How Hospitals Can Prepare for Ransomware Attacks

10 STEPS TO TAKE NOW

In light of recent ransomware attacks on hospitals, ISACA experts weighed in on some key actions you can take to protect your hospital and keep providing uninterrupted patient care.

1 UNDERSTAND

YOUR RISK PROFILES

Hospitals, like most organizations, must understand their risks in order to accurately prepare for potential attacks. To do this, you must understand what your responsibilities, products and services are, and know the technical requirements affiliated with each. In gaining understanding of these risks, your hospital can better assess areas that require the most attention when allocating cybersecurity resources.

2 REALIZE

YOUR DATA RESPONSIBILITIES

You should realize the types of data that you are responsible for storing, transmitting, and protecting. Understanding the data types will help your hospital identify what policies, such as HIPAA, may apply to the protection of the information.

3 TEST

FOR INCOMING PHISHING ATTACKS

Most attacks start with a phishing campaign, and they are still effective. Try testing filters by sending yourself "de-weaponized" phishing emails identified by others from an external test email account. How often will they make it through? Test it; maybe your email filters need to be tuned up.

4 ASSESS

ALL CYBERSECURITY CONTROLS ON A REGULAR AND EVENT-BASED BASIS

Regularly assess and audit your cybersecurity controls to ensure that they are applied and maintained appropriately. A truly mature organization will test these controls on both a time-based schedule and in response to incidents. In this case, use recent ransomware attacks against other hospitals as an opportunity to assess your systems to ensure they are not at risk. Consider setting up tests to ensure that your red team will be detected in a ransomware test exercise.

5 EVALUATE

PATCHES IN A TIMELY FASHION

Healthcare organizations often struggle with vulnerability management and patching. In many cases, hospitals fail to patch systems connected to patient care equipment. It is understandable that most hospitals will not apply a security patch immediately upon dissemination from the issuing organization – business processes may break, and delivery systems may fail. However, ensure that patches are applied in an organized and methodical fashion. For vulnerable legacy systems that can't be patched or updated, hospitals need to isolate them in their network and ensure they do not have access to the internet.

> "When healthcare organizations understand their critical assets, along with the potential impacts on operations in the event of a ransomware or other disruptive attack, they will be well-positioned to determine the more tactical approaches to reducing risk exposure, such as user security awareness training, data backups, hardened baseline configurations, system patching, privileged account management, and network segmentation."

—Mike Green, CISSP, CDPSE, CAP, Senior Cybersecurity Engineer, Optic Cyber Solutions

> "Hospitals are very vulnerable to ransomware attacks as they typically focus their limited resources on the latest medical technologies, but not always on keeping legacy systems up to date. This, as well as having systems that are often siloed and disparate, can leave hospitals with unprotected gaps that make them easier to attack."

—Pam Nigro, Vice President Information Technology and Security Officer at Home Access Health Corporation, and ISACA board director

6 PERFORM

REGULAR POLICY REVIEWS

Make sure that all pertinent cybersecurity policies not only exist at your hospital, but are also regularly evaluated and updated based upon the ever-changing cybersecurity landscape. Specifically, update these policies based on both time-based schedules and event-based instances.

7 LEVERAGE

THREAT INTELLIGENCE APPROPRIATELY

Reading and disseminating threat intelligence throughout a cybersecurity team can be overwhelming. Hacks and cyberattacks occur on a 24/7 basis, with different forks of similar attacks emerging overnight in many instances. Understanding which type of intelligence applies to your hospital and parsing it out correctly will help you understand what threats may pose the greatest danger to your organization.

8 PROTECT

END-USER DEVICES

We often forget to ensure 100 percent protection on end-user devices – not only for devices within the network, but all devices used by remote users to access systems. Exclusion lists should be minimal. In today's healthcare landscape, there are many sensitive applications – do not let application vendors dictate anti-virus policies.

9 COMMUNICATE

CLEARLY WITH EXECUTIVE LEADERSHIP AND EMPLOYEES

To gain executive support, ensure that your reporting and communication to the leadership level is clear and accurate. Once leadership understands the threat, the risk, and the potential impacts, cybersecurity teams stand a greater chance to receive the funding and support required to protect the organization. Hospital employees also need to be trained on how to open emails and websites safely—some tactics include gamification, highlighting hospital cyber heroes, and creating a rewarding phishing reporting structure.

10 COMPREHEND

THE ORGANIZATIONAL CYBERMATURITY

All of the points listed here are part of comprehending an organization's cybermaturity—or comprehending an organization's developed defensive readiness against potential cyber-attacks and exploitations. If you understand your hospital's maturity level and actively work to raise it, you stand the best chance to defend your hospital in today's chaotic cyber landscape.

“Right now, hospitals and health service providers that did not fall victim to the most recent ransomware attacks should be assessing their systems to ensure they are not at risk and then taking key actions to protect themselves and bolster their cybermaturity so they are in a stronger position to fend off future attacks.”

–Frank Downs, Senior Director, Cybersecurity Advisor and Assessment Solutions, ISACA

“Should the worst happen, and hospitals fall prey to ransomware, they have two choices: pay the ransom, or restore and recover all systems affected from backups. We often see that either backups aren't working, recovery times are way too long, or the organization doesn't have the ability to recover.”

–George Quinlan, CISA, CISM, CRISC, CDPSE, Senior Manager – Security & Privacy, Protiviti

“Many anti-virus installations have a mile-long list of exceptions put in by different technical personnel, often without full review or merit. Hospitals may be surprised that their defenses are rendered blind because of someone's troubleshooting effort from a few years ago.”

–Alex Holden, Chief Information Security Officer, Hold Security, LLC
See Alex's related blog post.

ISACA

For more cybersecurity resources, visit **www.isaca.org/resources/cybersecurity**. To learn more about strengthening enterprise cybermaturity, visit **https://cmmiinstitute.com/products/cybermaturity**.