# Protecting City Data

Don't let your city be impacted by ransomware and security threats. Find out what you can do to protect yourself and what you should do if your walls are breached.

**Presented by Joe Howland**

**Session #9**

## Grand Prizes!

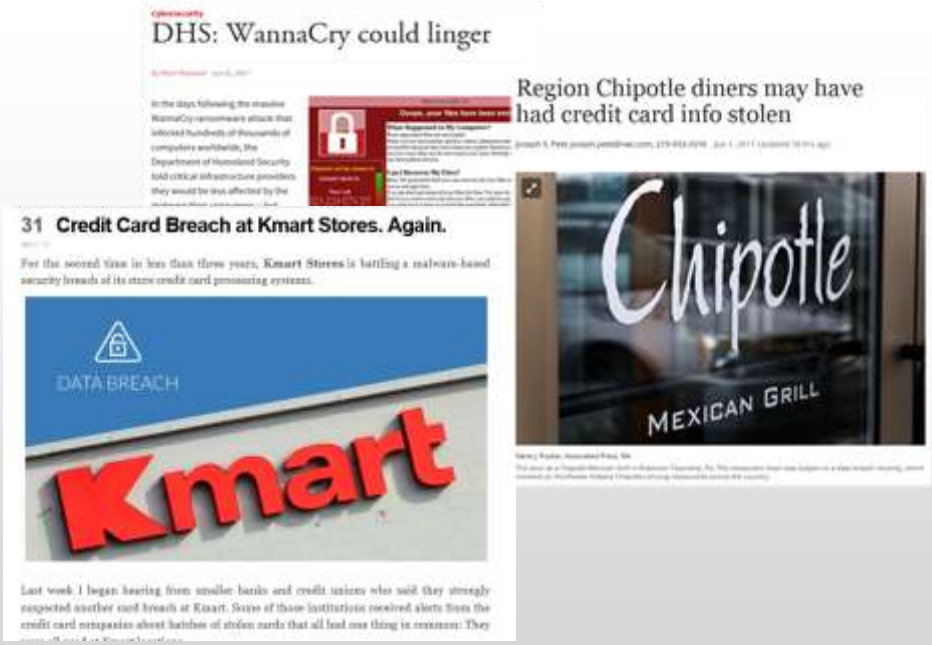
**Don't forget to fill out your cards!**

**Merge VR Headset**

**Amazon Echo**

VC3

Assess | Improve | Manage Information Technology



# End Users

## *Your #1 Security Risk*

- Grant access rights on an as needed basis
- Don't click on links in emails/texts
- Don't open attachments unless you are expecting them
- Don't click on email or pop-up messages that ask for personal or financial information
- Don't download and install software
- Don't email personal or financial information
- Implement encryption on laptops and mobile devices
- Exercise caution when accessing public hotspots
- Avoid risky sites (gambling, foreign, etc.)
- Install a comprehensive security suite
- Limit use of Administrator accounts
- *Don't ever share your password!!!!!*
- Implement dual factor authentication

# End User Training

***"Education is the first line of defense"***

- Explain the ramifications of a breach
- Start with basics
- Document rules for various situations
- Expose your employees to real work scenarios
- 3rd party providers that specialize in user security education

# Questions to ask your IT department

## *Preventative Maintenance*

- Do you regularly patch servers and workstations?
- When new IT assets are brought online, are they fully secured to organization best practices?
- Do you have a defined set of security best practices?
- When assets are retired, is care taken to ensure data cannot be recovered? (Printers!)
- Are you running Anti-Virus on every system in your organization? How do you know?
- Do you have an Anti-Spam solution in place?
- How will we react when a phone or laptop is lost or stolen?
- When was the last time we tested our backups?

# Incident Response Plan

***How will you react when the inevitable occurs?***

- 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

# Assess your security posture

## *Ask a 3rd party for assistance*

- Validate adequate protection on servers and workstations
- Perform an external penetration test to validate adequate firewall rules
- Review data backup configuration and policies
- Am I protected from a user clicking on a malicious link?

## Stop by our booth to learn more

Joe Howland, CSIO
Joe.Howland@vc3.com

# Don't Forget Your Cards!

**Merge Virtual Reality Headset**


**Amazon Echo**