Minimizing Online Security Threats in your Municipality

Joey Howland
Chief Information Security Officer

What is Cybersecurity?

- Set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access
- Many different pieces go into securing your environment

2

Cyber Security Quiz!

Open https://kahoot.it/ in your browser

Kahoot!

3

What is Cybersecurity?

eGobbler group target US users with a massive malvertising campaign

February 20, 2019 | Identity Theft, Fraud, Scams

Phishing campaign uses fake Office 365 page with live chat support

February 25, 2019 | Identity Theft, Fraud, Scams

Hinesville suffering IT outage

City's servers, computers and phones impacted

Staff report
Coastal Courier
POSTED: February 20, 2019 2:20 p.m.

Scammers Are Spoofing DHS Phone Numbers to Get Your Personal Info

Voicemail system at Newfane Town Office hacked

Big phone bill

Are Local Governments Prepared?

Cybersecurity survey performed by University of Maryland

- Over 3,400 local governments polled

- 41% of respondents did know if they had ever been breached
- 66% have no formal cybersecurity risk management or recovery processes
- 42% top appointed officials believe security responsibility belongs only to technologists
- 31% of respondents knew an attack had occurred but did not know if it started inside or outside the organization

5

Quiz Time!

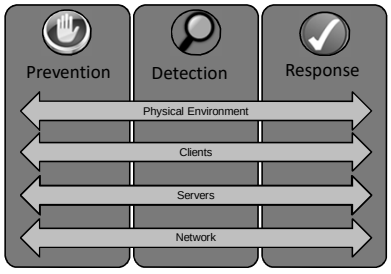
6

Security Breach Statistics

- In 2017, the government vertical in the US became the largest group to suffer loss due to data breaches
- On average, 57 confidential records are lost every second
  ...that's 4,924,800 records per day
- Almost 1.5 billion were lost in the month of March 2018
- The average cost for organizations reporting data breaches in 2017 was $3.62 million dollars per breach
- Security experts believe the majority of data breaches are either undetected or unreported!

7

Security Management Framework



8

Prevention Framework

Solutions to pro-actively identify weaknesses in your IT infrastructure and alert to issues that may be security related

Examples:

- Anti-Virus is a security prevention mechanism that runs on workstations and servers
- Monthly software patching prevents security incidents by closing known security holes

9

Detection Framework

Technologies used to detect suspicious traffic or behaviors

Examples:

- Security scans are used to probe networks for holes so they can be closed before an attacker identifies them
- Intrusion Detection Services identify malicious network traffic and can alert someone that an attack is occurring

10

Response Framework

Solutions and processes that help mitigate the impact of a security incident

Examples:

- An Incident Response Plan defines how an organization will respond to various categories of security incidents
- Cyber liability insurance helps cover the cost of mitigation should a breach occur

11

Assets to Protect

- Physical
- Local Client
- Server
- Network

12

Physical Security

- Limited access to critical areas
- Secure keys/badges
- Do not write passwords down somewhere potentially accessible
- Secure devices that have access to data
- Do not connect unknown devices to the City network

13

Local Clients

- Antivirus installed on the local PCs
  - Protects the local client from malware and viruses
- User data saved to servers or cloud
  - Ensures data is backed up to prevent loss
- Do not give users administrative access to PCs
  - Helps prevent malicious code from executing
- Two factor authentication
  - Prevents even a compromised ID and password from being used by an attacker
- Apply security patches monthly
  - Closes known security holes

14

Servers

- Antivirus installed on all servers
  - Protects the server from malware and viruses
- Backup data and replicate offsite
  - Maintain ability to recovery deleted or encrypted files
- Give users access only to data they need
  - Users actions can't impact data they can't access!
- Apply security patches monthly
  - Closes known security holes

15

Network Security

- Separate wireless networks
  - Public Wi-Fi and internal Wi-Fi are on separate networks
- Monitor your firewalls
  - You can't stop something if you don't know it's happening!
- Security scans performed by independent agencies
  - Identify and close security holes before they are exploited

16

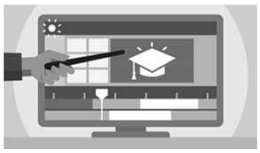
Incident Response Plan

How do I prepare my organization for a potential breach?

- Assess and categorize impact
- Engage your Incident Response team
  - Roles should be pre-defined
  - Nature of incident dictates which roles are required
- Containment – Stop the spread
- Eradicate – Remove the cause of the incident
- Recovery – Return to normal operation
- Lessons learned – How did it happen?
- Complete Incident Report

17

Quiz Review



18

Security Framework

- **Prevention**
  - Anti-Virus Platform
  - SPAM Filtering
  - Malware Protection
  - Data Loss Prevention
  - Patch Management
  - IPS (Intrusion Prevention Services)
  - User Policies and User Training
  - Change Control Policies and Procedures
  - Two Factor Authentication
  - Mobile Device Management
  - Web Filtering
- **Detection**
  - Rogue System Detection
  - IDS (Intrusion Detection Services)
  - SIEM (Security Incident and Event Management)
  - Regular Security Scans
- **Response**
  - Rock Solid Backups
  - Offsite Log Retention
  - Incident Response Plan

19

Contact Info:
lynn.kenyon@vc3.com
(803) 753-5441