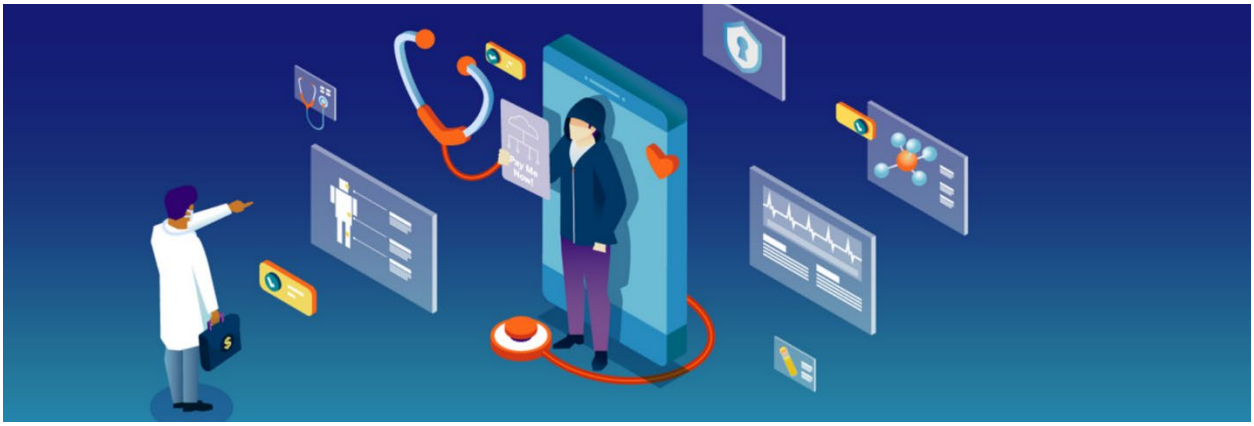

Ransomware attacks are plaguing the healthcare industry. Here are actions organizations should take now before they find their systems victimized.

In Brief:

As the threat of ransomware attacks on healthcare systems continues to rise, some traditional defensive measures are becoming obsolete. To better prepare, and to mitigate issues following an attack, firms must take a holistic approach to fortifying their cybersecurity posture.

The ransomware attacks that grab headlines typically tend to involve big payouts or major system disruptions. In late April, for instance, a cybersecurity incident that caused huge gas shortages in the United States and netted hackers USD$4.4 million (later partially recovered by the U.S. government) splashed across global newsfeeds for weeks.

But for every headline-worthy ransomware incident, many others fly under the radar. Nowhere is this more evident than in the global healthcare industry. In May, the FBI linked the same threat group responsible for a ransomware attack on Ireland's health service IT system that month to at least 16 past attempts to disrupt U.S. healthcare first-responder networks.

Health systems have been attractive targets for ransomware operators for several years now because of the sensitive patient data they own and the urgency around

accessing healthcare in general. A single attack can force system outages that result in hundreds of missed appointments, exposure of patient records and shutdowns of operating room machinery — and even death.

Due to recent developments, health systems have become even more enticing targets. These include increased use of telehealth and new applications that grant access to protected health information (PHI). The COVID-19 pandemic, which accelerated the digital transformation that was slowly progressing throughout the industry, also contributed, with wider adoption of cloud services, software as a service, and more medical devices connecting to the Internet and core clinical systems.

All this leaves the healthcare industry in a difficult spot. While technological change is vital to advancement, the pace of change now exceeds the resourcing and planning speed at which many health systems traditionally operate. Compounding the issue, ransomware operators continue to stay a step ahead of cybersecurity defenses. Due to evolutions in tactics, techniques and procedures, some traditional ransomware remedial measures are no longer effective on their own.

Outdated Defenses

Mixed in with the news about ransomware attacks are a number of remediation tactics that might best be described as outdated or even misguided. Relying on backup systems to restore service is one. While maintaining robust backups is critical for any company, the action in itself does not defend against "double-extortion schemes" (where hackers threaten to expose sensitive information they've stolen to the public). Nor does it remediate instances of data theft.

Further, organizations that do not effectively segment their backups from their production systems or remove them from the environment entirely leave the backups at risk.

Cyber insurance, a standard industry fallback, is becoming less effective as more insurance firms consider halting payments and raising premiums for organizations that aren't well protected against ransomware. Insurance companies have also become

targets themselves, as holding policy data ransom provides cyber actors with perfect bargaining power.

Finally, there's simply paying the ransom, which some victimized organizations have chosen to do. But doing so may only provide access to some of the encrypted data held hostage. And, following recovery, performing integrity checks is critical to resuming function.

Proactive Measures to Take Now

Addressing the threat of ransomware requires a holistic, proactive approach. Here are measures every health system should implement to reduce the threat of ransomware.

Take inventory.
Ensure that systems involved in processing and storing critical data, particularly PHI, are inventoried, data flows are well documented, and the criticality of the system is appropriately identified. Effective controls cannot be properly implemented if the data flows throughout these systems are not understood.

Manage critical systems.
Access to critical systems, including users and application programming interfaces (APIs), should be tightly controlled. Direct access to these systems should be limited to the users with explicit need, such as database administrators. Credentials should be kept in vaults and only granted as needed.

Servers should have endpoint management and protection solutions deployed that are specifically tuned to identify potentially malicious files, processes, and binaries that could contain ransomware. Continuous monitoring of these is key so that teams can react to warnings quickly and isolate infected systems before malware can spread.

Critical systems should be regularly assessed for vulnerabilities. Any identified vulnerabilities should be patched expeditiously.

Assess application architectures regularly.
This includes underlying code. Follow strict change control procedures to ensure that

vulnerabilities are not introduced into critical systems. Third parties that supply applications, such as electronic medical record vendors and medical device manufacturers, should be held to strict information security and data protection standards and regularly assessed for new risks.

Control networks.
Those that provide access to critical systems should be tightly controlled and continuously monitored for evidence of suspicious traffic.

Conduct regular testing.
Identify gaps and weaknesses in the security controls through penetration tests against critical systems. This enables immediate remediation efforts before attackers can exploit the same weaknesses. Penetration tests should have explicit rules of engagement so as not to cause inadvertent outages to production systems.

Reactive Measures to Mitigate Damage

A health system that suffers a ransomware attack and doesn't have the following remedial steps in place courts ongoing trouble. Here are measures that should be implemented now to facilitate recovery if the worst should happen.

Back it up.
Critical systems and applications must have redundancies, backups and recovery plans. Specifically, backups should be completely segregated from the production network to prevent ransomware from spreading to the backup systems.

Have a plan.
Well-tested and up-to-date business continuity plans, including plans that can be accessed via hard copy only, are a must. It's not enough to only have backups; testing of backups is a must, and the organization should understand how long a full recovery will take for each system.

RANSOMWARE DEFINED The FBI defines ransomware as "a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return."

Source: Federal Bureau of Investigation

Be ready to respond.

Organizations must design incident response plans that are tailored to ransomware attacks against specific critical systems, allowing stakeholders to react to an ongoing attack instantly. Incident response plans are most effective when they are tested regularly.

Have insurance.

Despite reduced effectiveness, cyber insurance remains a must-have. Organizations may refuse to pay a threat actor group for access to decryption keys to save expense, but the cost of response and recovery activities can be burdensome (and out of budget), such as complex investigations to identify the source of the attack. Cyber insurance can help offset some of these costs.

Relying on information security programs to effectively prevent ransomware attacks is possible, but only if certain controls are specifically designed for and tested against specific attributes that make ransomware attacks challenging. In today's — and tomorrow's — cybersecurity world, mitigating the threat from ransomware attacks requires health systems to adapt and build stronger cybersecurity immune systems by implementing new strategies and processes that emphasize readiness.

Key Contacts

Jordan Rae Kelly
Senior Managing Director, Head of Cybersecurity, Americas

Matt McManus
Senior Director

About The Journal

The FTI Journal publication Offers deep and engaging insights to contextualize the issues that matter, and explores topics that will impact the risks your business faces and its reputation.