HIPAA & GLOBAL PHI COMPLIANCE

How to prevent 2x and 3x-threat ransomware in the Healthcare Industry with NIST CSF

Protected Health Information (PHI) threats are a significant concern for every healthcare-related organization because:

- In 2020, over 26 million healthcare records were compromised in the US alone.[1]
- Ransomware attacks had cost the healthcare industry over $20 billion in 2020.[2]

Under the HIPAA privacy rule, a ransomware attack is a notifiable violation even if PHI is just encrypted and not copied or stolen. Therefore, proactive defense against all forms of cyberthreats is vital for organizations in the healthcare sector.

Read further to learn how your organization can protect against sophisticated ransomware and other threats that affect healthcare data security and compliance around the globe.

KNOW THE EXPANDING RANSOMWARE THREATSCAPE

Ransomware caused close to 10% of breaches reported in 2021.[3] Cybercriminals using this attack vector adopt three approaches:

TRADITIONAL RANSOMWARE

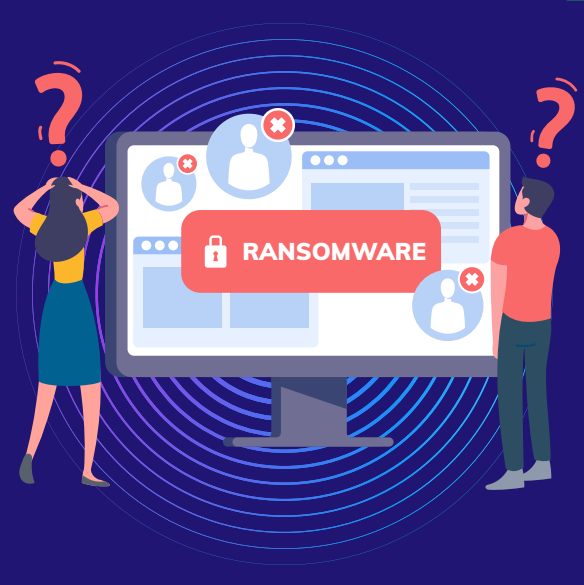
It is the simplest form of ransomware— once a network and devices fall prey to malware, hackers will encrypt the files and share the decryption keys until the victim pays the ransom.

DOUBLE-THREAT RANSOMWARE

Hackers using this approach encrypt healthcare data and make a copy for themselves. The victims then receive a note demanding payment for decryption keys and threaten the disclosure of protected data if the victim does not pay the ransom.

TRIPLE-THREAT RANSOMWARE

Victims receive a ransom note demanding payment and threatening the disclosure of protected data, but additionally, their patients also receive ransom notes demanding payments.



An example to prove the dangers of triple-threat ransomware is the case of Vastaamo, a psychiatric clinic in Finland that fell for ransomware. They did not pay the ransom, but their patients received notes demanding payment to keep psychotherapy data secret. The extortionists eventually released close to 300 files.[4]

RANSOMWARE IMPACT ON PATIENT CARE

DELAYS IN CARE

A May 2021 ransomware attack on a California-based healthcare provider, Scripps Health, caused close to four weeks of downtime, resulting in many appointments being rescheduled or recorded via paper documentation as the ePHI system was unavailable.[5]

PAPER RECORD CHALLENGES

Urgent appointments that Scripps Health couldn't reschedule were recorded on paper as the ePHI remained unavailable. Paper records present issues of their own — could be lost, misfiled, damaged, etc.

PRIVACY CONCERNS

Perhaps the worst outcome of an attack is that healthcare consumers (especially those seeking sensitive services like mental healthcare) might avoid seeking professional help because of fears of their most private information being posted online for all to see.

Healthcare facilities must view cybersecurity as paramount to providing care. Without security, there can't be privacy. Without privacy, there can't be trust. Thus, healthcare organizations must make security and compliance priorities when balancing budgets.

HOW THE NIST CYBERSECURITY FRAMEWORK CAN MINIMIZE RISKS

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a joint initiative by the US government and private sector. It provides a globally applicable policy framework of cybersecurity guidance. This framework outlines how organizations can assess and enhance their capability to block, detect and respond to cyberattacks.

The five functions under NIST CSF are:

IDENTIFY

This function helps an organization understand its cyber risks related to people, assets, systems, data and capabilities.

PROTECT

This function summarizes suitable precautions to safeguard the delivery of critical infrastructure services.

DETECT

This function specifies the necessary activities to detect the occurrence of a cybersecurity event.

RESPOND

This function highlights key activities to respond to a detected cybersecurity incident.

RECOVER

This function identifies appropriate activities to protect resiliency plans and restore capabilities/services damaged by a cybersecurity incident. It supports the timely recovery of normal operations to lessen the impact of an incident.

The above five functions have 23 categories and 108 subcategories. It provides greater clarity than HIPAA Security Rule's 42 requirements that were written almost 20 years ago — and is universally applicable beyond the United States.

A new federal law sanctioned on January 5, 2021, plans to reward HIPAA-covered entities that have implemented NIST CSF. ***The law takes off an enormous burden by reducing fines and providing audit relief if you prove you have applied the NIST CSF for the past 12 months.***

START PROTECTING PHI WITH NIST CSF

If NIST cybersecurity framework sounds too complicated, don't worry. We not only specialize in helping organizations comply with HIPAA, but also help you implement and hold accountability to the NIST CSF.

Contact us today to learn how we can identify and bridge ePHI gaps in healthcare practices with a detailed assessment and risk analysis.

SOURCE
1. Businesswire | 2. Healthcare Innovation | 3. Verizon DBIR 2021 | 4. Wired.com | 5. Kpbs.org

RESTECH SOLUTIONS

Contact Us:
713-936-6855
info@restech.solutions
https://restech.solutions/contact