• Timothy M. Lott, Director of Operations – SEARCH

• Paul Weatherhead, CISSP – Digital Boundary Group

• Chief Terry Sult – City of Hampton, VA
Types of Attacks

- Denial of Services (DoS)
- Phishing
- Ransomware
- Malware
- Virus

- Worms
- Trojan Horse
- Social Media Attacks
- Social Engineering
- Theft
**History of ransomware**

— Emerged in Eastern Europe 2009

— Cyber criminals started using malicious code to lock up unsuspecting user machines

— Demand approximately 100 euros for user to regain access to their machine

— Over last decade multiple cyber criminal outfits as well as nation states have expanded these tactics
  - Targeting networks over individual machines
Cyber Attack Examples: Ransomware

- **How ransomware works**
  - Commonly begins when a single person opens malware disguised as a recognizable email attachment from a known user.
  - Once the attachment is opened the malware will begin to freeze data block by block until all the data is locked.
  - Often a countdown clock will appear with a ransom demand.
  - Some of the ransom notes contain directions on how to purchase bitcoin.
• **How ransomware works**
  — Not always delivered through email attachments
    ○ 3rd party access to network
  — Evolving from holding hostage to destruction
  — Loitering ransomware
Cyber Attack Examples: Ransomware

• **Attempted attacks worldwide**
  - 2014 3.2 million
  - 2015 3.8 million
  - 2016 638 million
  - 2017 2.4 billion

• **By the end of 2019 ransomware estimated to attack a business every 14 seconds by the end of 2019**

• **Why interested in my agency?**
  — automation

Cyber Attack Examples: Ransomware

- **Scope of Damages in US Dollars**
  - 2015 325 million
  - 2016 1 billion
  - 2017 5 billion*
    - Estimation due to underreporting
Atlanta Ransomware Attack

- March 22\textsuperscript{nd} 2018
- City of Atlanta Information Management Team learned of a computer outage
- Estimated cost to recover from attack 17 million
Police had to write incident reports by hand
Lost access to nearly all archived in-vehicle video
Affected processing of cases in Municipal Court
   — Unable to validate warrants
Payment for tickets, water bills and business licenses were also affected
Stopped taking employment applications
Shutdown WiFi at Hartsfield-Jackson Airport
Two months after initial attack 141 our of 424 software programs remained offline or partially inoperable
—30 percent of those were deemed mission critical by the city
A map of SamSam ransomware infections across America. DEPARTMENT OF JUSTICE
City of Baltimore Attack

- May 7th city services hit with Ransomware attack called RobbinHood
- Hackers demanded $75,000 to unlock the system
- FBI advised the City not to pay
- Total could reach 18 million dollars
An Unlikely Attack Vector?

Sports Arena (could be yours…)
City Hall (IT Partner)
Police Station (rather obvious…)

Pelladon at en.wikipedia

By Thomas1313 - Own work, CCBYSA3.0, https://commons.wikimedia.org/w/index.php?curid=22767785
Police Departments: Ransomware Victims

- **Collinsville, Alabama**
  - Refused to pay
    - Lost access to files
- **Dixon County, Tennessee**
  - Paid 622 dollars in bitcoin
- **Lincoln County, Maine**
  - Impacted four other police departments
- **Dallas, TX**
  - Hackers were able to set off tornado warning sirens in middle of the night
Real World Information Security

Presented by:
Paul Weatherhead, CISSP
Senior Security Specialist
- Vulnerability Assessments
- System Security Auditing
- Building Robust Security
• Full assessment should be performed every 12 – 18 months

• Vulnerability scans should be performed on a monthly basis or after any significant change

• Interpreting vulnerability scan results can be difficult, sometimes several low risk vulnerabilities can be combined to create high risk vulnerabilities

• Perform your own scans? Outsource? Maybe both?
• Which vulnerabilities do I remediate first?

• RemEDIATE CRITICAL SYSTEMS FIRST

• HOSTS EXPOSED TO THE INTERNET SHOULD BE THE HIGHEST PRIORITY

• VULNERABILITIES THAT REQUIRE NO USER INTERACTION OR AUTHENTICATION TO EXPLOIT ARE OFTEN WEAPONIZED TO DELIVER RANSOMWARE AND OTHER MALWARE. THESE VULNERABILITIES ARE CRITICAL TO REMEDIATE.
<table>
<thead>
<tr>
<th>Sev</th>
<th>Name</th>
<th>Family</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>MS17-010: Security Update for Microsoft Windows SMB Server (401...)</td>
<td>Windows</td>
<td>130</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Microsoft Windows SMBv1 Multiple Vulnerabilities</td>
<td>Windows</td>
<td>129</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>AXIS Multiple Vulnerabilities (ACV-128401)</td>
<td>Misc.</td>
<td>43</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>MS14-066: Vulnerability in Schannel Could Allow Remote Code Exec...</td>
<td>Windows</td>
<td>16</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Unsupported Windows OS</td>
<td>Windows</td>
<td>11</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>Microsoft Windows XP Unsupported Installation Detection</td>
<td>Windows</td>
<td>8</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>SNMP Agent Default Community Names</td>
<td>SNMP</td>
<td>7</td>
</tr>
<tr>
<td>CRITICAL</td>
<td>IBM Baseboard Management Controller Default Credentials</td>
<td>Misc.</td>
<td>6</td>
</tr>
</tbody>
</table>
• Can reveal evidence of a current or past incident
• Is useful for comparing system settings to best practices
• Tends to focus on policies, procedures, and documentation
• Is an important component of system hardening
- Multiple layers of security is the best approach
- System hardening
- Vulnerability scanning and penetration testing
- Policies, Procedures, and Documentation
- End-User training
- Advanced endpoint protection to help defend against known and unknown malware
- Monitoring, alerting, and Honeypots