Is Your Organization Prepared for a CYBER ATTACK?

understand and mitigate your risks

WHAT ARE THE TOP THREATS?

Cyber security threats continue to grow in strength and prevalence within the healthcare ecosystem, and with health records being one of the most comprehensive set of records for an individual, alongside records stored with financial institutions, it is imperative for organizations to stay abreast of current risks and mitigate those risks adequately.

RANSOMWARE

*All six of the largest healthcare IT hacking events reported in 2017 were attributed to ransomware attacks**

DATA BREACHES

*The average cost of a medical record being $355, twice the amount of the mean across industries of $158**

IoT RISKS

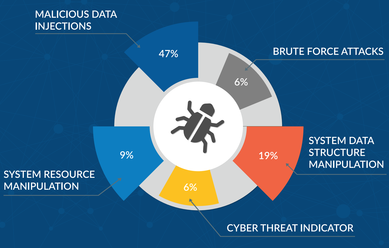
*2018 is suspected to be the year of IoT attacks, with the prevalence of healthcare management on devices**

Source: IBM Security Trends in the Healthcare Industry https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03123USEN
https://www.healthcare-informatics.com/news-item/cybersecurity/report-ransomware-attacks-against-healthcare-orgs-increased-89-percent-2017

TOP 5 ATTACK VECTORS

An attack is defined as a security event observed in a system or network that has been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, falsify or destroy information system resources, or the information itself.*

Source: IBM Security Trends in the Healthcare Industry
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03123USEN



WHO IS AT RISK?

TOP 10 ATTACKS OF 2017

Below is the top 10 healthcare cyber attacks of 2017, showing how no type of organization is safe from these malicious attacks.

Entity Breached	# Of Records Exposed	Attack Type
Airway Oxygen, Inc.	500,000	Ransomware
Women's Health Care Group of PA	300,000	Ransomware
Urology Austin	279,663	Ransomware
Pacific Alliance Medical Center	266,123	Ransomware
Peachtree Neurological Clinic	176,295	Hacking
Arkansas Oral & Facial Surgery Center	128,000	Ransomware
McLaren Medical Group, Mid-Michigan Physicians Imaging Center	106,008	Hacking
Harrisburg Gastroenterology	93,323	Hacking
VisionQuest Eyecare	85,995	Hacking
Washington University School of Medicine	80,270	Phishing (Email)

Source: https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/

HOW DO WE REDUCE OUR RISK?

Although **RISK WILL NEVER BE ZERO** there are ways to help improve your odds of avoiding a security breach. Strengthening your information security posture from top to bottom is the first step and is imperative for proteticng your organization as a whole from malicious attacks.

TOP BUSINESS PRIORITY

One of the most important aspects of improving your security posture is ensuring that cyber security is a business priority. This will help to ensure that an organization has buy-in from all units, budget, and head count to implement all security measures.

BACKUP YOUR DATA

With ransomware becoming an increasingly prevalent problem, it is incredibly important to back up your data. On top of just backing your data up, you also want to do testing of those backups to ensure no corruption or loss of information.

REVIEW MEDICAL DEVICES

It is important to review all medical devices for any security issues and apply data protection methods to all of them. This may include ensuring software is up to date, patching known security holes, and reviewing outdated items to decide on usage.

MITIGATE INTERNAL THREATS

To reduce the chance of internal threats, organizations need to implement data security and identity/access management in order to protect that data and access control. This includes all log-in's that employees may use and data they have access to.