Cybersecurity for Emergency Managers

Alaska Spring Preparedness Conference 2019
Cybersecurity is everyone’s problem

- Cybersecurity is NOT just IT’s problem.
  - IT
  - Emergency Management
  - Law Enforcement
  - And everyone in your organization
The threat

- Malicious vs unintentional
- Active attacks
- Data breaches
- Human error
- Cyber warfare

Atlanta spending $2.7 million on ransomware cyber attack; ransom was $50,000

Updated 6:57 AM; Posted 6:43 AM

Every State Now Has a Data Breach Notification Law

BY STATELINE | APRIL 3, 2018

Baltimore's 911 system hit with cyber hack

TUE, MAR 27

For 17 hours on Saturday, Baltimore's automated 911 system was hacked and offline as dispatchers were forced to take over manual operations.

Security firm: All it took was $35 and a laptop to hack SF emergency alert system

By Bill Disbrow  Updated 3:14 pm PDT, Tuesday, April 10, 2018
THE CITY OF SAMMAMISH IS STILL IN A STATE OF EMERGENCY DUE TO THE RANSOMWARE ATTACK WE FIRST BECAME AWARE OF ON JANUARY 23, 2019.

We are committed to making sure that employees and the public are kept informed as our cross-functional team continues its work to assess what happened and how best to protect our city from not just this attack, but others we may face in the future.

While some customer applications are disabled, the City continues to operate and is open for business on behalf of our residents. City employees and residents are encouraged to visit this site regularly for updates.

FREQUENTLY ASKED QUESTIONS (FAQS)

UPDATED MARCH 4, 2019, AT 2:49 P.M.

Q. Is the City still in a state of emergency?
A. Yes; we have made some progress but will be in a state of emergency until we are completely out of this situation.
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

****@*****.com

Oh no — pwned!

Pwned on 16 breached sites and found no pastes (subscribe to search sensitive breaches)
359 pwned websites 7,840,611,051 pwned accounts 92,853 pastes 113,337,856 paste accounts

Largest breaches

<table>
<thead>
<tr>
<th>Breach</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection #1</td>
<td>772,904,991</td>
</tr>
<tr>
<td>Verifications.io</td>
<td>763,117,241</td>
</tr>
<tr>
<td>Onliner Spambot</td>
<td>711,477,622</td>
</tr>
<tr>
<td>Exploit.In</td>
<td>593,427,119</td>
</tr>
<tr>
<td>Anti Public Combo List accounts</td>
<td>457,962,538</td>
</tr>
<tr>
<td>River City Media Spam List</td>
<td>393,430,309</td>
</tr>
<tr>
<td>MySpace accounts</td>
<td>359,420,698</td>
</tr>
<tr>
<td>NetEase accounts</td>
<td>234,842,089</td>
</tr>
<tr>
<td>LinkedIn accounts</td>
<td>164,611,595</td>
</tr>
<tr>
<td>Dubsmash accounts</td>
<td>161,749,950</td>
</tr>
</tbody>
</table>

Recently added breaches

<table>
<thead>
<tr>
<th>Breach</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataCamp accounts</td>
<td>760,561</td>
</tr>
<tr>
<td>Knuddels accounts</td>
<td>808,330</td>
</tr>
<tr>
<td>Demon Forums accounts</td>
<td>52,623</td>
</tr>
<tr>
<td>Everybody Edits accounts</td>
<td>871,190</td>
</tr>
<tr>
<td>Intelimost accounts</td>
<td>3,073,409</td>
</tr>
<tr>
<td>Whitepages accounts</td>
<td>11,657,763</td>
</tr>
<tr>
<td>500px accounts</td>
<td>14,867,999</td>
</tr>
<tr>
<td>Bookmate accounts</td>
<td>3,830,916</td>
</tr>
<tr>
<td>HauteLook accounts</td>
<td>28,510,459</td>
</tr>
<tr>
<td>8fit accounts</td>
<td>15,025,407</td>
</tr>
</tbody>
</table>
Lifecycle
Prevention

• What have you done to prepare?
• What policies are in place?
• What training is in place?
• How are the policies enforced?

• THINGS YOU MUST HAVE
  • Emergency Operations Plan
  • Cybersecurity Policy
  • Acceptable Use Policy
Password Managers

The Best Password Managers

https://thewirecutter.com/reviews/best-password-managers/
Protection

VPN

2FA
TWO-FACTOR AUTHENTICATION

ANTIVIRUS
Mitigation

• What steps have you taken?
• What steps can you take?

• Insurance
• Backups
• Redundancy
• Monitoring
  • https://haveibeenpwned.com
• Early Reporting
• Training
Response

- Do you have a response plan?
- Does everybody know how to recognize an incident?
- Does your staff know what to do if they suspect an incident?
- Who do you call for help?
Recovery

What’s your recovery plan?

Who do you call for help?

Beyond just the technology
Sample Incident annex

Comprehensive Emergency Management Plan
Major Cyber Incident Annex

Primary Department
Information Technology

Support Departments/Divisions
Emergency Management
Police
All Other Departments

INTRODUCTION

1. Background

The City uses a variety of systems, services, and devices that rely upon both internal and external computer networks in order to function properly. These networks as a whole are commonly referred to as “cyberspace” and failures in them, regardless of cause, are commonly referred to as “cyber incidents”. Cyber incidents have the potential to disable city services, release non-disclosable information to unknown parties, and create public safety issues, among other things.
References

- Computer Security Incident Handling Guide (Revision 2) National Institute of Standards and Technology, 2012
Annex Parts

Policies
Sets expectations

Situation/ Assumptions
Requires all components to be in place

Concept of Operations
Will require local discussion

Responsibilities
EM/IT/LE
Expect some pushback
Major Cyber Incident Checklist

- Action items
  - Pre-Incident Phase
  - Response Phase
  - Recovery/Demob Phase

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Incident Phase</td>
<td>Develop an Incident Action Plan (<em>recurring</em>). This document is developed by the Planning Section and approved by the EOC Manager. The Incident Action Plan should be discussed at regular intervals and modified as the situation changes.</td>
</tr>
<tr>
<td>Recovery/Demob Phase</td>
<td>Implement objectives and tasks outlined in the IAP (<em>recurring</em>).</td>
</tr>
<tr>
<td></td>
<td>Coordinate with private-sector partners as needed.</td>
</tr>
</tbody>
</table>

**RECOVERY/DEMOBILIZATION PHASE**

<table>
<thead>
<tr>
<th>Action</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure an orderly demobilization of emergency operations in accordance with current demobilization and community recovery plans.</td>
<td>ICS Form 221: Demobilization Plan</td>
</tr>
<tr>
<td>Activate, if necessary, the appropriate recovery strategies, continuity of operations plans, and/or continuity of government plans.</td>
<td>Continuity of Operations/Government plans</td>
</tr>
</tbody>
</table>
Common Issues

Most entities lack a comprehensive cybersecurity policy that vests responsibility with every employee.

Those that have policies don’t enforce them.

A greater number of incidents occur than are reported in any formal way.

Lack of response plans leads to slow recognition, response, recovery.

Lack of individual security leaves entire organization at risk.
### Human Factor

<table>
<thead>
<tr>
<th>Phishing, social engineering</th>
<th>Careless info access/dissemination</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enabled by agency and employee use of social media and other things</td>
<td>• Public spaces</td>
</tr>
<tr>
<td></td>
<td>• Public wifi</td>
</tr>
<tr>
<td></td>
<td>• Unlocked computers</td>
</tr>
<tr>
<td></td>
<td>• Lack of caution</td>
</tr>
</tbody>
</table>
Social Engineering

Social Engineering

The clever manipulation of the natural human tendency to trust.
Social Media

Names

Personal details provided by third parties

Account spoofing

Operational details shared
Meet Desai
Investigators traced the calls and discovered they originated from a link posted to Twitter and YouTube. The link was to a site named "Meet Desai" and its domain was hosted out of San Francisco. When the link was clicked, it continually called 911 and would not let the caller hang up.

His page received 151,000 hits

Desai said his intent was to make a non-harmful, yet annoying, bug that was meant to be funny, officials said.
• Surprise Police Department notified the Maricopa County Sheriff’s Office of more than 100 hang-up 911 calls within a few minutes.

• The volume put authorities "in immediate danger of losing service to their switches."

• The emergency systems for the nearby Peoria Police Department and the Maricopa County Sheriff’s Office also received a large number of repeated calls.

• Agencies in California and Texas were also affected.
Meetkumar Desai, age 19, was sentenced to 3 years supervised probation for carrying out a reckless cyberattack on 911 emergency call systems in Maricopa County.

Authorities will also be able to monitor Desai’s computer while he is on probation.
Other Examples

This Photo by Unknown Author is licensed under CC BY-NC-SA
QUESTIONS?

Contact me:
Sarah Miller, MPA, CEM
President, IAEM Region 10
Past Chair, IAEM Emerging Tech Caucus
sarah@skmillerconsulting.com
twitter: @scba