ECF

Microsoft

13 CYBER SECURITY THREATS THAT COULD JEOPARDIZE YOUR PATIENT DATA

AND HOW TO DEFEND YOUR HEALTHCARE ORGANIZATION

Since 2009, over 382 million healthcare records have been exposed due to data breaches. There are many ways that hackers can infiltrate your business and compromise sensitive information. But with the right managed IT environment, you can keep them at bay.

We've uncovered the Top 13 nefarious techniques that attackers use every day and how you can defend against them.

1. PHISHING ATTACKS.

THREAT ID: The most standard yet effective way for cyber attackers to infiltrate your business is through malicious emails and websites. Look out for emails that contain gibberish or have unknown senders.

SYMPTOM: Once in your system, a virus delivered by email will replicate itself and spread to other computers on the network. Look out for a system crash, unwanted pop-ups, or monetary theft.

RECOMMENDED SOLUTION: Microsoft Defender combined with ECF Microsoft 365 assessment, remediation & training services.

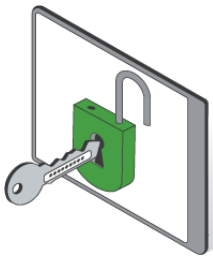
2. DENIAL OF SERVICE (DoS) ATTACKS

THREAT ID: A DoS attack floods your servers with requests in order to freeze your business operations. Worse still, Distributed Denial of Service (DDoS) attacks use multiple systems to target your network.

SYMPTOM: DoS attacks bar access to critical services such as bed capacity, data sharing, and appointment scheduling services, which can jeopardize patient care, hospital safety, and incur legal fines and loss of trust among your consumers.

RECOMMENDED SOLUTION: Microsoft Azure DDoS Protection, Azure Application Gateway & Web Application Firewall for combined with ECF Managed Security Services.

3. ATTACKS AGAINST I NDUSTRIAL CONTROLS, EQUIPMENT, & IoT DEVICES



THREAT ID: From the smallest phone to the largest server, no device is safe from an attack in today's world. IoT devices such as bedside monitors, implanted medical devices, and smart door locks, can exchange data with other systems over the internet.

This increases vulnerability and positions these devices for attacks.

SYMPTOM: Once an IoT device has been infiltrated, hackers can carry out phishing, ransomware, and DoS attacks.

RECOMMENDED SOLUTION: Microsoft Defender for IoT combined with ECF Managed Security Services.

4. UNAUTHORIZED USE OF COMPANY PCs, NETWORKS, OR MOBILE DEVICES

THREAT ID: In 2022, 113 unauthorized access data breaches were reported. These range from errors by employees, negligence, snooping, and data theft by malicious insiders.

SYMPTOM: Unauthorized access breaches can lead to reduced revenue, legal fees, and delays in patient care.

RECOMMENDED SOLUTION: Microsoft Defender & Intune solutions combined with ECF Microsoft 365 assessment & remediation Managed Security Services.

5. THEFT OF PASSWORDS OR OTHER PERSONAL INFORMATION

THREAT ID: Over 80% of data breaches are due to compromised passwords and password sharing is common among hospital staff. Weak password policies expose patient information.

SYMPTOM: Password theft can jeopardize medical records, patient history, test results, and other confidential patient and financial data.

RECOMMENDED SOLUTION: Microsoft Purview combined with ECF Protect & Govern Sensitive Data assessment & remediation Managed Security Services.

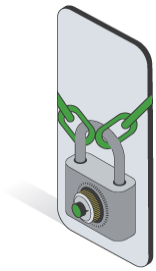
6. IMPERSONATION OF YOUR ORGANIZATION'S STAFF

THREAT ID: Impersonation takes place when someone lies about their qualifications or identity to attempt to gain access to data, drugs, or other sensitive information.

SYMPTOM: If left untreated, impersonation can lead to stolen equipment or medications, data leaks, forgery, and heavy fines.

RECOMMENDED SOLUTION: Microsoft Defender for IoT combined with ECF Managed Security Services.

7. PHYSICAL BREAK-IN AT YOUR BUSINESS SITE



THREAT ID: We talk a lot about digital security, but what about physical break-ins? These can be just as detrimental to the safety of your patients, staff, and organization.

SYMPTOM: Physical break-ins can lead to permanent equipment damage, theft of drugs and computer hardware, as well as jeopardize the safety of everyone in the facility.

RECOMMENDED SOLUTION: Microsoft Azure Sentinel combined with ECF Defend Against Threats with SIEM Plus XDR assessment & remediation Managed Security Services.

8. UNAUTHORIZED ACCESS INTO YOUR NETWORK

THREAT ID: Hackers are often the first thing that comes to mind when we think of security risks. They are the main cause of healthcare data breaches, according to the HIPAA Journal.

SYMPTOM: Data breaches can lead to a loss of trust in your organization, legal fees, and permanent loss of data.

RECOMMENDED SOLUTION: Microsoft inbuilt strong password & MFA combined with ECF Microsoft Identity assessment & remediation Managed Security Services.

9. THEFT OR LOSS OF SMARTPHONES, PCs, OR TABLETS

THREAT ID: It's easy to misplace your personal and work devices. When devices like tablets and PCs store patient data, misplacing one shifts from disruptive to downright dangerous.

SYMPTOM: A lost or stolen healthcare device places sensitive medical information right into the hands of someone not authorized to access it.

RECOMMENDED SOLUTION: Microsoft Intune combined with ECF Managed Security Services.

10. THEFT OF CUSTOMERS' PERSONAL OR CREDIT CARD INFORMATION

THREAT ID: When facilities collect a patient's financial data, it can put them at risk for theft of health insurance cards, billing statements, and other financial documents.

SYMPTOM: When a patient loses access to their financial information, it is costly for them and the facility. Patients may not know they were a victim of financial fraud until it's too late.

RECOMMENDED SOLUTION: Microsoft Purview combined with ECF Protect and Govern Sensitive Data assessment & remediation Managed Security Services.

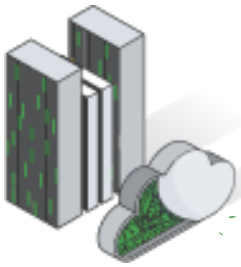
11. RANSOMWARE

THREAT ID: Ransomware attacks occur when a hacker locks healthcare professionals out of their systems until they make payments. In 2020, Ransomware attacks cost US healthcare organizations $20.8 billion.

SYMPTOM: These attacks delay patient treatments, bar access to files and test results, and can lead to a permanent loss of business-critical data and damage your organization's reputation.

RECOMMENDED SOLUTION: Microsoft Defender, Azure Sentinel, Purview, Intune, and MFA combined with ECF Protect & Govern Sensitive Data assessment, remediation Managed Security Services.

12. THEFT OF CRITICAL BUSINESS DATA



THREAT ID: Your business data is just as important as patient data. From finance, to operations, to human resources, your business information holds essential details.

SYMPTOM: A permanent loss of business-critical data can lead to a decrease in productivity, loss of trust,roadblocks in workflow, and threaten your organization's viability.

RECOMMENDED SOLUTION: Microsoft Defender, Azure Sentinel, Purview, Intune, and MFA combined with ECF Protect & Govern Sensitive Data assessment, remediation Managed Security Services.

13. NO IT SECURITY RELATED EVENTS IN THE LAST YEAR

THREAT ID: An absence of a security-related incident may seem like a success, but it could suggest that you aren't detecting threats. Healthcare data breaches happen every day and are on the rise with almost two data breaches reported daily in 2022.

SYMPTOM: Just like our health, a robust security system requires regular checkups and proactive planning. A security approach that isn't catching hacking attempts isn't properly prepared to remediate successful attacks.

RECOMMENDED SOLUTION: Microsoft Azure Sentinel combined with ECF Defend Against Threats with SIEM Plus XDR assessment, remediation Managed Security Services.

DON'T WAIT UNTIL THESE 13 THREATS BECOME YOUR REALITY:

GET PROTECTED WITH ECF MANAGED HEALTHCARE IT SERVICES

A healthy security system needs more than a yearly exam. ECF will ensure your security is at the top of its game every day of the year. Our agile, efficient, and experienced IT professionals help remove the burden of around-the-clock cybersecurity monitoring from your organization's already taxed internal IT staff.

AS AN EXTENSION OF YOUR TEAM, WE'LL HELP:

- Detect and respond to threats on your behalf
- Implement cost-effective technology to reduce enterprise-wide risk
- Employ the full potential of Microsoft Azure and the Microsoft 365 stack

OUR PROVEN TRACK RECORD SPEAKS FOR ITSELF:

- Microsoft Security certification including facility authorization
- 1 of 12 Hybrid Managed Partners selected for Microsoft's Black Partner Growth Initiative program
- 7 Microsoft Certified security professionals on staff

STAY AHEAD OF HACKERS THAT THREATEN YOUR HEALTHCARE ORGANIZATION.

CONTACT US FOR A FREE SECURITY ASSESSMENT:

JOSEPH.HENDERSON@ECFDATA

ECFDATA.COM/XXXXXXXXXX