

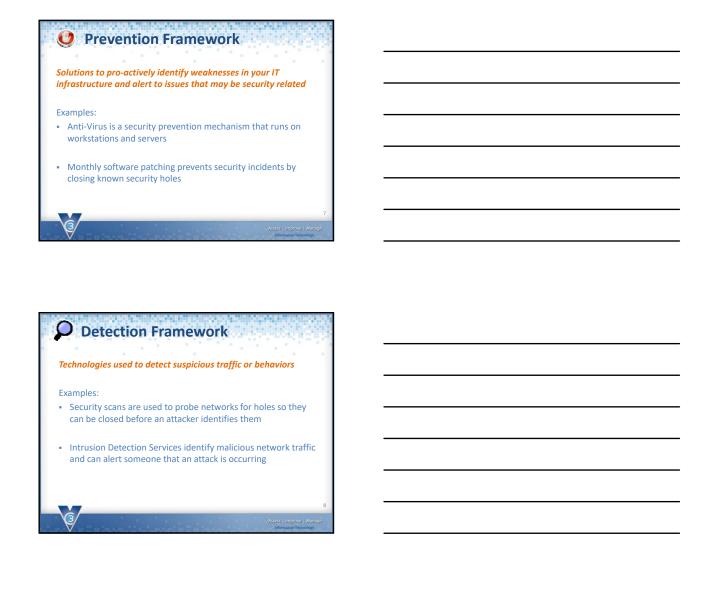






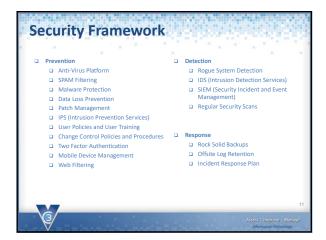
Security Breach Statistics The government vertical in the US has become the largest group to suffer loss due to data breaches On average, 57 confidential records are lost every second ...that's 4,924,800 records per day Almost 1.5 billion were lost in the month of March 2018 The average cost for organizations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







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







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

Assets to Protect Physical Local Client Server Network

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 | Man

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

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 | Mar

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 	<u></u>
• Identify and close security noies before they are exploited	
Assess Improve Menalge Information Rethology	