Culture of Cybersecurity in America’s 911 Call Centers

Class Expectations

Networking! (2 minutes)

- Introduce Yourself, Your organization and how long they have lived at their current residence?
- Does your organization have a Cyber Security Policy?
- How often does your organization review the Cyber Security Policy with all personnel?
- Who do you report to of a Cyber breach occurs?
The former NSA chief, who also commanded the U.S. Cyber Command, warned that cyber-attacks were the greatest threats posed by jihadist terrorists.

- Keith Alexander, former National Security Agency
Public Trust and Expectations

• Answer My Call
• Send Help in a Timely Manner
• Keep My Data Secure
• Do it Right the First Time!

What is Cyber Security?

• Cybersecurity is the body of:
  • Technologies,
  • Processes,
  • Practices designed:
    • to protect networks, computers, programs and data from attack, damage or unauthorized access.

The Human Firewall
You!
The Problem

Top 7 Brutal Cyber Attacks
• #1 "Hacking Team" Data Company-Hacked by a hacker- 400 gigabytes of its internal sensitive data on the Internet.
• #2 Ashley Madison Data Breach - "Life is Short. Have an Affair"
• #3 Sony Pictures Hack
• #4 'Fappening' and 'Snappening'-Nude photos of celebrities

http://thehackernews.com/2015/09/top-cyber-attacks-1.html
• #5 Car Hacking - Jeep Cherokee, Cadillac Escalade, Toyota Prius, Dodge Viper, Audi A8

• #6 Data Breach at US Government Office of Personnel Management - 21.5 million

• #7 Anthem Health Insurance Data - 80 million people

Major Corporations that have been violated:

<table>
<thead>
<tr>
<th>Target</th>
<th>Neiman Marcus</th>
<th>Michaels</th>
<th>Yahoo! Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>(retail)</td>
<td>(retail)</td>
<td>(retail)</td>
<td>(communications)</td>
</tr>
<tr>
<td>Arron Brothers</td>
<td>AT&amp;T (communications)</td>
<td>eBay (retail)</td>
<td>Westinghouse Electric (energy and utilities),</td>
</tr>
<tr>
<td>(retail)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>United States Steel</td>
<td>Feedly (communications)</td>
<td>Evernote (technology)</td>
<td>P.F. Chang’s China Bistro (restaurant)</td>
</tr>
<tr>
<td>(industrial)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(services)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Motivations Behind Attacks November 2015

- Cyber Crime: 69.7%
- Health/Finance: 20.2%
- Cyber Espionage: 6.7%
- Cyber Warfare: 3.4%
Who—You, Me, Everybody
Where—Anywhere

• Intentionally Left Blank

Juice Jacking

• Charging Kiosk to charge your telephone-
• May access your data—passwords
### Speed of Virus

- **ILOVEYOU Virus**
  - Once the ILOVEYOU virus attachment was opened, after only one day the virus had infected more than 45 million computers.

- **Sasser Worm**
  - The Sasser Worm infected multiple sectors. In Europe, the computer security company Sophos reported that the worm hit all 19 of Britain's Coastguard control centers forcing them to go back to pen and paper.

---

### Terminology

<table>
<thead>
<tr>
<th>Exploit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephony Denial of Service (TDoS)</td>
<td>Preventing or delaying the ability to answer emergency calls by flooding the system with a volume of calls that exceeds the ability to service</td>
</tr>
<tr>
<td>Distributed Denial of Service (DDoS)</td>
<td>Placing high processing demands on the system's servers or networks rendering it unavailable</td>
</tr>
<tr>
<td>Phishing/Spearphishing</td>
<td>Sending emails that appear to come from a legitimate source such as a bank, credit card company, tricking recipient into providing sensitive personal information</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>An attempt to trick someone into revealing information that can be used to attack systems or networks</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Use of personal information of other persons, may occur in a cover of phishing, social engineering, or direct hijacking</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that makes the program malicious, operating as a surreptitious program that a user would likely install</td>
</tr>
<tr>
<td>Virus</td>
<td>A computer program that can copy itself to new computers, without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use an e-mail program to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate</td>
</tr>
<tr>
<td>Worm</td>
<td>A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread. Unlike a computer virus, a worm does not require human involvement to propagate</td>
</tr>
</tbody>
</table>

---

http://www.go-gulf.com/blog/cyber-crime/
Applications

• Keylogger- are applications that monitor a user’s keystrokes and then send this information back to the malicious user.

Apple- A Message to Our Customers

• February 16, 2016 A Message to Our Customers
• The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.
• Requesting Apple to create a “Back Door” into your iPhone.
• Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The Comm. Center

Intentionally Left Blank
January 20, 2015-Indianapolis, Indiana

Intentionally Left Blank

Comm. Center

• Telephone
  • Text.....Media.....Images.....the future
• CAD........CAD-to-CAD
• Radio Systems
• Systems......Cloud Based vs Premise Base
• Station Alerting Systems
• Primary to Secondary PSAP Transfers
• Primary/Secondary PSAP Transfers to Private Ambulance Providers
• Private Ambulance Providers Transfer to PSAPs

Comm. Center Problems

• A virus infecting at least two computers because of employee on the Internet
• A total radio outage resulting from the loss of a T1 line's connectivity, producing a chain of events that uncovered a software glitch in the trunk controllers
• A hacker entering the system and changing a hyperlink on the department’s Web site to that of an adult site's address, despite the presence of firewalls, routers and security software
• A virus on the network that targeted computers without the most recent security patches

• A virus received via e-mail from an unknown sender and another incorporated into a file
• A virus and spyware attack on a computer running the computer aided dispatch (CAD) system and numerous law enforcement software applications. This attack was the consequence of an employee using the Internet on that machine in contradiction to policy
• CAD vendor logging in remotely and transmitting a virus to the system
• Server software issues that unexpectedly rebooted the entire 9-1-1 system
• Accidental deletion of more than half of a user database by a third party administrator

What is NG911?

NG911 provides networks of networks.

• Friday, February 7, 2014 The Government Accountability Office wants the Department of Homeland Security to work with the departments of Commerce, Justice, and Transportation and the Federal Communications Commission to ensure next-generation, IP-based 911 emergency response systems are not vulnerable to cyber attack.
Call centers cannot have NG911 without cyber security

Why the NG 911’s Need for Cyber security?

- NG 911 systems rely upon IP-based technologies
- Reliance on IP exposes systems to a new, online threat environment,
- Communication through NG 911 may hide malicious threats (e.g. viruses can be embedded in texts, images, video and other files)
- NG 911 systems connect with other critical systems or devices; infecting one system may impact other integrated systems

### The Internet

- What does it provide that CAD can not?
  - Volume of DATA
- Ask the person you introduced yourself to, What is the address to the grocery store you go to?

Gas stations at Wendy and Old Conejo Road Newbury Park, Ca
Policies and Procedures

- Preventing a Breach
- Preparing for a Breach
- Dealing with a Breach
- Regrouping After a Breach

How to Protect?

- Recognize why Comm. Center cyber security is important.
- Understand how we are interdependent and interconnected (Cascading vulnerabilities).
- Distinguish between the levels of cyber security threats.
- Recognize that we are vulnerable to cyber attack and there are those who are willing to exploit those vulnerabilities.
- Describe how everyone is affected by and has a role in cybersecurity efforts.
NENA NG-SEC

- Next Generation 9-1-1 Security (NG-SEC) Audit Checklist December 14, 2011
- 102 page document with 90 pages of Audit Questions


- Provide Adequate Training to Team Members
- Use “Long and Strong” Passwords
  - Different passwords for different accounts,
  - Never use sequential numbers
- Consider Alternative Authentication Measures
- Prohibiting email attachments
- Limit Administrative Rights on Computers
- Disable USB Ports for Storage
- Get a Grip on BYOD (Bring Your Own Devices)

“Most attacks are not sophisticated and they never were because they don’t need to be.”

Rear Admiral (ret.) David Simpson, Chief of the Public Safety and Homeland Security Bureau

- Adopt cybersecurity risk management policies.
- Assess your risk. Nena self-audit-Cyber Resiliency Review
- Train your staff
- Find gaps in security and address them
- Protect your data at rest—Data backup and encrypted
Rear Admiral (ret.) David Simpson
Chief of the Public Safety and Homeland Security Bureau

- **Protect your data in motion**: Use virtual private networks to connect your servers locally and remotely.
- **Be a hard target**: A solid Identity, Credential, and Access Management (ICAM) program
- **Monitor internal communication**: Set up automated ways to analyze network and user behavior
- **Monitor external communication**: Many PSAPs engage in active social media and outreach efforts, so be sure these don’t introduce risks.

---

**What are you doing??**

---

<table>
<thead>
<tr>
<th>Technology &amp; Information</th>
<th>Types of Attacks</th>
<th>Impact</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Aided Dispatch (CAD)/911</td>
<td>Denial of Service (DoS/DDoS), Malware, viruses, trojans</td>
<td>Disruption of emergency services/communications</td>
<td>Severe risk to both public and officer safety/loss of public confidence</td>
</tr>
<tr>
<td>Land Mobile Radio (LMR)</td>
<td>DOS, Malware, jamming, physical attack on transmitters, loss, or damage due to vandalism or forces of nature</td>
<td>Disruption or loss of communications</td>
<td>Severe risk to both public and first responder safety</td>
</tr>
<tr>
<td>Records Management System (RMS)</td>
<td>Malware, trojan, keystroke logger, physical intrusion/loss or theft</td>
<td>Loss or distortion of information/evidence privacy and HIPAA</td>
<td>Threat to safety of individuals, responders, informants, etc. degradation of evidence; case/judicial impact; loss of public trust</td>
</tr>
<tr>
<td>Technology &amp; Information</td>
<td>Types of Attacks</td>
<td>Impact</td>
<td>Consequences</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>Investigative Databases</td>
<td>Malware, Trojan, keystroke logger, false credentialing</td>
<td>Loss or distortion of information/evidence</td>
<td>Threat to safety of individuals, officers, informants, etc.; degradation of evidence; case/judicial impact; privacy violations; loss of public trust</td>
</tr>
<tr>
<td>Wireless Mobile Devices</td>
<td>Malware, virus, intrusion, loss or theft</td>
<td>Loss of communications and confidential information; disruption of duties</td>
<td>Threat to responder and public safety; breach of privacy</td>
</tr>
<tr>
<td>Public Safety Information (digital and hard copy)</td>
<td>Loss or theft by both electronic and physical means</td>
<td>Personal Identifiable Information (PII) Type Infor and confident information release</td>
<td>Significant potential liability, potential violation of statutes, responder and public safety diminished; Server risk of public trust</td>
</tr>
</tbody>
</table>

Cyber Security Resources:
- The NIST Glossary of Key Information Security Terms, NISTIR 7543 Revision 2 Requirements and Transition Document

QUESTIONS

Tom Somers
tsomers@fitchassoc.com