MEDICAL CYBERSECURITY

DO YOU KNOW WHAT'S UNKNOWN?

DISCLAIMER

- I HAVE NO FINANCIAL INTEREST ASSOCIATED WITH THIS TALK
- THIS IS A PUBLIC AWARENESS EFFORT

RAJIV SHARMA MD

FOUNDER

- DIGESTIVE HEALTH ASSOCIATES www.dhagastro.com
- DR GUT HAPPINESS www.drguthappiness.com
- EAT HEALTHY INDIANA www.eathealthyindiana.com
- CONTACT: drsharma@dhagastro.com
- CELL PHONE: 707 290 5198

PUBLIC SAFETY INFORMATION SHARING AND ANALYSIS ORGANIZATION : NON PROFIT

PUBLIC SAFETY ISAO

- info@psisao.net
- https://psisao.org
- LT COL JAMES EMERSON (FOUNDER)

- The Question here is WHEN would you get hacked and what do you do next
- Damage- Financial And Reputational

Chinese man 'marries' robot he built himself

https://www.theguardian.com/world/2017/apr/04/chinese-man-marries-robot-built-himself

NEWS FLASH: Cybercrime in General

- Cybercrime cost $600 Billion globally in 2017
- Cyberattacks cost US $57 -$109 Billion in 2016
- Public sector had 21,239 cyber incidents, 20751 targeted large organizations, 239 known breaches
- EU - punitive General Data Protection Regulation, 4% revenue penalty

Lauren Williams FCW Cybersecurity feb 21, 2018

COMMON TERMS

- Cybersecurity (information security) concepts is the protection of information and information systems from intentional or unintentional unauthorized access, use, disclosure, disruption, modification, or destruction in order to preserve their confidentiality, integrity, and availability

- Vulnerabilities may include weaknesses in technical security controls and physical security controls of a medical device, hardware, and software, as well as in implementation

- Risk is a measure of potential harm to an organization due to adverse events that might occur and the likelihood of occurrence

- Assets are things that are to be protected from compromise and include patient safety, patient privacy, and an organization’s intellectual property, including proprietary care protocols and medical device availability and integrity

COMMON TERMS

- Threats represent the potential for an attacker to violate security and cause harm to assets

- Mitigation is an act or control that reduces risk

CYBER SECURITY STATS John Mason

- In 2016, the U.S government spent a whopping $28 billion on cyber-security – and this is expected to increase in 2017 – 2018.
- According to Microsoft, the potential cost of cyber-crime to the global community is a mind-boggling $500 billion, and a data breach will cost the average company about $3.8 million.
- According to data from Juniper Research, the average cost of a data breach will exceed $150 million by 2020 — and by 2019, cybercrime will cost businesses over $2 trillion — a four-fold increase from 2015.
- Ransomware attacks increased by 36 percent in 2017.
- The average amount demanded after a ransomware attack is $1,077.
- 1 in 131 emails contains a malware.

Feb 27, 2018

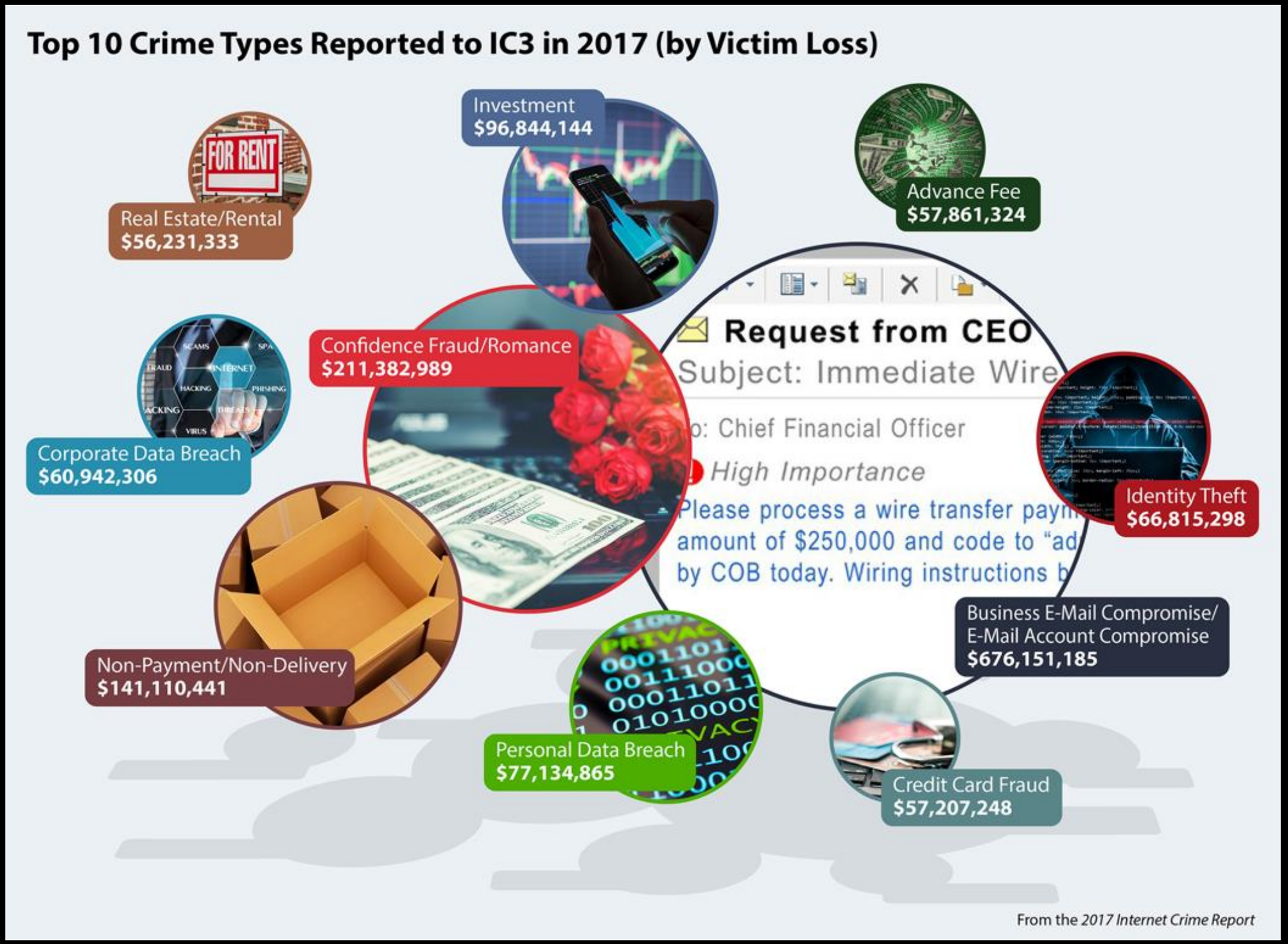
THREATS

- Hactivists (anonymous individuals) trying to cause service disruption
- Thieves intending to sell or monetize PHI, enagage in identity theft, commit financial fraud against individuals, healthcare organizations, Medicare or Medicaid
- Malicious group or people trying to target certain individuals (VIPs) or damage Healthcare Organizations' brand
- Malware that evades antivirus engines and rules and specifically doesn't attack medical devices

FBI FILES

- FBI Releases the IC3 2017 Internet Crime Report and Calls for Increased Public Awareness
- Total of 301,580 complaints with reported losses in excess of $1.4 billion. The top three crime types reported by victims in 2017 were non-payment/non-delivery, personal data breach, and phishing
- The IC3 received its 4 millionth consumer Internet crime complaint on October 12, 2017, and has received a total of 4,063,933 since its inception in 2000

FBI.GOV


Top 10 Crime Types Reported to IC3 in 2017 (by Victim Loss)
Real Estate/Rental
$56,231,333
Investment
$96,844,144
Advance Fee
$57,861,324
Request from CEO
Subject: Immediate Wire
o: Chief Financial Officer
High Importance
Please process a wire transfer payn
amount of $250,000 and code to "ad
by COB today. Wiring instructions b
Confidence Fraud/Romance
$211,382,989
Corporate Data Breach
$60,942,306
Identity Theft
$66,815,298
Non-Payment/Non-Delivery
$141,110,441
Business E-Mail Compromise/
E-Mail Account Compromise
$676,151,185
Personal Data Breach
$77,134,865
Credit Card Fraud
$57,207,248
From the 2017 Internet Crime Report

FOOD FOR THOUGHT

- In 2017, 6.5 percent of people are victims of identity fraud — resulting in fraudsters defrauding people of about $16 billion
- 43 percent of cyber attacks are aimed at small businesses
- Unfilled cyber security jobs are expected to reach 3.5 million by 2021 — compared to about 1 million in 2016
- According to billionaire investor Warren Buffett, cyber attacks is the BIGGEST threat to mankind — even more of a bigger threat than nuclear weapons
- 230,000 new malware samples are produced every day — and this is predicted to only keep growing
- China is the country with the highest number of malware-infected computers in the world
- * John Mason CyberSecurity Statistics

FOOD FOR THOUGHT

- More than 4,000 ransomware attacks occur every day.
- 78 percent of people claim to know the risks that come with clicking unknown links in emails and yet still click these links.
- 90 percent of hackers cover their tracks by using encryption.
- It takes most business about 197 days to detect a breach on their network.
- Android is the second most targeted platform by hackers after Windows.
- 81 percent of data breach victims do not have a system in place to self-detect data breaches.
- 95 percent of Americans are concerned about how companies use their data.
- * John Mason CyberSecurity Statistics

- The two most important reason people use VPNs is to browse anonymously and to unlock better entertainment content: 31 percent of people use VPNs mainly to browse anonymously, while 30 percent of people use VPNs to unlock content

- 42 percent of VPN users use a VPN at least 4 to 5 times a week — with most of them using it every day

WHY SHOULD I CARE?

Cyber Concern Survey

- 83% of 1,300 physician practices surveyed already have experienced a cyberattack—increasing the need to better support medical practices; https://www.ama-assn.org/about/medical-cybersecurity-patient-safety-issue
- 79 Percent of Healthcare Pros Concerned About Cybersecurity of Personal Data. Venafi, HIMSS 2018
- 79 percent of respondents believe government-mandated backdoors into encryption technology could harm the privacy and personal information of patients. Venafi, HIMSS 2018
- 87 percent of respondents are concerned that the reliability and availability of critical healthcare infrastructure could be compromised by cyber attacks. Venafi, HIMSS 2018

COST OF DATA BREACH STUDY : 15
Countries/Regions * Not specific to Healthcare

- IBM Security and Ponemon Institute
- 2200 IT, data & compliance professionals from 477 companies breached over past 12 months
- Average total cost of a data breach: $3.86 Million
- Average cost per lost or stolen record $148
- Mean time to identify : 197 days
- Mean time to contain: 69 days

Companies that contained breach less than 30 days saved over $1 million vs those who took more than 30 days to resolve

SECURITY AUTOMATION AND EXTENSIVE USE OF INTERNET OF THINGS (IoT) DEVICES [TWO NEW COST FACTORS]

- Average cost of a breach for organizations that fully deploy security automation $2.28 Million
- Without automation, estimated cost $4.43 Million, a $1.55 Million net cost difference
- Extensive use of IoT devices increased cost by $5 per compromised record
- Mega breach of 1 Million records yields average cost of $40 Million
- Mega breach of 50 Million yields an average total cost of $350 Million

2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW. Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC

IOT HEALTH

- Recent research from Accenture found that the Internet of Health Things (IoHT) is delivering tangible cost savings, but continuous investment is essential
- By introducing more connectivity, remote monitoring and information gathering, IoHT can encourage better use of healthcare resources, more informed decisions, a reduction in inefficiencies or waste and the empowerment of health consumers
- Estimates from the report show that the value of IoHT will top $163 billion by 2020, with a Compound Annual Growth Rate (CAGR) of 38.1 percent between 2015 and 2020

READ MORE: Prioritizing Data Security Strategies for Health IT Infrastructure

HIPAA SECURITY GUIDELINES

- HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

HIPAA & HITECH

- 2 PATIENT PRIVACY ACTS: HIPAA (1996) and the Health Information Technology for Economic and Clinical Health Act (HITECH, 2009)
- HITECH Expanded HIPAA's rules, increasing the potential legal liability for non-compliance and providing more enforcement actions
- Civil monetary penalties issued by OCR for HIPAA violations can reach up to $50,000 per violation, with an annual maximum of $1.5 million. The U.S. Justice Department may impose fines up to $250,000 and imprisonment up to 10 years for HIPAA violations, depending on the circumstances of the breach.

HIPAA through the years: 5 biggest fines since 2008- JULIE SPITZER, Becker’s Healthcare Review

- Memorial Healthcare System in Hollywood, Fla., paid $5.5 million in 2017 to settle allegations that employees inappropriately disclosed 115,143 individuals' data to affiliated physician office staff

- Advocate Health Care Network agreed to pay $5.5 million in 2016 after an investigation showed it failed to protect patient data, which led to the loss of 4 million patients' information in 2013

- NewYork-Presbyterian Hospital and Columbia University, both based in New York City, paid

- June 2018,University of Texas MD Anderson Cancer Center in Houston was ordered to pay $4.3 million in civil penalties for HIPAA violations related to the organization's encryption policies

- Temple Hills, Md.-based Cignet Health paid $4.3 million in 2011 to settle claims it violated 41 patients' rights by denying them

Health Care Industry Cybersecurity Task Force- EST. 3/2016, Cybersecurity act of 2015

- To meet its charge under the Cybersecurity Act and improve cybersecurity practices in the health care industry, the Task Force members held four in-person meetings which were open to the public (public summaries are archived on this site for public review), as well as additional virtual meetings to address the following five (5) requirements of the Act:

- analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries

- analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks

- review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record

- provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry

- establish a plan for implementing title I of this division, so that the Federal Government and health care industry stakeholders may in real time share actionable cyber threat indicators and defensive measures

https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx

The Task Force members represented a wide variety of organizations within the health care and public health sector, including hospitals,

Remember Garcia?

- https://youtu.be/nD7XQ1yjgB0

https://youtu.be/nD7XQ1yjgB0

- **In the June 2013 Safety Communication on cybersecurity for medical devices and hospital networks, the FDA observed that it has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices).**

FBI WARNING 2014

- Health companies have been viewed in recent years as lagging in computer security compared to financial institutions and retail operations
- In 2014, the FBI issued a warning to health companies that stronger computer security would be needed to deter hacking

HEALTHCARE INDUSTRY IS CYBER GOLD MINE

- Trusting nature of victims
- Lack of computer savviness
- No place to really report & understand the depth of damage
- Digitalization of Health care
- Medical Data is deep wholesome data

HEALTHCARE INDUSTRY IS CYBER GOLD MINE

- ELECTRONIC MEDICAL RECORDS
- MOBILE APPS
- REMOTE ACCESS MONITORING
- MEANINGFUL USE, PATIENT PORTALS
- MEDICAL DEVICES, PACEMAKERS
- TELEMEDICINE

MOBILE HEALTH APPS

Mobile apps are software programs that run on smartphones and other mobile communication devices

They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software

Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device

VISIT:
https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm

MOBILE HEALTH APPS

- 325,000 MOBILE HEALTH APPS IN 2017 per -Google Play store is shopping center for Healthcare App
*https://research2guidance.com/325000-mobile-health-apps-available-in-2017/
- Manage health and wellness, easy access, portability

MOBILE HEALTH APPS

- NIH’S - LACTMED app targeting nursing mothers
- The Radiation Emergency Medical Management (REMM) app targeting healthcare providers
- Diagnose cancer
- Cardiac rhythm issues

MOBILE MEDICAL APPLICATION : FDA REGULATION

The FDA is taking a tailored, risk-based approach that focuses on the small subset of mobile apps that meet the regulatory definition of "device" and that:

- are intended to be used as an accessory to a regulated medical device, or
- transform a mobile platform into a regulated medical device.
- Mobile apps that transform a mobile platform into a regulated medical device and therefore are mobile medical apps: These mobile apps use a mobile platform's built-in features such as light, vibrations, camera, or other similar sources to perform medical device functions (e.g., mobile medical apps that are used by a licensed practitioner to diagnose or treat a disease). Possible product codes: Varies depending on the intended use and function of the mobile medical app; see additional examples below.
- Mobile apps that use a sensor or lead that is connected to a mobile platform to measure and display the electrical signal produced by the heart (electrocardiograph or ECG). Possible product code(s): DPS, MLC, OEY (21 CFR 870.2340), MLO, MWJ (21 CFR 870.2800).

Mobile apps span a wide range of health functions.

While many mobile apps carry minimal risk, those that can pose a greater risk to patients will require FDA review.

LINK : https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368741.htm

https://www.fda.gov/MedicalDevices/DigitalHea

Does the FDA regulate mobile devices and mobile app stores?

FDA's mobile medical apps policy does not regulate the sale or general consumer use of smartphones or tablets

FDA's mobile medical apps policy does not consider entities that exclusively distribute mobile apps, such as the owners and operators of the "iTunes App store" or the "Google Play store," to be medical device manufacturers

FDA's mobile medical apps policy does not consider mobile platform manufacturers to be medical device manufacturers just because their mobile platform could be used to run a mobile medical app regulated by FDA

Does the guidance apply to electronic health records?

- FDA’s mobile medical app policy does not apply to mobile apps that function as an electronic health record (EHR) system or personal health record system

HUNGRY FOR MORE INFORMATION?

- digitalhealth@fda.hhs.gov
- https://www.fda.gov/MedicalDevices/DigitalHealth/default.htm
- https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

Healthcare IT News

- 8 out of 10 mobile health apps open to HIPAA violations, hacking, data theft
- Most health apps are susceptible to code tampering and reverse-engineering, two of the most common hacking techniques, the report found
- Majority of executives surveyed by said they believe their apps are secure
- Survey placed special emphasis on mobile health apps, was based on analysis of 126 popular health and finance apps from the United States, United Kingdom, Germany and Japan

https://www.healthcareitnews.com/news/8-out-10-mobile-health-apps-open-hipaa-violations-hacking-data-theft

EASY TARGETS

- Outdated IT systems are pivot points for cybercriminals, lack of uptodate security

RECENT HEALTH CARE CYBER ATTACKS

- Data breach at New York ASC possibly exposes 135,000 patient records (HHS.GOV, TIMESUNION)
- ANTHEM 2015, 80 MILLION HACKED, SETTLED 115 MILLION DOLLARS
- Newkirk Products 3.4 million August 2016
- Emblem Health-GHI 81,122 November 2016
- Elderplan Inc 22,000 August 2017
- MetroPlus Health Plan 15,212 September 2017
- Shop-Rite Supermarkets 12,172, NOVEMEBER 2017
- Pediatric Healthcare Solutions 6,932 June 2017

Centers Plan for Health Living 4.3F3 March 2017

- https://www.timesunion.com/business/article/Hackers-hit-patient-records-at-St-Peter-s-center-12723418.php

- Attacks on medical devices running on Outdated software that lack adequate security updates
- Conficker a computer worm (2008- 2009) that affected early version of MS can still infect outdated healthcare systems, per Alex Wirth, Healthcare solutions architect with Symantec, 2017 HIMSS.

TARGETS: What devices can be hacked?

- PET CT, Infusion Pumps, Medical Lasers, Ventilators, Dialysis Machines
- Pacemakers, AICD
- X RAY machines
- Central monitoring stations

Hollywood is Aware!

- In a December 2012 episode of the popular television series *Homeland*, the Vice President of the United States was assassinated when a terrorist organization wirelessly hacked his pacemaker

TV CAN KILL YOU

- In 1998, low-power heart monitors at a hospital were overwhelmed with electromagnetic interference and unable to provide critical care readings when a nearby TV station turned on
a new digital television transmitter using a previously vacant TV channel

RANSOMWARE

- Rising in number, 1000 per day 2015 to 4000 per day 2016
- Hack- Encrypt- Demand money to Decrypt

LEGACY APPLICATIONS Spawning Ground

- Many are holdovers from the last PACS or IT upgrade, according to Jamie Clifton, director of product management at BridgeHead Software
- Installers of the more efficient IT systems are either unable or unwilling to bring all the data into the new equipment, Clifton told Imaging Technology News (ITN) in an interview at HIMSS 2017
- Each time you do an EMR migration, a vast number of legacy applications are generated

COMPLICATED INTERFACE

- The interfaces often become so complicated that, when problems occur, the IT staff has trouble finding the root causes. That can be a nightmare from a cybersecurity perspective
- If you have black holes in the system you will NOT be able to tell when you got cyberattacked
- Healthcare providers should sack legacy applications as soon as possible, according to a leading expert
- A lot of healthcare organizations not paying attention to this

CLOUDS OF DANGER

- We all love Cloud (when we remember our passwords)- share, save cost, efficient
- Its any cybercriminal’s mid summer night’s dream
- Hybrid system- cloud and on site data storage can be beneficial if you get attacked

Hacker group Orangeworm attacks long-standing vulnerabilities in healthcare imaging devices, by EVAN SWEENEY. https://www.fiercehealthcare.com/tech/hacker-orangeworm-imaging-legacy-devices-cybersecurity

ENTERPRISE VULNERABILITIES

- Per FDA “networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. This vulnerability increases as medical devices are increasingly connected to the internet, hospital networks and to other medical devices”.

- Patient Portal Attacks against a patient portal might come if a patient accesses medical records while on a public network eg Starbucks.

- Denial of service attacks against patient portals can unleash attack by millions of “bots” that can cripple the portal, EMR and IT system.

NETWORKED MEDICAL DEVICES: Double edged swords

- Networked medical devices and other mobile health (mHealth) technologies are a double-edged weapon
- They can play transformational role in health care but also may be a vehicle that exposes patients and health care organizations to safety and security risks
- Among the unintended consequences of health care's digitization and increased networked connectivity are the risks of being hacked, being infected with malware, and being vulnerable to unauthorized access

NETWORKED MEDICAL DEVICES

Potential risks

- Electromagnetic interference
- Untested or defective software and ransomware
- Theft or loss of networked medical devices (external or portable) Security and privacy vulnerabilities
- Failure to install timely manufacturer security software updates and patches to medical devices and concerns about causing service disruptions to functional devices
- Improper disposal of patient data or information, including test
- Uncontrolled distribution of passwords, such as employee carelessness in leaving a password unattended in public,disabled passwords, or hard-coded passwords for software intended for privileged medical device access (e.g., to administrative, technical, and maintenance personnel)
- Network transfer (via email, remote access channel)

NETWORKED MEDICAL DEVICES: Potential risks

- spearphishing attacks
- unauthorized device setting changes, reprogramming, infection via malware
- denial of service attacks (DoS)
- targeting mobile health devices using wireless technology to access patient data , monitoring systems and implanted medical devices

- For Questions about Medical Device Reporting, including interpretation of MDR policy:
- Call: (301) 796-6670
- Email: MDRPolicy@fda.hhs.gov
- Or write to:

Food and Drug Administration

Center for Devices and Radiological Health

MDR Policy Branch

10903 New Hampshire Avenue

WO Bldg. 66, Room 3217

Silver Spring, MD 20993-0002

What to do

- https://www.phe.gov/Preparedness/planning/CyberTF/Documents/hccs-tf-resource-catalog.pdf

Health Care Industry Cybersecurity Task Force- EST. 3/2016, Cybersecurity act of 2015

- To meet its charge under the Cybersecurity Act and improve cybersecurity practices in the health care industry, the Task Force members held four in-person meetings which were open to the public (public summaries are archived on this site for public review), as well as additional virtual meetings to address the following five (5) requirements of the Act:

- analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries

- analyze challenges and barriers private entities (notwithstanding section 102(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks

- review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record

- provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry

- establish a plan for implementing title I of this division, so that the Federal Government and health care industry stakeholders may in real time share actionable cyber threat indicators and defensive measures

https://www.phe.gov/preparedness/planning/CyberTF/Pages/default.aspx

The Task Force members represented a wide variety of organizations within the health care and public health sector, including hospitals,

HOW TO BE CYBER READY

- Back up the computers and servers so that replacement data is available if hacked
- Secure mapped network drives with password and controls
- Download the latest patches, plug ins for the OS
- Email security to protect against spam email

HOW TO BE CYBER READY

- Frequent audits to identify gaps and vulnerabilities
- Policies and procedures
- The Electronic Healthcare Network Accreditation Commission (EHNAC) offers such services to vendors who then assist customers

HOW TO BE CYBER READY

- Isolate the infected computer
- Replace encrypted files with good back up files
- Do not pay ransom. Remember they are bad guys. They will reinvest their profits- Symantec 2017 HIMSS

HOW TO BE CYBER READY

- Perform regular penetration testing: Like the Pentagon, Federal reserve

Roll up your sleeves

- Identify risk and assets
- Protect; training & educating staff and install protective technology
- Monitor & Survey assets for early detection
- Plan to mitigate the effects of attack
- Plan to recover from the attack

TEAM EFFORT

- It appears that much more can be done within provider organizations to increase awareness among stakeholders – physicians, Chief Medical Information Officers (CMIOs), CIOs, and clinical engineering teams – about current

and potential medical device threats and vulnerabilities. Educating these stakeholders may increase their support for appropriate cybersecurity capabilities in devices being considered for procurement.

Average patient: 15 health tech devices

- “Depending on the statistics provider, the average patient in a hospital bed has between 10-15 health tech devices,” Terry Ray, chief technology officer at Imperva, said in an email. “Unfortunately, most of these are legacy devices which have very little, if any, security controls in place.”

- Healthcare providers can take several measures to protect their network and limit the scope of an attack by ensuring malware signatures and antivirus programs are up-to-date

- Segmenting the hospital network to isolate vulnerable devices can prevent a larger attack

PUBLIC SAFETY EMERGENCY

- **Cybersecurity is a patient safety issue.** Cybersecurity must not be viewed only as a technical issue. Stakeholders from health IT, health systems and the federal government have to come together to protect patients' health information.

- **Physician practices rely on health IT vendors for network and system security.** Most practices do not have internal security support and must sort through a lot of information to find trusted vendors. The AMA wants to ensure physicians understand good cyber hygiene and is partnering with organizations like HITRUST to offer workshops and resources on good cyber hygiene to assist small and mid-sized practices.

- **HIPAA compliance is not enough to protect patient records.** Of the physicians surveyed, 85% believe it is crucial to share electronic data outside of their health system for quality care but want to do it safely. They need ways to provide secure electronic protected health information.

https://www.ama-assn.org/about/medical-cybersecurity-patient-safety-issue

- NEED GOOD CYBER HYGIENCE

TEAM EFFORT

- It appears that much more can be done within provider organizations to increase awareness among stakeholders – physicians, Chief Medical Information Officers (CMIOs), CIOs, and clinical engineering teams – about current and potential medical device threats and vulnerabilities.
- Educating these stakeholders may increase their support for appropriate cybersecurity capabilities in devices being considered for procurement.

SOS

- FBI
- https://www.ic3.gov/default.aspx

Resource Catalog

- HealthIT.gov Cybersecurity: HHS ONC has developed resources for Healthcare cybersecurity and risk management
- HHS Office of the Assistant Secretary for Preparedness and Response (ASPR): TRACIE - Technical Resources, Assistance Center, and Information Exchange to help regional ASPR staff, healthcare coalitions,health care entities and more

- DHS: https://www.dhs.gov/topic/cybersecurity
- NIST: https://www.nist.gov/topics/cybersecurity
- Healthcare and Public Health (HPH) Sector Critical Infrastructure Protection Partnership: HHS/ASPR's Critical Infrastructure Protection Program leads a public and private sector partnership to protect the HPH Sector from all hazards, including cyber threats

- HITRUST: https://hitrustalliance.net
- NH-ISAC: The NH-ISAC is the official ISAC for the HPH sector https://nhisac.org
- InfraGard is a partnership between the FBI and the private sector dedicated to sharing information and intelligence to counter threats. https://www.infragard.org
- U.S. Computer Emergency Readiness Team (US-CERT : https://www.us-cert.gov
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) : https://ics-cert.us-cert.gov
- https://www.dhs.gov/topic/cybersecurity-information-sharing

- For Health Care Providers – EHRs
  HIPAA Security Rule: OCR provides a summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

- ONC Security and Privacy Guide: ONC, in coordination with OCR, created a guide to privacy and security of electronic health information, along with a Security Risk Assessment Tool. https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

- OCR Security Rule: OCR created a collection of resources on the HIPAA Security Rule, including guidance for implementing the security standards, risk analysis, pointers to key NIST documents, and OCR Awareness Newsletters on vulnerabilities and threats.
  https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

- Cybersecurity Center of Excellence (NCCoE): One of the NCCoE health IT projects is related to EHRs on mobile devices.
  https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices

- NCCoE: One of the NCCoE health IT projects is related to wireless infusion pumps.
- https://www.nccoe.nist.gov/projects/use-cases/medical-devices

ARE YOU CYBER READY?