County of San Luis Obispo Public Health Department
Disaster Healthcare Coalition (DHCC) Meeting
April 4, 2019

In attendance: Chris Anderson, Joni Anderson, Dave Blanchard, Kerry Boyle, Robin Hendry, Emma Lauriston, Ann McDowell, Elizabeth Merson, Alex Natham, Susan Noone, Nate Paul, Michelle Pinney, Jorge Rodriguez, Tim Rohan, Eric Ruelas, Mary Jean Sage, Paula Smith, Patti Shay-Dagenais, Jeanette Tosh, Denise Yi

Please email corrections to Michelle Pinney: mpinney@co.slo.ca.us

Call to Order	Meeting began at 10:30 with a welcome from Elizabeth Merson and introductions.
TOPIC	**DISCUSSION**
AGENDA ITEMS	
ROBIN HENDRY CYBER SECURITY PRESENTATION	• Healthcare organizations are at risk of cyber-attacks, particularly to gain access to medical records and patient information, See full presentation at the end of minutes. • Discussion from group: • Medical records are more valuable to hackers because they can be used to create patient profiles and access bank records. Cyber attackers can also hold medical company's information ransom and receive huge sums. FBI encourages companies not to pay ransoms because it promotes future attacks and there is no guarantee that the attackers will give the information back, however, organizations often pay the ransom because the ransom is less than the loss of revenue caused by not getting the records back. • Healthcare systems are working actively working to mitigate their threats to cyberattacks as it has become a priority to improve cybersecurity.
ELIZABETH MERSON SAN BERNADINO COUNTY TERRORIST ATTACK LEGACY REPORT	• San Bernardino County Terrorist Attack Legacy Report highlights many lessons learned from SB county's experience. The after action report focuses on preparedness, response and recovery issues for other organizations to consider within 8 categories: Emergency Protocols, Operational Response, Communication, Employee Support, Continuity of Operations and Organizational & Financial Recovery • The full report can be found online: http://www.sbcounty.gov/uploads/CAO/reports/December2LegacyDocument.pdf

Disaster Healthcare Coalition Meeting Minutes 1/03/2019

Elizabeth Merson Public Health Emergency Preparedness Program Report	• This is National Public Health Week and SLO Public Health will have various exhibits at Farmers Market on Morro Street to show case Public Health programs. • SLO EMS Division is collaborating with Ventura and Santa Barbara Counties to cross train staff to provide mutual aid support to each other's EOCs and DOCs during disasters. • PHEP is in the process of revising several plans: CHEMACK (revision complete and will be distributed soon), Point of Distribution SOPs, Pan Flu Plan and Communicable Disease Response Plan.
Denise Yi Medical Reserve Corps& Healthcare coalition sub committees	*Medical Reserve Corps* • SLO MRC is made up of volunteer healthcare professionals and auxiliary staff trained to respond with and assist local emergency responders and public health professionals. SLO MRC provides an organized group for healthcare professionals to efficiently volunteer their expertise to fulfill crucial staff needs in large-scale emergencies. Please share the attached flyer with anyone who may be interested in joining the SLO MRC. *Coalition Surge Test Exercise* • The 2nd annual Coalition Surge Test Exercise will take place on Friday May 10th. This exercise is a new requirement to test a healthcare coalition's ability to quickly evacuate 20% of a participating coalition's staffed beds. All 4 hospitals in SLO County along with members from the Healthcare Preparedness Work Group will participate in May.
Ann McDowell Epidemiologist	• Flu H3N2 now circulating which is particularly dangerous for really young, elderly. Flu activity should hopefully die down by the end of April. • Oct/Nov is prime time to get flu shot for maximum protection for oncoming flu season, which generally occurs December-February.
Jorge Rodriguez OES Representative	• Emergency Worker Decontamination Exercise – FEMA report due to OES within 90 of exercise date • Joe Guzzardi is new OES manager – came from Santa Clara County OES and was with Santa Barbara County OEM prior to that • Our next exercise is a Medical Exercise at French Hospital – August 2019 – Will evaluate the hospital's capability to decon a worker from diablo who is contaminated with radiation – will also demonstrate capability to monitor and decon a person who is potentially contaminated after being in an area that could be contaminated by a radiological release.
Partner Reports	**N/A**
Next Meeting	Thursday, July 11, 2019 at 10:30 am CHP Coastal Division, 4115 Broad St #B-10, San Luis Obispo, CA 93401
Adjourn	The meeting adjourned at 12:02 p.m.

COUNTY OF SAN LUIS OBISPO

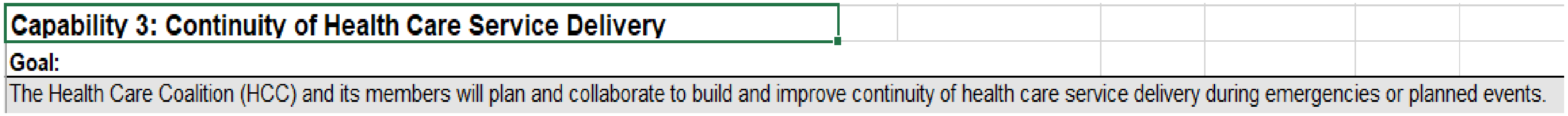
www.slocounty.ca.gov

Cyber Security Best Practices in the Healthcare Industry
DHCC Meeting April 4, 2019

"I'm no expert, but I think it's some kind of cyber attack!"

Background

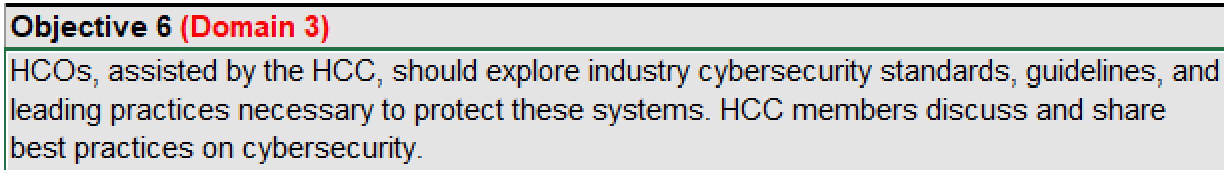
2018 – 2019 Hospital Preparedness Program Grant Requirement



Capability 3: Continuity of Health Care Service Delivery

Goal:

The Health Care Coalition (HCC) and its members will plan and collaborate to build and improve continuity of health care service delivery during emergencies or planned events.



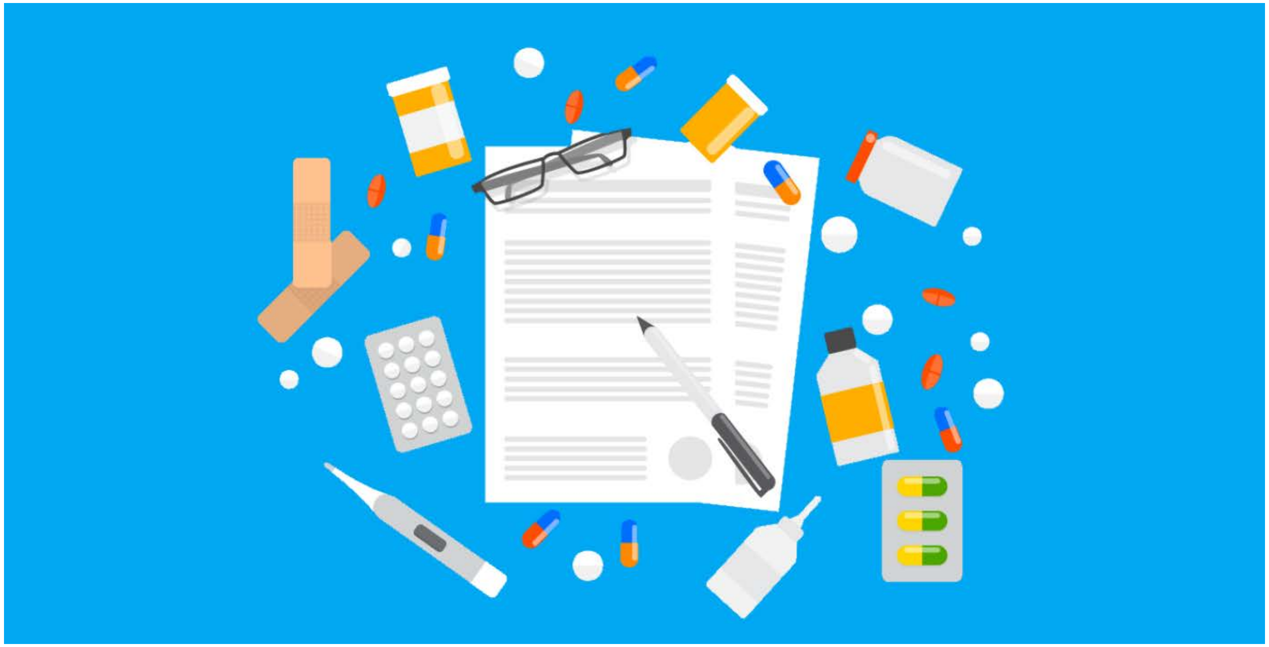
Objective 6 (Domain 3)

HCOs, assisted by the HCC, should explore industry cybersecurity standards, guidelines, and leading practices necessary to protect these systems. HCC members discuss and share best practices on cybersecurity.

By 2020 there will be roughly 200 billion connected devices

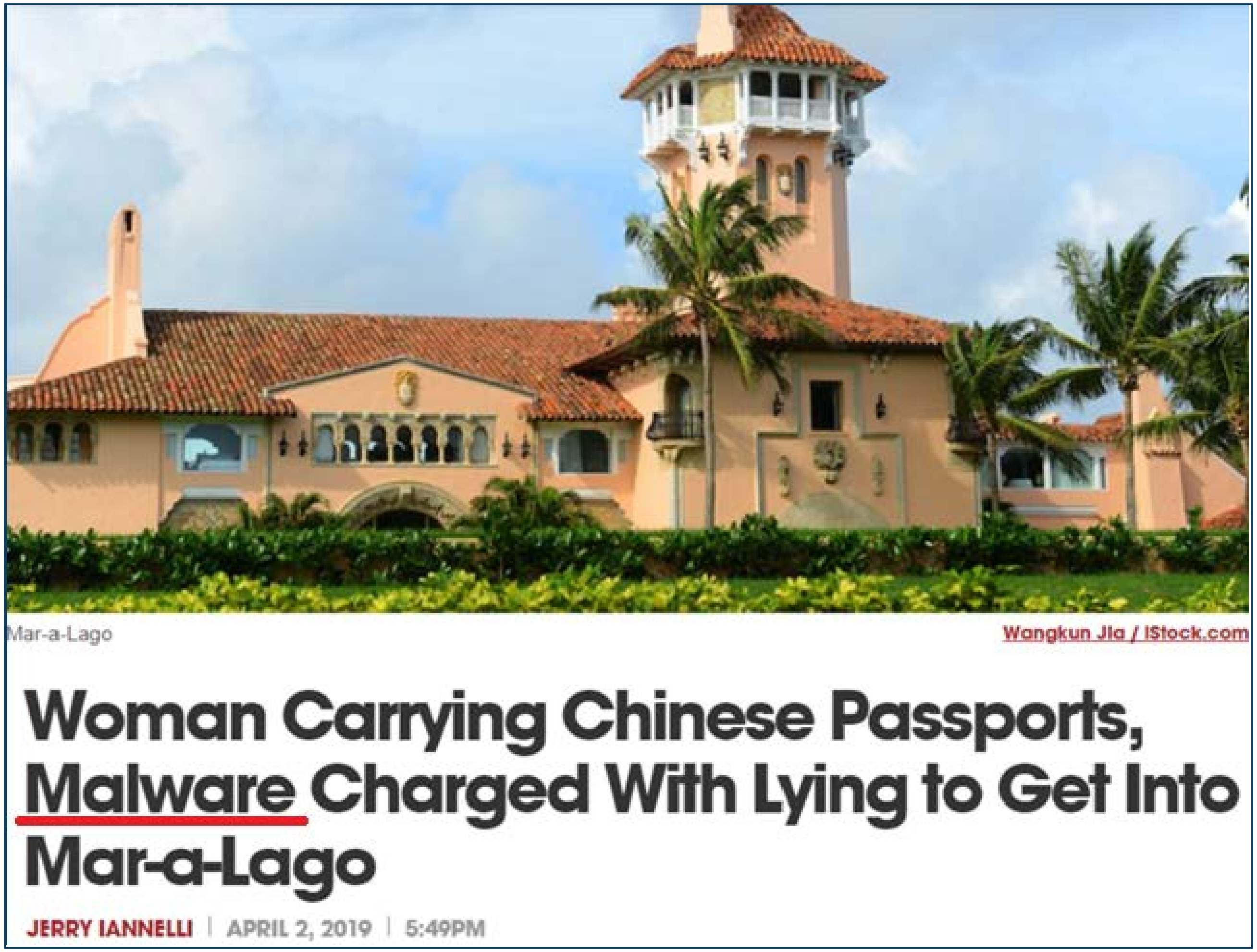
- Technological advancements in health care continue to save lives.
- However, increased use and dependence on information technologies such as electronic health records and connected medical devices potentially puts sensitive patient data at risk.
- Healthcare organizations, including medical insurance, labs, providers and pharma are becoming much more popular targets for hackers.
- Hospitals spend 64% MORE on advertising after a data breach
- The value of medical records on the darknet is higher than that of passwords and credit cards

Over 75% of health care industry has been infected with malware over last year



Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Straight from the Headlines!



Mar-a-Lago

Wangkun Jia / iStock.com

Woman Carrying Chinese Passports, Malware Charged With Lying to Get Into Mar-a-Lago

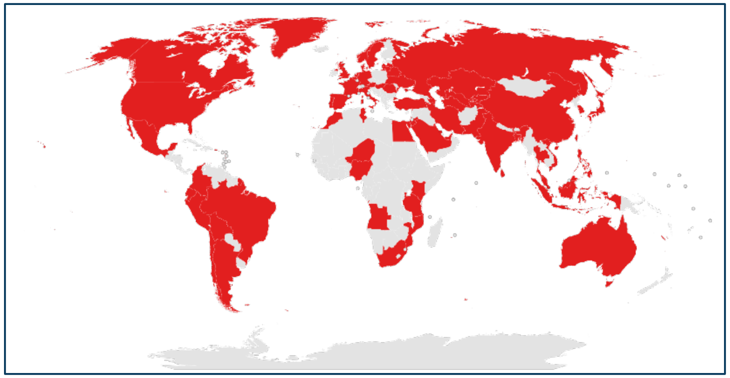
JERRY IANNELLI | APRIL 2, 2019 | 5:49PM

Healthcare Cyberattacks Cost $1.4 Million on Average in Recovery

The cost is directly tied to a loss of productivity, reputation damage, and service disruption, among other business impacts.

REAL LIFE EXAMPLE

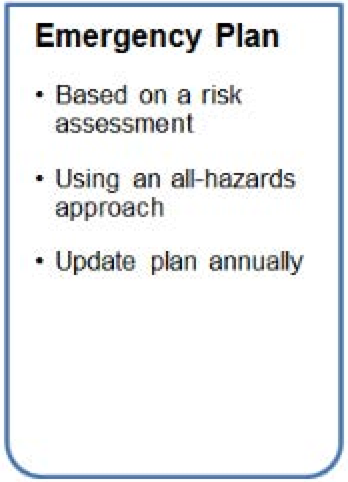
- The 2017 WannaCry Ransomware cyberattack disrupted over 200,000 computers in more than 150 countries.



Encrypted data and demanded ransom payments in the Bitcoin cryptocurrency.

- One of the largest agencies affected was the National Health Service with hospitals in England and Scotland, impairing 70,000 devices including computers, MRI scanners, blood storage refrigerators, and surgery theatre equipment.
- The WannaCry cyberattack caused some services to turn away non-critical emergencies

On a positive note: “At 82%, healthcare leads industries that have an emergency response plan in place” according to a recent report from Radware.



Emergency Plan

- Based on a risk assessment
- Using an all-hazards approach
- Update plan annually

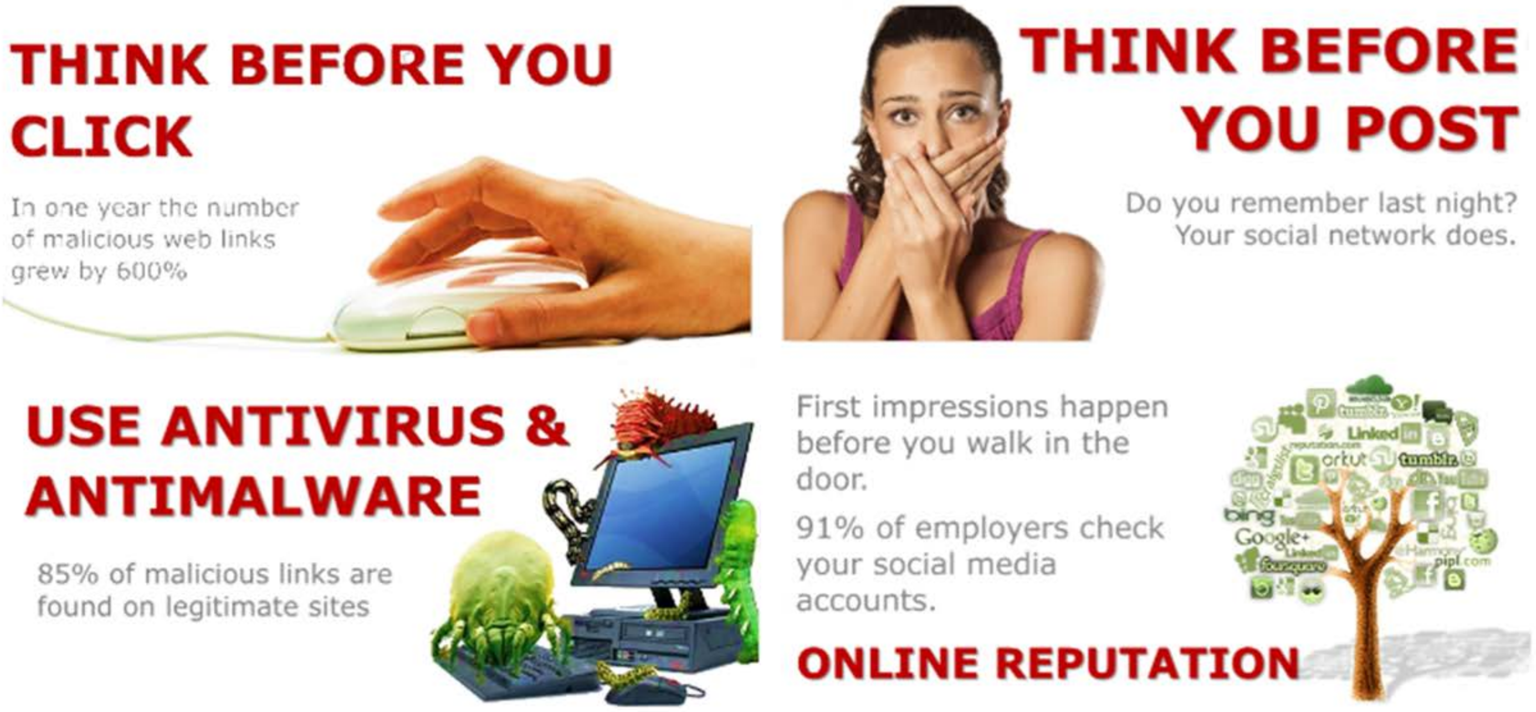
When developing an emergency response plan, include an information technology disaster recovery plan (IT DRP), and consider the following:

Information technology systems require hardware, software, data and connectivity. Without one component of the “system,” the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- **Computer room environment** (secure computer room with climate control, conditioned and backup power supply, etc.)
- **Hardware** (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- **Voice Over Internet** (VoIP)
- **Connectivity to a service provider** (fiber, cable, wireless, etc.)
- **Software applications** (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- **Data and restoration**

95% of cybersecurity breaches are due to human error

Cyber-criminals and hackers will infiltrate your company through your weakest link, which is almost never in the IT department.



THINK BEFORE YOU CLICK

In one year the number of malicious web links grew by 600%

THINK BEFORE YOU POST

Do you remember last night? Your social network does.

USE ANTIVIRUS & ANTIMALWARE

85% of malicious links are found on legitimate sites

First impressions happen before you walk in the door.

91% of employers check your social media accounts.

ONLINE REPUTATION

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your usernames, passwords, or other computer/website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization’s network without permission from your IT department.
- Make electronic and physical back-ups or copies of all your important work.
- **Report all suspicious or unusual problems with your computer to your IT department**.

5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

1. REQUIRE A SECURITY REVIEW DURING THE PROCUREMENT PROCESS

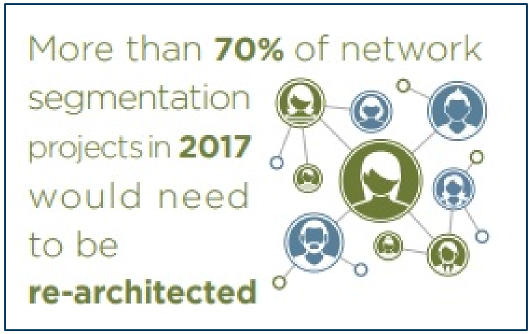
- What type of data will the medical device create, store and transmit?
- Does the medical device encrypt data in-transit and at rest?
- Does the medical device allow the password to be changed by the administrator, and does it support appropriate password complexity?
- What operating system is used?
- How will patch management of the device take place?
- Does the device contain USB or other removable media ports?

67 % of device manufacturers believe it is likely there will be an attack on one of the devices they've built within the next 12 months

5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

2. REVISIT YOUR NETWORK SEGMENTATION STRATEGY

Experts recommend healthcare institutions segment based on data sensitivity, location and criticality, and place less emphasis on things such as organizational structure.



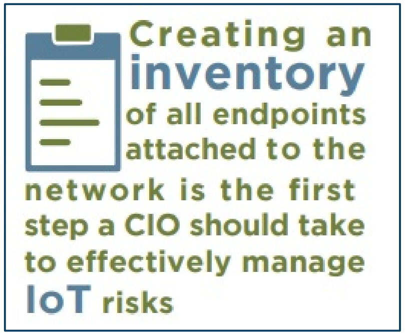
More than **70%** of network segmentation projects in **2017** would need to be **re-architected**

5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

3. IDENTIFY AND INVENTORY ALL MEDICAL DEVICES

- Network visibility is the first step to mitigating the risk of connected medical devices.

- In order to secure a device, you must first know it exists.



Creating an inventory of all endpoints attached to the network is the first step a CIO should take to effectively manage IoT risks

5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

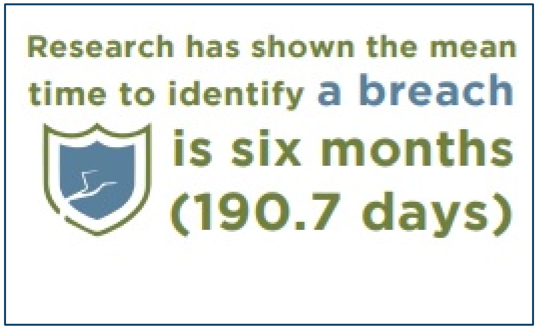
4. ONBOARD (attach to network-wire or wireless) MEDICAL DEVICES SECURELY

- More difficult than traditional devices (computers etc) because medical devices can't hold credentials like a log in and password
- Most importantly, consider only buying from medical device vendors that value cybersecurity.
- Limit access to PHI by segmenting devices inside your network.
- Protect these devices with strict firewall rules allowing access to only specific services and IP addresses.

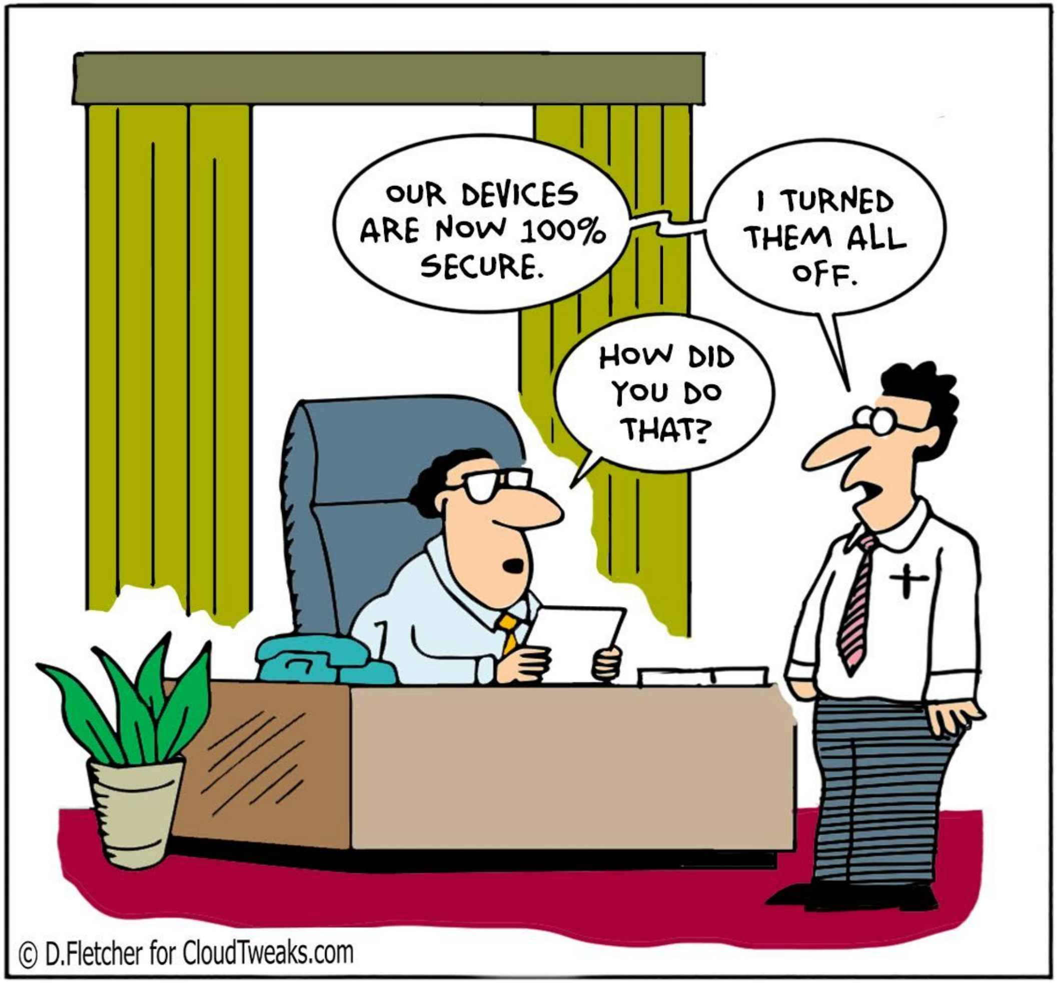
IF YOUR MEDICAL DEVICES AREN'T SECURE YOUR ORGANIZATION IS NOT HIPAA COMPLIANT.

5 BEST PRACTICES FOR MITIGATING MEDICAL DEVICE SECURITY RISKS

5. MONITOR ALL MEDICAL DEVICE BEHAVIOR
   - Detect any unusual or high-risk activity that would require security investigation



Research has shown the mean time to identify a breach is six months (190.7 days)


OUR DEVICES ARE NOW 100% SECURE.
I TURNED THEM ALL OFF.
HOW DID YOU DO THAT?
© D.Fletcher for CloudTweaks.com

Additional Resources

- Cybersecurity Best Practices
  - https://healthitsecurity.com/tag/cybersecurity-best-practices
- Homeland Security Stop.Think.Connect
  - https://www.dhs.gov/stopthinkconnect
- How to Secure your Medical Devices
  - http://info.securitymetrics.com/how-to-secure-your-medical-devices-white-paper
- IT Disaster Recovery Plan
  - https://www.ready.gov/business/implementation/IT
- Tip Cards from the Department of Health and Human Services
  - https://www.dhs.gov/publication/stopthinkconnect-government-resources

Discuss and Share Best Practices on Cyber Security

Discussion Questions

1. Has your facility experienced a cyber attack? Please explain the situation and how it affected your facility.

2. If you come across something suspicious in the cyber world (email, Internet, programs), do you know who to report it to?

3. Does your facility have a requirement to use only strong passwords or pass phrases, and change them on a regular basis?

4. Does your facility have "connected" non-computer devices and if so, are these devices secure?

5. Does your facility have an emergency response plan, that includes an information technology disaster recovery plan?

medical reserve corps

COUNTY of SAN LUIS OBISPO

Join the County of San Luis Obispo Medical Reserve Corps

1. Register to Volunteer on California Disaster Healthcare Volunteers

Complete a profile on the California Disaster Healthcare Volunteers (DHV) site: www.healthcarevolunteers.ca.gov

Make sure to choose **"San Luis Obispo County Medical Reserve Corps"** as your Unit Affiliation

2. Complete Required Training Courses

MRC Orientation—Overview of Emergency Management and the Role of the MRC (in person or classroom)

IS 100b – available online: http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-100.b

IS 700b – available online: http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-700.b

Working in a POD (Point of Distribution) – available online: http://www.ualbanycphp.org/learning

Email course completion certificates to slomrc@aol.com

3. Complete Background Check

Once you are registered on DHV and have completed all your training, the MRC Coordinator will provide you with paperwork to authorize the County of San Luis Obispo to complete a criminal and sex offender background check on you.

4. Final Paperwork, ID and Oath

Upon successful completion of your background check, the MRC Coordinator will contact you to schedule an appointment for you to come to the Health Campus (2180 Johnson Ave, SLO) to complete the remaining items:

Sign MRC Code of Conduct form

Sign HIPPA form

Take photo and receive photo ID badge

Take Disaster Services Worker Volunteer Oath

5. You are a qualified MRC Volunteer!

Access the MRC Manual online at www.slocounty.ca.gov/MRC

Questions? Contact Denise Yi: slomrc@aol.com
or visit www.slocounty.ca.gov/MRC