Cyber security:
Why it matters
Agenda

• Introduction
• Understanding the threats
• Defending against the threats
• Game plan and best practices
• Q&A
Cyber security in the news

IRS Tax Fraud And Phishing Advances
New techniques and automation have bad guys making more money than ever off of unsuspecting taxpayers.
By ERICKA CHICKOWSKI Contributing Writer, Dark Reading, 3/23/2016

OPM government data breach impacted 21.5 million
By Jim Sciutto, Chief National Security Correspondent
Updated 1:15 PM ET, Fri July 10, 2015

Concerned by cyber threat, Obama seeks big increase in funding
WASHINGTON | BY DUSTIN VOLZ AND MARK HOFENBERG

Big Data privacy risks

FBI Says Threat From ‘Ransomware’ Is Expected to Grow
Law-enforcement agency sees problem of extortion by hackers worsening in 2016

DEFCON 2.0: Expert warns cyber warfare has reached critical turning point
Updated 11 Oct 2015, 10:15pm

Another Day, Another New Threat to Privacy on the Internet

Here Are 4 Vulnerabilities Ransomware Attacks Are Exploiting Now

TridiumTalk
Cyber security: Why it matters
The cost of doing nothing

$3.5 million

Average cost of ONE data breach (not including revenue losses due to lost business)

- Ponemon Institute Research Report, May 2014
Understanding the threats
Connected devices: “Hacked in minutes”

USA Today/Avantgarde Cyber Security Study:

• 6 PCs were directly connected to the Internet
• 305,922 attacks, beginning instantly
• Intruder successfully broke in within 4 minutes
• Machines w/ security patches attacked the least
• Most attacks were automated (BOTS, not live hackers)

“Unprotected PCs Can Be Hijacked in Minutes”
USA Today
Connected devices: objects of desire

- IoT: a “bright new shiny object” for hackers
  #internetOfThingsIWantToHack

- Recent publicized hacks on webcams, CCTVs, baby monitors, cars, medical devices

“If your industrial control system is connected to the Internet, it has almost a 100 percent guarantee to be hacked the first day.”

— E. Kapersky, founder, Kapersky Lab
Shodan – “Google” for hackers

EXPOSE ONLINE DEVICES.
WEBCAM. ROUTERS. POWER PLANTS. iphONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES.

TAKE A TOUR FREE SIGN UP
Attacking an Internet-facing device

1. Searches “Niagara” on Shodan

2. Tries published vulnerabilities, default passwords
   - Do you use easy-to-guess passwords?
   - Are you current with security patches?

3. Attempts to log on to device

Successful attacks result in “owning your building,” crashing your system, and/or exploring your network for more attacks
How to deter the bad guy

- Set up security gateway that acts as a VPN server
- Put your Niagara devices behind the security gateway, requiring that all remote clients establish a VPN tunnel
- Devices & systems behind security gateway are concealed from Internet discovery
- All transmissions will be encrypted
- You can remotely manage Niagara systems this way safely and securely
Defending against the threats
Advisories and updates

- Organizations such as US-CERT and ICS-CERT provide a great service (internationally), reporting vulnerabilities in hardware and software
  - Some of these affect millions of devices (e.g., 2014: Heartbleed, POODLE)

- Vendors release security patches and updates

- Remember: Hackers pay attention!
  - Very important to install security patches in a timely manner, before hackers get to you

https://www.us-cert.gov

https://ics-cert.us-cert.gov/
Security Bulletins at Tridium

- Security patches are uploaded to Niagara Central periodically – it’s critical to patch your systems.

- Check our Web site for Security Updates and Bulletins.

www.tridium.com/en/resources/library
Niagara 4 security improvements

- “Secure by default”
  - Strongest authentication mechanism
  - Enforcement of strong passwords
  - Encrypted communications (FOXS and HTTPS)
  - Force default credentials change immediately on commissioning

- Encryption of sensitive information at rest

- Signed Tridium code

- JACE 8000 secure boot

- Role-based access control
Game plan and best practices
Security best practices

1. People, processes, and technology
   Security isn’t just an “IT thing”

2. Establish important IT security policies

3. Make sure security policies are followed
   Security education is important

4. Have a response plan
   “I won’t get hacked” is not a strategy
Niagara best practices

1. **DO NOT** connect stations directly to the Internet
   - Don’t end up on Shodan (or the front page of the paper)
   - For remote access, use a VPN solution
2. Niagara 4: Use “secure by default” configurations
3. Don’t use default credentials for station or platform
4. Work closely with IT departments
5. Don’t forget about physical security
6. Keep up with Niagara security patches
7. Read our security manuals!

Thank You!

Kevin Smith
Chief Security Architect
ksmith@tridium.com

www.tridium.com/en/resources/events