

The 26th National HIPAA Summit

*The Leading Forum on Healthcare EDI, Privacy,
Confidentiality, Data Security and HIPAA Compliance*

March 29-31, 2017 • Washington, DC



IoT & DDoS Threats: *Prepared?*



Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP), CCSFP
Member (FBI) InfraGard





Agenda

- Emerging Cyber Threats
- IoT Cyber Threat
- HHS IoT Guidance



Emerging Cyber Threats

Sun Tzu, The Art of War

“If you know your enemy & you know yourself, you need not fear the result of a hundred battles.”



FORRESTER® Cybersecurity Predictions

- The talent gap will force CISOs to allocate 25 percent to external expertise & automation
- Forrester estimates that security services & automation will combine to consume 25% of security budgets in 2017
- A Fortune 1000 company will fail because of a cyber breach
- More than 500,000 IoT devices will suffer a compromise
 - Today, firms are developing IoT firmware with open source components in a rush to market; unfortunately, many are delivering these IoT solutions without good plans for updates, leaving them open to not only vulnerabilities, but vulnerabilities that security teams cannot remediate quickly

The 45th U.S. president will face a cybersecurity incident





2017 Annual Cybersecurity Report

State of Cybersecurity: Facts

- Adversaries have more tools at their disposal
- Adversaries are taking advantage of:
 - Lapses in patching & updating
 - Luring users into socially engineered traps
 - Injecting malware into supposedly legitimate online content
- 27% of connected 3rd party cloud apps introduced by employees into the enterprise posed a high security risk
- Spams account for 65% of emails; and about 10% of spam is malicious
- Adware infections lead to malware attacks; 75% of organizations are impacted by adware infections
- Vulnerabilities in middleware are becoming more apparent



2017 Annual Cybersecurity Report (Cont'd.)

Challenge for Organizations Today!

- When breaches occur, operations and finance were the functions most impacted
- Most organizations use more than five security products and more than five security vendors
- Top constraints for organizations are: Budget, product compatibility, and talent
- Organizations must contain adversaries' operational space
- Key challenge for organizations is top operationalize people, processes, and technology in an integrated manner



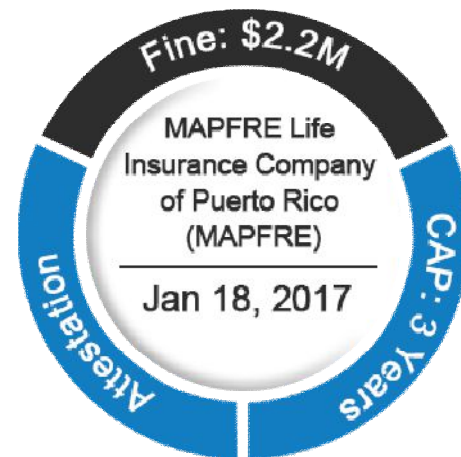
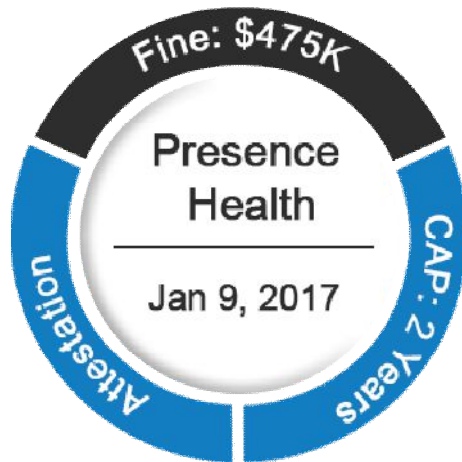
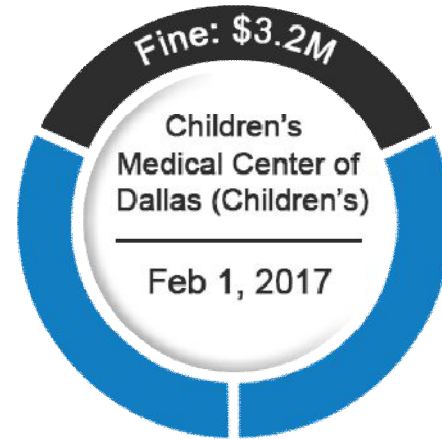
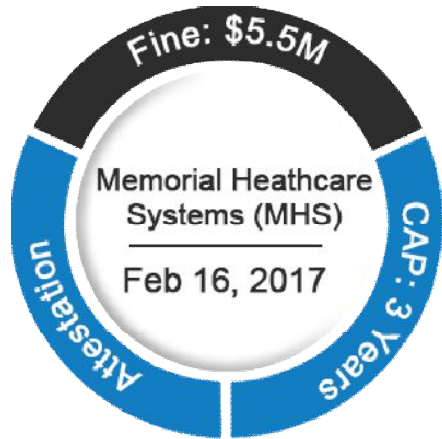
10 Largest Health Data Breaches 2016

Source: U.S. Department of Health & Human Services

Entity	Number of Affected Individuals	Type of Breach
Banner Health	3.6 million	Hacking incident
Newkirk Products	3.5 million	Hacking incident
21st Century Oncology	2.2 million	Hacking incident
Valley Anesthesiology Consultants	883,000	Hacking incident
County of Los Angeles Department of Health & Mental Health	749,000	Hacking incident
Bon Secours Health System	652,000	Unauthorized access/disclosure
Peachtree Orthopedic Clinic	531,000	Hacking incident
Radiology Regional Center	483,000	Loss
California Correctional Health Care Services	400,000	Theft
Central Ohio Urology Group	300,000	Hacking incident



HIPAA Fines 2017



IoT & DDoS Threats: Prepared?



HIPAA Fines 2016

Fine: \$650K

University of Massachusetts Amherst (UMass)

Nov 22, 2016

Attestation

CAP: 2 Years

Fine: \$2.14M

St. John Hospital (SJH)

Oct 17, 2016

Attestation

CAP: 3 Years

Fine: \$400K

Care New England Health System

Sep 23, 2016

Attestation

CAP: 2 Years

Fine: \$5.55M

Advocate Health Care Network

August 4, 2016

Attestation

CAP: 2 Years

Fine: \$2.75M

The University of Mississippi Medical Center

July 21, 2016

Attestation

CAP: 3 Years

Fine: \$2.7M

Oregon Health & Science University

July 18, 2016

Attestation

CAP: 3 Years

Fine: \$650K

Catholic Health Care Services

June 29, 2016

Attestation

CAP: 2 Years

Fine: \$2.2M

New York Presbyterian

April 21, 2016

Attestation

CAP: 2 Years

Fine: \$750K

Raleigh Orthopaedic Clinic, P.A. of North Carolina

April 20, 2016

Attestation

CAP: 2 Years

Fine: \$3.9M

Feinstein Institute for Medical Research

March 17, 2016

Attestation

CAP: 3 Years

Fine: \$1.55M

North Memorial Health Care

March 16, 2016

Attestation

CAP: 2 Years

Fine: \$25K

Complete P.T., Pool & Land Physical Therapy, Inc.

Feb 16, 2016

Attestation

CAP: 3 Years

Fine: \$239K

Lincare, Inc.

Feb 3, 2016

Attestation

CAP: 3 Years



IoT Cyber Threat

Gartner Analysis

“More than half of business processes & systems will incorporate some elements of IoT by 2020. It is estimated that compromises in IoT security will be roughly 20% of companies’ annual security budgets, up from a mere 1% in 2015.”



IoT Facts

- Today there are approximately 6.4 billion IoT devices (DVRs, surveillance cameras, & many others) all connected to the web & all with an IP address
- IoTs include smart devices like light bulbs, routers, refrigerators, washers, dryers, cameras, baby monitors, door locks, & anything else you can remotely operate from a mobile device
- By 2020, web-connected devices will increase to 20.8 billion!





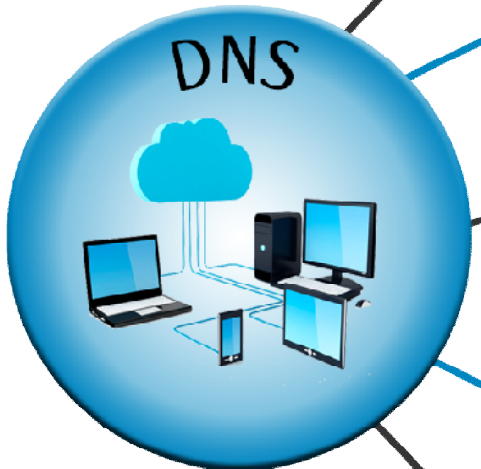
DDoS Attack Facts (Fortune, January 2017)

- No network is safe from hackers
- Hackers are getting bolder
- Average of 414,985 DDoS incidents/month in 2016
- New malware hijack IoT devices & increases DDoS threat & reach
- DDoS attack speeds ~ 800 gigabits/second in 2016

IoT & DDoS Threats: Prepared?



IoT-driven Internet Wobble on Oct 21, 2016: Why it Matters in 2017!



7:10 AM EST, Friday, October 21, 2016, witnessed a massive cyber assault on the servers



DYN is one of the handful of entities on the Internet that provides vital DNS services



The DDoS by hundreds of thousands of IoT devices on Dynamic's DNS servers made the systems inaccessible to all users



More than 500,000 IoT devices were earlier compromised by the Mirai malware



10% of compromised IoT devices were associated with the cyber-attack. zombie devices compromised by Mirai formed a botnet army led by cyber-attackers through their command and control servers



The IoT Cyber Challenge

- Hackers have learned how to take control of these devices located in homes & businesses to remotely order the devices to attack specific Internet addresses
- By controlling & coordinating tens of thousands of devices, hackers can attack a victim with data arriving at 500-1,000 gigabytes per second, overwhelming the ability of the targeted servers to deal with them & ultimately making them fail
- FDA has issued warnings concerning several medical devices that could be hacked & harm a patient. It's certainly possible that some devices could be exploited to gain further access to your network & data



How Hackers Compromise IoT

- In some cases, weak passwords were built into devices without a lot of thought. In other cases, third parties have used shared passwords to make their remote maintenance activities easier
- Some IoT devices don't come with information explaining how to change the password. Others don't provide for software updates to their devices to close security holes

Analyses have shown that if IoT devices are turned off & then restarted, the malware is typically gone – but in several cases, reinfection can occur within 30 seconds!



Walk Through the Security Challenges

- IoT fact: these devices were not designed or developed with security at their core
 - These devices are typically not configured securely

IoT = Internet of Threats!





- Focus on:
 - Walk through the security challenges associated with IoT devices, which are proliferating organizational entities
 - Key steps organizational entity should take to be better positioned to address this area of emerging cyber-risk



HHS IoT Guidance



HHS IoT Guidance

- To prevent the DDoS attacks, CEs & BAs consider:
 - ❑ Continuously monitor & scan for vulnerable & comprised IoT devices 
 - ❑ Create & implement password management policies & procedures for devices & their users 
 - ❑ Configure firewall to restrict network traffic
 - ❑ Install & maintain anti-virus software & security patches
 - ❑ Apply appropriate security controls to control access among network segments 
 - ❑ Disable Universal Plug & Play (UPnP) on routers unless absolutely necessary 



HHS IoT Guidance (Cont'd.)



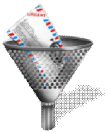
- Look for suspicious traffic on port 48101
 - ✓ Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor



- Monitor IP port 2323/TCP & port 23/TCP for attempts to gain unauthorized control over IoT devices using Telnet



- Practice & promote security awareness of IT systems capabilities, medical devices, & HVAC systems with network capabilities installed on CE & BA networks
 - ✓ If the device has open Wi-Fi connection & transmits data or can be operated remotely, it has the potential to be infected

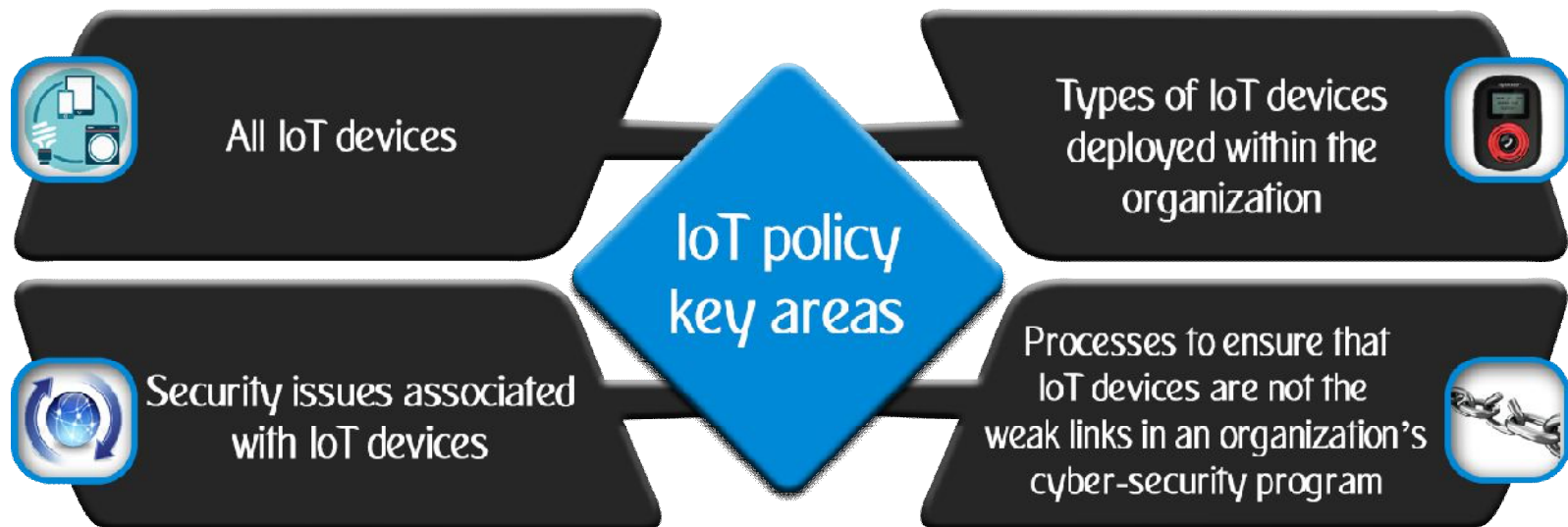


- Apply email filters to manage unwanted traffic while distributing email addresses



IoT Cyber Security Policy

- All organizations must develop an IoT cyber security policy





Key Steps for IoT Security

1

Acquisition of or immediate access to cyber security skills to lead & manage initiatives with discipline & consistency

2

Raise the cyber-security knowledge bar significantly throughout the enterprise

3

Create a credible enterprise cyber security plan that establishes the foundation for priorities & is funded appropriately

4

Conduct a comprehensive & thorough cyber security risk analysis that includes vulnerability assessment targeted at vital assets such as IoT & biomed devices



Certified HIPAA Professional

First HIPAA Training & Certification Program in the U.S Healthcare Industry!

Orlando, FL | May 23-24, 2017

Chicago, IL | Jul 18-19, 2017

Philadelphia, PA | Sep 19-20, 2017

Las Vegas, NV | Nov 28-29, 2017



Certified Security
Compliance Specialist™

First Compliance & Cyber Security Program, Globally!

Orlando, FL | May 25-26, 2017

Chicago, IL | Jul 20-21, 2017

Philadelphia, PA | Sep 21-22, 2017

Las Vegas, NV | Nov 30-Dec 1, 2017



Certified Cyber
Security ArchitectSM

An Executive Cyber Security Program

- First executive training program designed to enable development of a cyber security program in the class
- The CCSASM training validates knowledge & skill sets in cyber security with particular focus & emphasis on the development of an applicable cyber security incident response & an enterprise cyber security program

Washington, DC | Mar 29, 2017

Las Vegas, NV | May 2, 2017

Dallas, TX | May 12, 2017

Program Delivered as a Private Class Anywhere, Worldwide!

Thank You!

The 26th National HIPAA Summit

*The Leading Forum on Healthcare EDI, Privacy,
Confidentiality, Data Security and HIPAA Compliance*

March 29-31, 2017 • Washington, DC



+1.949.528.5224

Ali.Pabrai@ecfirst.com

