Cyber Security

Mark Danaj – City of Fremont

ICMA Conference Presenter

Who am I?

- Why Am I Here?

- What will I accomplish?

- What can you learn from this presentation?

Cyber Security

- Why is cyber security important?
- Who is responsible for cyber security?
- What is the role of government?

Did you know:

- More than 90% of successful breaches required only the most basic techniques. [1]

- 96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls. [1]

- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching. [1]

- Outsiders were responsible for most breaches. [1]

[1]James A. Lewis, "Raising the Bar for Cybersecurity," Center for Strategic & International Studies, February 12, 2013.

ICMA

Let's take a closer look…

Planning

- Strong Policy and Governance
- Data Discovery
- Security Procedures
- Compliance
- Budget

Operational Cyber Security

Network Security Team

- Service Desk Technician (1FTE)
  - Answer phones/emails review spam
- Network Engineer (1 FTE)
  - Vulnerability Assessment (1 FTE)
  - Workstation and Servers
  - Email monitoring
- Network Engineer (1 FTE)
  - Firewall Monitoring
  - Modify network/firewall/proxy rules
  - Wireless security
- Infrastructure Services Manager (1 FTE)
  - * Incident Response, Security Architecture, Penetration Tests

Current State of Affairs

- Government Sector

What are the Problems? Solutions?

- Wireless Access
- Mobile Devices
- Cloud Computing
- Social Media

- Zero Day Malware
- Spear Phishing
- Hactivists

ICMA

Wireless Access

- Problem:
  - Wired network connections are costly, inconvenient and shrinking drastically. Wireless makes eavesdropping and unauthorized network access easier.

- Solution(s):
  - Cisco Wireless Controller
    - Intrusion Prevention
    - Access Control
  - Authentication Server
   - Cisco ASA

Mobile Devices

- Problem:
  - Exponential growth drives exponential growth in security risks and data distribution
- Solution(s):
  - Mobile Iron
    - Mobile Device Management
  - ForeScout
    - Access Control

ICMA

Cloud Computing

- Problem:
  - The cloud is better, cheaper, faster, stronger.
  - Opportunities for data theft increase.
- Solution(s):
  - Cyber security guidance
    - ISO 27001 (International Standards Organization)
    - NIST (National Institute for Standards and Technology)
  - Server certificates
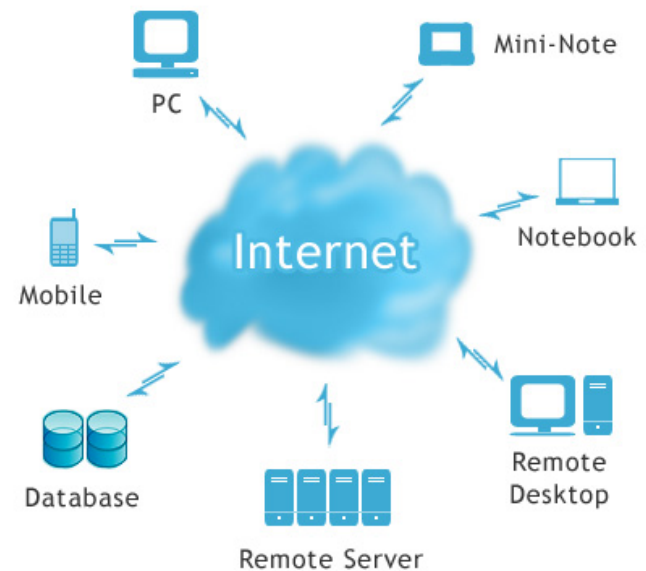
Social Media

- Problem:
  - A profile or comment on a social media platform can be used to build very targeted attacks or another avenue of attack.

- Solution(s):
  - Palo Alto Networks Firewall
    - Application Control
  - WebSense
  - Cyber Security Policy
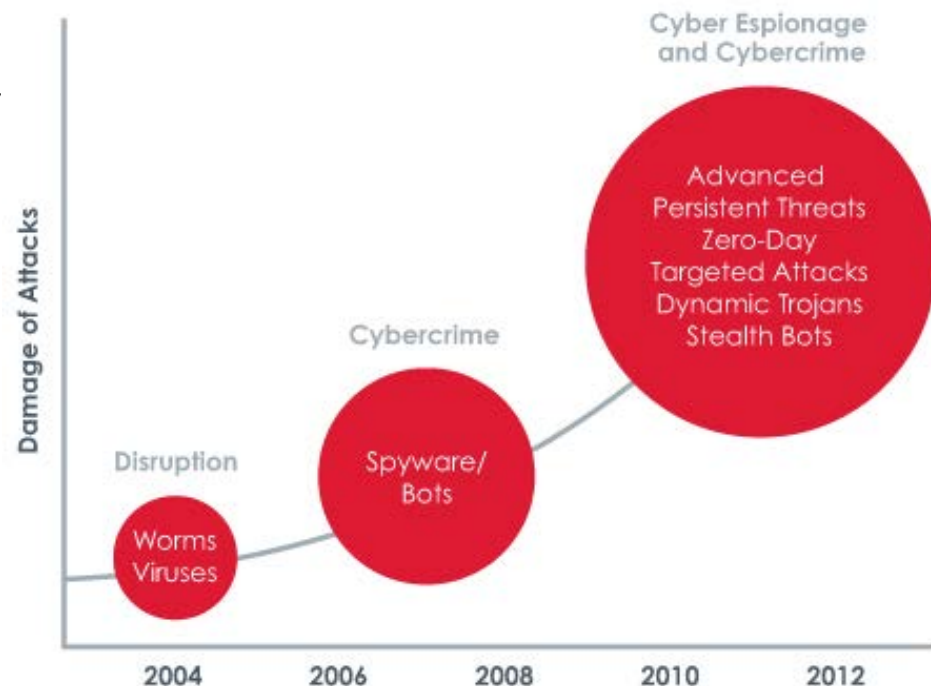   - Incidental Use / Guidance

Social Media Landscape

FredCavazza.net

ICMA

Zero Day Malware

- Problem:
  - Software developers cannot patch faster than exploits are discovered
- Solution(s):
  - Palo Alto's Intrusion/
    Detection Engine
    - Behavioral detection
  - Sophos

ICMA

Spear Phishing

- Problem:
  - Persistent adversaries lure unsuspecting users into a cyber trap with relevant sounding (but malicious) emails

- Solution(s):
  - Spam/Anti-virus Gateway
    - * Sophos
  - Internet content filter
    - * WebSense
  - User awareness training
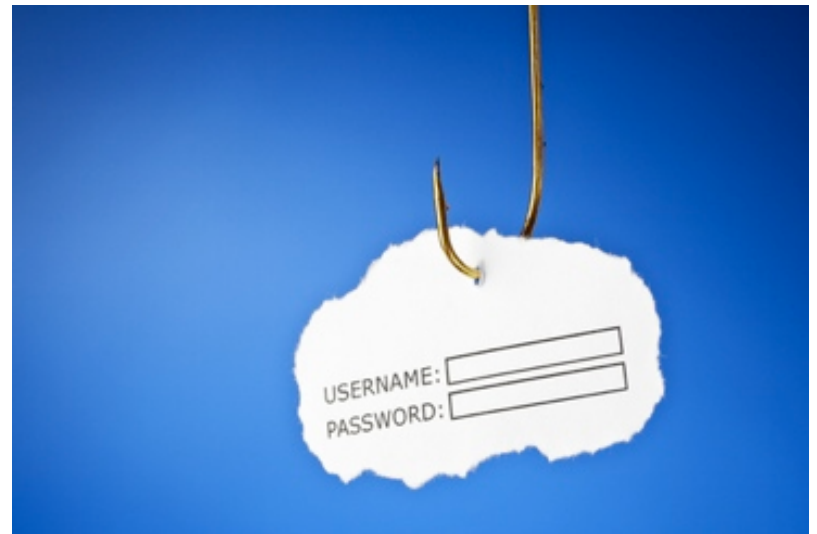
Hacktivists (latest criminal element)

- Problem:
  - The act of breaking into computer systems for politically or socially motivated purposes is on the rise.

- Solution(s):
  - Prevention
    - Palo Alto Firewall
    - ProofPoint mail gateway
  - Detection
    - Palo Alto Networks

ICMA

Future Initiatives

- Two-Factor Authentication

- Off-Site Disaster Recovery

Questions/Comments?

Additional Information…

Mark Danaj – mdanaj@fremont.gov

City of Fremont Cyber Footprint

- ## City of Fremont, CA
  - ~833 Employees
  - ~960 computers
    - Primarily a Windows environment
    - Support client and web applications
    - Intranet/Internet access
    - ~30 Thousand emails received/month
      - Roughly 60% is spam

The 10,000 foot view…

http://www.nasa.gov/vision/earth/lookingatearth/NIGHTLIGHTS.html

THE WALL STREET JOURNAL.

China's Cyber Thievery Is National Policy And Must Be Challenged
January 27, 2012
(Mike McConnell, Michael Chertoff and William Lynn)

"Evidence indicates that China intends to help build its economy by intellectual-property theft rather than by innovation and investment in research and development (two strong suits of the U.S. economy). The nature of the Chinese economy offers a powerful motive to do so."

Source: Wall Street Journal, January 27, 2012, page A15

ICMA

Attacked From Within

"I intend to seek asylum in any country that believes in freedom of expression and oppose that global privacy is being victimized."