. No information was omitted from this report because it was deemed privileged or confidential.

Background

Cyber Attacks

Cyber attack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[2] Cyber attacks may include[3]:

- External/removable media: an attack executed from removable media or a peripheral device, such as a flash drive.
- Attrition: an attack that employs a brute force method to compromise, degrade, or destroy systems, networks, or services.

[2] "*National Information Assurance (IA) Glossary*", Committee on National Security Systems (CNSS) Instruction No. 4009, April 2010, p. 22.
[3] "*Computer Security Incident Handling Guide*", National Institute of Standards and Technology, August 2012, p. 2.

- Web: an attack executed from a website or web-based application.
- Email: an attack executed via an email message or attachment.
- Improper usage: any incident resulting from violation of an organization's acceptable information technology usage policies by an authorized user.
- Loss or theft of equipment: the loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

Social Engineering and Phishing

Social engineering is an attack to lure information system users and administrators into revealing sensitive and confidential information, such as social security numbers, bank account numbers, passwords, etc. Social engineering attacks include facility intrusion, impersonation via telephone, phishing email, etc. Social engineering exploits the user's lack of awareness of information technology security.

Phishing is a social engineering attack that uses email or malicious websites to solicit personal information or system credentials by posing as a trustworthy organization.

Identifying Phishing Emails

The best defense against phishing is being mindful of potential phishing traps and observant of the obvious signs of a scam. Below are some easy tips to identify phishing scams:

- The email has poor spelling or grammar.
- The email requests personal information. Legitimate businesses will not ask users to send their personal information through email.
- The email seems too good to be true or the content places any kind of urgency.
- The email is sent with a generic greeting such as "Dear Customer" or "Dear Member."
- The email contains attached files. The majority of banks and retailers will not send attachments via email.
- If you see a link in a suspicious email message, do not click on it. Rest your mouse on the link to see whether the address matches the link that was typed in the message.
- You can view the email sender to see from where the message really originated. Just hover your mouse arrow over the name in the "From" column to determine whether the email is from a recognizable domain that is linked to the actual sender.

Sources: *Protect Yourself from Email Phishing Attacks*, Multi-State Information Sharing and Analysis Center, April 2013; *Avoiding Social Engineering and Phishing Attacks*, US Computer Emergency Readiness Team, February 2013; *How to Recognize Phishing Email Messages, Links, or Phone Calls*, Microsoft.com Safety and Security Center; *How to Recognize Phishing Email*, CNET, November 2009*; Identifying Fraudulent Phishing Email*, Apple Support, March 2014; *How Can I Identify a Phishing Website or Email?*, Yahoo Safety; and *10 Tips on How to Identify a Phishing or Spoofing Email*, Return Path, May 2013.

City Auditor's Office Conducted a Phishing Test

As part of our audit, we sent phishing emails to all city employees with city email addresses to determine whether employees are alert for phishing emails and respond appropriately. The email was designed to entice employees to provide sensitive information, such as login IDs and passwords, as would a phishing email from a hacker. The email contained indications that should have alerted staff that the email was a phishing attempt.

Findings and Recommendations

Summary

During our phishing email test, some employees put the city's information systems at risk by clicking on the link of a fake website in the phishing email; providing valid login credentials that could be used to hack the city's system; and not changing their passwords after they were alerted. Hackers can take advantage of employees' actions to harm the integrity, confidentiality, and availability of the city's information systems. Information technology security is as much a human issue as it is a technology issue. Employees need to be aware of cyber security and learn to recognize and protect the city from phishing and other social engineering attacks.

During our phishing test, ITD took appropriate steps to respond to our phishing email. Although ITD has practices in place to respond to phishing emails, they are not written. In addition, ITD does not have a comprehensive cyber security incident response plan. A cyber attack can happen at any time. It is important to have a comprehensive response plan in place so the response will be quick, consistent, and effective.

Employees' Actions Put City's Information Systems at Risk

During our phishing email test, a number of employees put the city's information systems at risk by clicking on the link of a fake website in the phishing email; providing valid login credentials that could be used to hack the city's system; and not changing their passwords after they were alerted. In addition, the city does not provide IT security awareness training. Employees need to be trained to recognized and protect the city from phishing and other social engineering attacks.

Employees Visiting Unknown Websites Puts City Information Systems at Risk

Some employees inappropriately clicked on the website link embedded in our phishing email. Hackers can send a link to a fake website that is laced with malware, a type of software intended to steal information or spy on computer users without their knowledge. If the computer is

infected with malware, the hacker can log the user's key strokes and gain remote access to the employee's computer, and ultimately the network, which could harm the integrity, confidentiality and availability of the city's information systems.

We embedded a link to a fake website in our phishing email test, enticing city employees to click on the link to the website. Employees visited the website over 600 times within the first 24 hours after the emails were sent.[4] Had this been an actual phishing attack and the fake website laced with malware, over 600 city computers could be infected with malware.

Employees Sharing Their Credentials Places City's Information Systems at Risk

About 280 city employees provided their system login information, including email address, login ID, and password to the fake website. Employees should not use their city email address for personal online activities. Employees should also not provide their city email address or network login and city password to any website even if it appears work related because hackers can use this information to gain direct access to the city's network and perform malicious acts. Had our test been an actual phishing email, a hacker would have about 280 chances to infiltrate the city's information systems. Although some employees gave invalid credentials because they suspected the email was a phishing email, just clicking the website link in the email could expose the city's information systems to risk.

Employees who provided their credentials were from all city departments, including staff from departments that have greater access to PeopleSoft and other important city systems. These systems contain confidential and sensitive information such as tax records, personnel information, and financial information. Information in these systems attracts hackers because it can be illegally sold or used to make money.

Employees Not Taking Action Once Alerted Puts the City at Risk

Not all employees responded appropriately after being alerted about the phishing attack. City Communications sent out a myKC email advising employees that the phishing email was fraudulent and not to click on the link. The email instructed employees who had clicked on the link to change their passwords as soon as possible. Not all employees reset their passwords as instructed.

[4] We cannot determine whether these visits were repeated or unique employee visits because when visiting the internet from the city's network, the IP address is the same.

We reviewed password change records for the employees who provided their credentials to the fake website. Twenty-eight employees still had not changed their passwords two months after being told the email was fraudulent. About 70 percent of the employees who provided their credentials changed their passwords within a day. (See Exhibit 1.) Some employees changed their passwords days or weeks after submitting their user names and passwords to the fake website, which suggests that these employees may have only changed their passwords when it expired. Had this been a real phishing attack, employees who did not change their passwords would have given hackers more time to use the password information to access the city's systems and cause damage.

Exhibit 1. Time Employees Took to Change Their Passwords

Time Passwords Changed	Number of Employees	Percentage of Employees
Within 24 hours	190	66%
Within 48 hours	10	3%
At least 48 hours later	58	20%
Password never changed	28	10%

Source: Information Technology Division and CAO analysis.

Information Technology Security Awareness Training Needed

The city does not provide information technology (IT) security awareness training. Recommended practices state "a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies and how to properly use and protect the IT resources entrusted to them."[5] Failure to provide security training puts the city at great risk. Although the city's spam filter blocks out many phishing emails, it does not block all. City employees need to be trained on how to recognize and protect the city from phishing and other social engineering attacks.

Recommended practices suggest IT security awareness training be mandatory for all users of an organization's information technology, including contractors with access to the organization's information. IT security awareness training should include information on known threats; the organization's security requirements; legal responsibilities; information on the organization's disciplinary process; and who to contact for further security advice or to report incidents. At a minimum, all computer users should be exposed to IT security awareness material annually. An on-going awareness program using multiple training

[5] *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology, October 2003, p. 1.

methods to suit different learning modes, can be very effective and could minimize training costs.

Training Methods for IT Security Awareness

Below are some methods for delivering awareness training:

- Citywide email messages
- Pop-up calendars with security contact information, monthly security tips, etc.
- "Brown bag" seminars
- IT security days or similar events
- Web-based sessions/webinars
- Posters, "do and don't lists," or checklists
- Screensavers and warning banners/messages
- Newsletters
- Desk-to-desk alerts (e.g., a hard copy, bright-colored, one page bulletin)
- Teleconferencing sessions
- In-person, instructor-led sessions
- Crossword puzzles
- Awards programs

Source: *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology, October 2003.

To protect the integrity, confidentiality, and availability of the city's information systems and ensure city employees respond to phishing emails and other social engineering attacks appropriately, the director of general services should implement an IT security awareness training program and provide mandatory security awareness training on a continuous basis for all city IT users, including contractors with access to the city's information systems.

Comprehensive Cyber Security Incident Response Plan Could Ensure Consistent Response

During our phishing test, ITD took appropriate steps to respond to our phishing email; however, ITD does not have written procedures to respond to a phishing or social engineering attacks. Standardized

response procedures could help to minimize errors, particularly those that might be caused by stressful incident handling situations. It is important to have a comprehensive incident response plan in place so the response will be quick, consistent, and effective.

ITD Took Appropriate Steps in Response to Phishing Email

ITD took appropriate steps to respond to our phishing email. After ITD noted how widespread the email was, ITD staff instructed help desk callers not to click on the link, investigated whether the email was legitimate, and alerted city employees that it was a fraudulent email. The information security officer also deleted the phishing email from the city's email so that no one else could click on the link; however, the email was not deleted for at least a day.

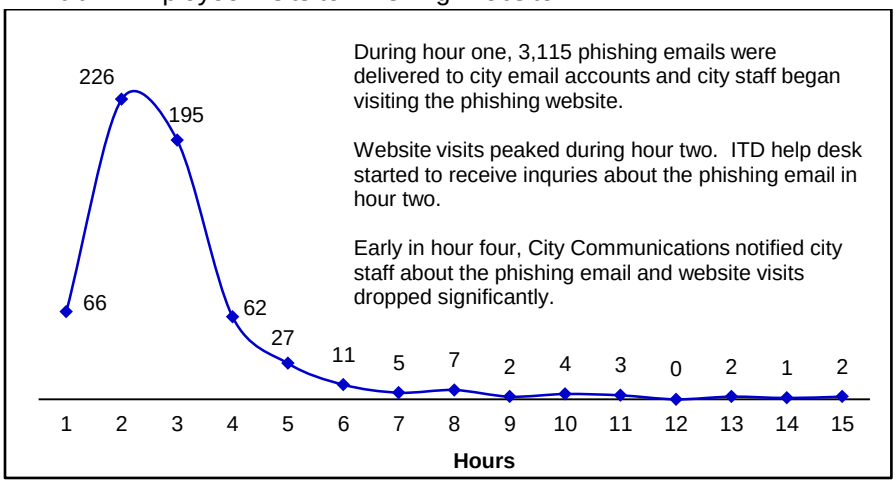
Comprehensive Response Plan Could Strengthen ITD's Response

ITD does not have written procedures to respond to phishing or social engineering attacks. Although ITD has a cyber terrorism mitigation plan to respond to incidents that disrupt operations and may require moving the operation to an alternate site, the plan does not include procedures on how to respond to lesser attacks, such as our phishing email. The impact of cyber attacks can range from system crashes to unauthorized access to sensitive data. A comprehensive response plan can help staff to respond to both major and minor cyber attacks.

ITD has detection tools for limiting phishing and other cyber attacks and can block employees' access to known dangerous websites. Although the city's email filters are set to detect and quarantine possible phishing emails from suspicious senders, not all phishing emails, like ours, can be detected. Once a phishing email gets through, ITD staff needs to know how to respond to it. In the case of our phishing email, help desk staff told callers not to click on the link and waited for the help desk manager to investigate whether the email was legitimate. It took about an hour for ITD to confirm that the email was fraudulent because the help desk manager was waiting for responses from some key staff.

A cyber attack and damages associated with such an attack can happen quickly. During our test, almost ninety percent of the phishing website visits happened within the first four hours after the email was sent. (See Exhibit 2.) Because a cyber attack can happen at any time and untrained employees may respond inappropriately to phishing or other social engineering attacks, it is important to have a comprehensive response plan in place so the response will be swift, consistent, and effective.

Exhibit 2: Employee Visits to Phishing Website



Source: Google Analytics and CAO Analysis.

According to recommended practices, a comprehensive cyber security incident response plan should include policies, plans, and standard operating procedures on how to detect and identify an incident quickly, how to limit the impact of the incident, and how to remove the threat and recover to normal operations. The plan should define computer security incidents, procedures, staff's roles and responsibilities, and prioritize the severity of incidents. In addition, the plan should include steps to document the incident, discuss the lessons learned, and identify ways to improve the process.

To promptly identify cyber security incidents, minimize loss and destruction, mitigate the weakness that was exploited, and restore IT services, the director of general services should develop a comprehensive cyber security incident response plan that includes policies, plans and procedures related to all types of cyber security attacks.

Recommendations

1. The director of general services should implement an IT security awareness training program and provide mandatory training on a continuous basis for all city IT users, including contractors with access to the city's information systems.

2. The director of general services should develop a comprehensive cyber security incident response plan that includes policies, plans and procedures related to all types of cyber security attacks.

Appendix A

Director of General Services' Response

CITY OF FOUNTAINS
HEART OF THE NATION

KANSAS CITY
MISSOURI

Inter-Departmental Communication

General Services Department

RECEIVED
MAR 18 2015
CITY AUDITOR'S OFFICE

Date: March 17, 2015

To: Douglas Jones, City Auditor

From: Earnest Rouse, Assistant City Manager/Director of General Services

Subject: Response to Performance Audit: *Employees' Response to Phishing Email Put City Information Systems at Risk*

Recommendation 1

The director of general services should implement an IT security awareness-training program and provide mandatory training on a continuous basis for all city IT users, including contractors with access to the city's information systems.

Agree. The director of general services will identify needed resources to administer this training to all city IT users. Upon the completion of this needs assessment and appropriate resources are identified, the training program can begin.

Recommendation 2

The director of general services should develop a comprehensive cyber security incident plan that includes policies, plans and procedures related to all types of cyber security attacks.

Agree. The director of general services has requested the chief information officer to develop a comprehensive cyber security plan and it is anticipated to be complete within four to six months.

cc: Troy M. Schulte, City Manager
Mary J. Miller, Chief Information Officer