



Avoid Becoming the Next News Headline

Presented by Joe Howland
Chief Information Security Officer
Session #5




Assess | Improve | Manage
Information Technology

Grand Prize



Don't forget to fill out your card!



Assess | Improve | Manage
Information Technology

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



Assess | Improve | Manage
Information Technology

Cybersecurity Events

Savannah city government recovering from malware attack

Loganville says city server may have been hacked
Social Security numbers, banking info among compromised data

Hinesville suffering IT outage
City's servers, computers and phones impacted

Staff report
Council Chamber
PHOTO: Savannah, GA, 2018 © J. Pittman



The FBI is investigating a ransomware attack on the city of Atlanta


City of Spring Hill computer system hit by ransomware
Phone: 651.557.4342 #17
Created: Nov 22, 2017 3:23 PM EST



Assess | Improve | Manage
Information Technology


Security Breach Statistics

- The government vertical in the US has become 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 was \$3.62 million dollars per breach
- Security experts believe the majority of data breaches are either undetected or unreported!



Assess | Improve | Manage
Information Technology

Security Management Framework




Prevention Detection Response

Physical Environment

Clients

Servers

Network



Assess | Improve | Manage
Information Technology


 **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


 Assess | Improve | Manage
Information Technology


 **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


 Assess | Improve | Manage
Information Technology

 **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

 Assess | Improve | Manage
Information Technology

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



10

Assess | Improve | Manage
Information Technology

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

11

Assess | Improve | Manage
Information Technology

Thank You!

For more information contact Lynn Kenyon.

lynn.kenyon@vc3.com

803-753-5441

12

Assess | Improve | Manage
Information Technology

Don't forget your card!



Suggestions and feedback?
Visit www.vc3.com/masc2018

13

Assess | Improve | Manage
Information Technology

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

14

Assess | Improve | Manage
Information Technology

Assets to Protect


- Physical
- Local Client
- Server
- Network

15

Assess | Improve | Manage
Information Technology

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




Assess | Improve | Manage
Information Technology

16

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




Assess | Improve | Manage
Information Technology

17

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




Assess | Improve | Manage
Information Technology

18

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



19

Assess | Improve | Manage
Information Technology
