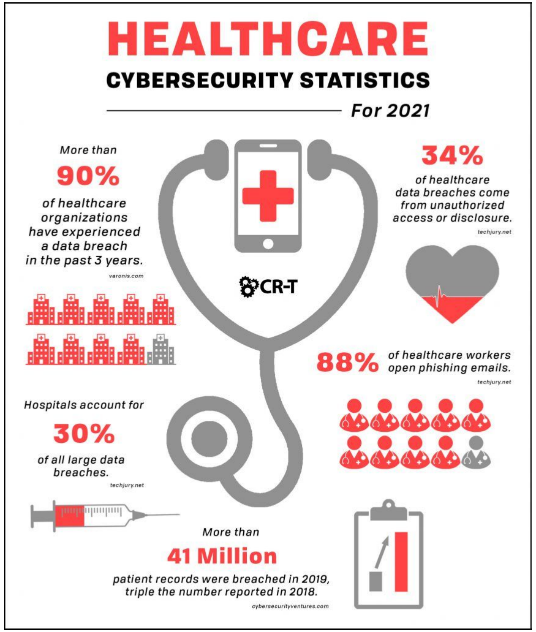
Digital Security in Hospitals

Priya Patel, Trevor Toerock, Jason Bilawsky

Introduction

- Lack of healthcare cybersecurity is one of the most significant threats to the healthcare industry
- In 2020, more than 18 million patient records were affected by successful cyber attacks
- ICS security focus has now been at an all time high trying to find ways to combat and cyber threats
- Hospitals hold not only important medical information, but important billing and personal information of patients


HEALTHCARE
CYBERSECURITY STATISTICS
For 2021
More than 90% of healthcare organizations have experienced a data breach in the past 3 years.
varonis.com
34% of healthcare data breaches come from unauthorized access or disclosure.
techjury.net
CR-T
88% of healthcare workers open phishing emails.
techjury.net
Hospitals account for 30% of all large data breaches.
techjury.net
More than 41 Million patient records were breached in 2019, triple the number reported in 2018.
cybersecurityventures.com

Prompt:

As the digital world continues to grow, so do the volume, variety, and velocity of cyber threats and attacks. The world is awash in data, and there is always someone trying to turn it into their own virtual currency. Today malware and ransomware are hitting everything from our personal cell phones to mission-critical infrastructure and supply chains.

Your team has been hired by a large hospital system to do an analysis of digital security threat that it may be facing. You are asked to present the current state of threats, various modes of attacks and how should the health system prepare itself?

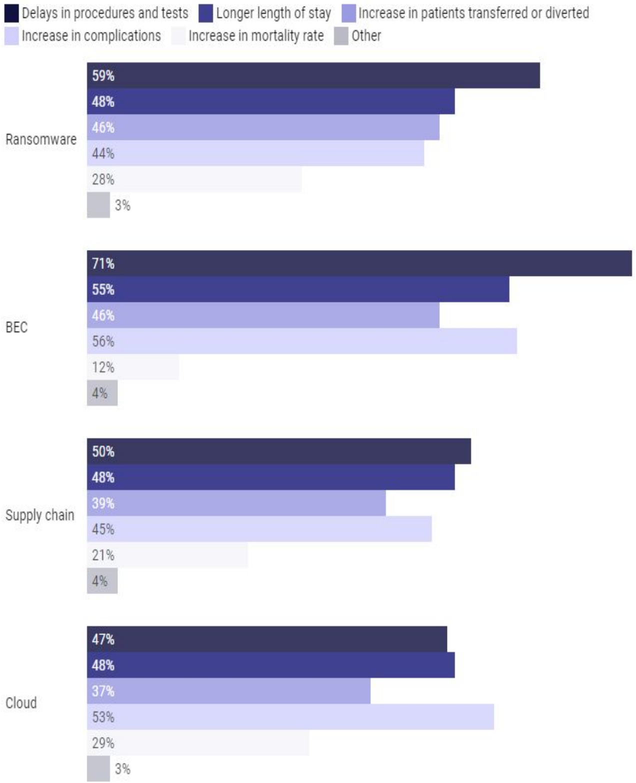
Current State Of Cyber Attacks

- 1 in 3 organizations were attacked in 2020
- There were 1,426 attacks per week in 2022 (~8.5 per hour)
    - 520,490 in 2022

Why Attack Healthcare?

Financial Gain

- Steal victim's identities and sell for profit
- Steal intellectual property
- ~$10 million per breach



Political Motives

- Raises costs of organizations
- Delays procedures/Services
- Increases Mortality Rates
- Overload Hospitals
  - Eastern Connecticut

Recent Attacks

CommonSpirit Health - started as IT problems and appointment cancellations

- Over $150 million due to legal fees, remediation and data breach mitigation. Excludes insurance company payouts

Scripps Health - IT attack resulted in portal going offline in May 2021

- Total lost revenue was around $91.6 million, recovery around $21.1 million
- Insurance/Legal Fees not included

Various Modes of Attack - Trevor

- Malware
  - Short for malicious software
  - Intrusive software developed by cybercriminals to steal, damage, or destroy data in computer systems
- Ransomware
  - Malicious software designed to steal or block access to data until a sum of money is paid
- Phishing
  - When an attacker sends fraudulent communications that seem to come from legitimate sources
  - Email, text, etc...
- Supply Chain Attacks
  - A type of cyber attack carried against organization’s suppliers
  - Used to gain unauthorized access to organization’s systems or data
  - Can be combined with previous forms of attack
- IoT Attack
  - A cyber attack done through exploiting vulnerabilities in internet-connected devices
  - Phones, laptops, industrial control systems (ICS)

How Can the Healthcare System Prepare Themselves?

The healthcare system must be vigilant at all times because of the large amounts of confidential information they are in possession of. It is important that they create strictly followed procedures and courses of action such as:

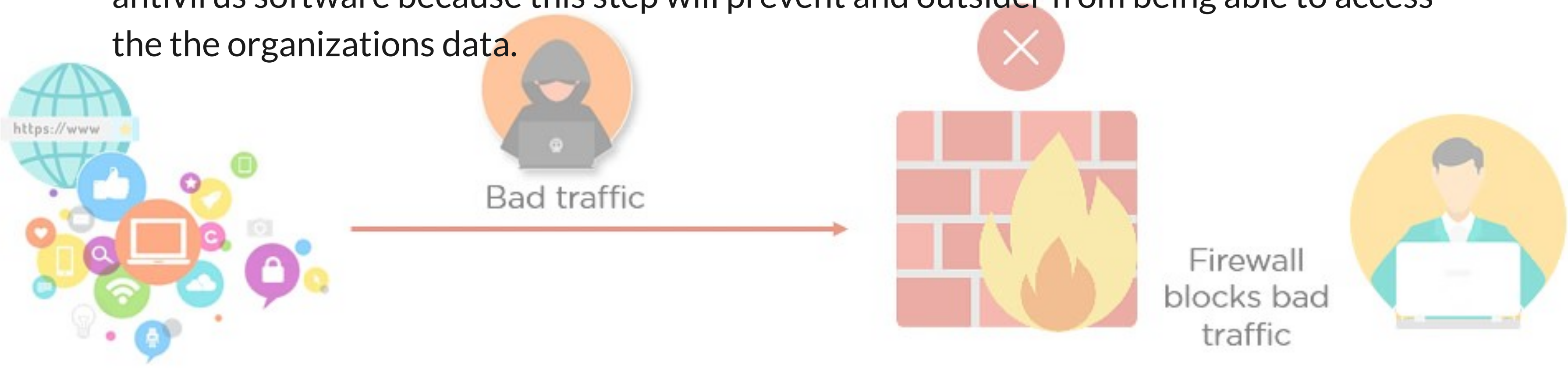
Establish Security Culture & Limit Network Access

- It is important to establish a security culture within the organization that applies to all users in the organization. In order to do this the organization must proactively implement and enforce procedures in regards to information security.
- All employees or members of the organization should be educated and trained on the importance of information security and procedures in effect to protect all protected information.
- If people understand the importance of protecting information, especially in a healthcare setting, future threats can be prevented.

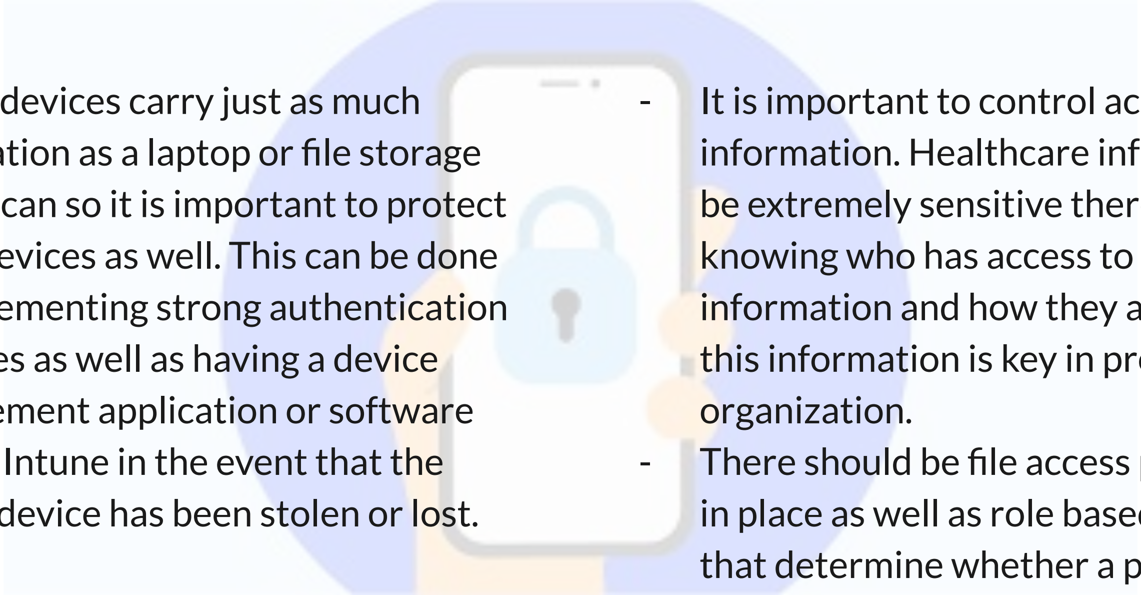
- Limiting Network Access within the organization is a simple but highly efficient way to protect information.
- Wireless routers have become incredibly easy to hack into and for a healthcare organization it is crucial that this doesn't occur. Therefore, all wireless networks should be encrypted.
- There should be separate wireless networks for employees and guests, as well as personal devices and company devices.

Anti-Virus Software & Firewalls

- Anti-Virus Software is a reliable and cost effective method to protect the healthcare system from stolen or damaged data. This software can be installed on all devices that contain confidential information and it can maintain and monitor if any threats have been detected. If there have been threats or malware detected antivirus software can automatically destroy it to protect the organization.
- Implementing firewalls can be the first step of precautionary measures even before an antivirus software because this step will prevent and outsider from being able to access the the organizations data.



Protect Mobile Devices & Control Access



- Mobile devices carry just as much information as a laptop or file storage system can so it is important to protect these devices as well. This can be done by implementing strong authentication practices as well as having a device management application or software such as Intune in the event that the mobile device has been stolen or lost.

- It is important to control access to information. Healthcare information can be extremely sensitive therefore knowing who has access to certain information and how they are accessing this information is key in protecting the organization.
- There should be file access permissions in place as well as role based permissions that determine whether a person needs access to data.

Plan for the Unexpected

- In the event that there is a data breach or information is at risk planning a course of action ahead of time is a step to prepare. This also applies to any natural or man-made disaster such as fires, floods, etc.
- Data should be backed up into hard copies or alternative forms of media as patient records may be needed on hand immediately. In the healthcare field missing data can lead to disaster therefore it is vital to have a recovery plan in place.

Conclusion

In a world of advancing technology protecting the healthcare system and the data associated with it is so important. With the various modes of attacks and current threats in place, taking proper precautions and setting procedures can make all the difference. Recently the number of cyber attacks on hospitals and healthcare organizations has been growing therefore educating yourself and others who may be involved is a key role in preventing these attacks down the road.

Any Questions or Comments?

Sources:

https://www.healthcaredive.com/news/88-percent-healthcare-organizations-report-cyberattack-ponemon-institute/696358/#:~:text=Eighty%2Deight%20percent%20of%20surveyed,by%20cybersecurity%20software%20company%20Proofpoint

https://www.checkpoint.com/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/#:~:text=The%20healthcare%20sector%20is%20a,the%20year%20targeted%20healthcare%20organizations.

https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare/#:~:text=Healthcare%20organizations%20worldwide%20averaged%201%2C463,experience%20multi%2Dmillion%20dollar%20penalties.

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

https://www.cisco.com

https://www.tripwire.com/state-of-security/ics-security-healthcare-software-vulnerabilities-threat-patient-safety