The Critical Steps Healthcare Providers and Systems Should Take to Combat the Surge in Ransomware Attacks

People's United Bank®

Healthcare providers and systems are squarely in the crosshairs of cybercriminals, and this threat will persist given the value of patient information and the vulnerability of their networks. By targeting providers with attacks that scramble and lock up data until victims pay a ransom, hackers can demand thousands or millions of dollars. Such attacks increased during 2020, which prompted the federal government to issue a warning to healthcare providers about "credible, ongoing and persistent" cybersecurity threats. In this environment, hospital and healthcare executives need to adopt best practices both to repel attacks and also respond to attacks if they are successful.

The scope of the problem is difficult to overstate. According to the Associated Press, ransomware is partly to blame for about 700 private health information breaches (affecting 46.6 million people) that the federal government is currently investigating. Recent attacks against healthcare organizations have resulted in outages lasting longer than 30 days, loses of over $1 million a day, and overall related expenses exceeding $50 million.

Not all victims pay a ransom, but many do, and they have cybersecurity insurance expressly for this purpose. Once cybercriminals have infiltrated a healthcare provider or network there are clearly strong incentives to pay the attackers as quickly and quietly as possible to avoid public embarrassment, regain access to systems and keep patient records private. "Once criminals get into certain systems, no one can be admitted or discharged," said Steve Stasiukonis, a managing partner at Secure Network Technologies, an information security consulting firm. "The costs are huge. These are really bad, sinister people." Typically, these criminals are part of syndicates based in Eastern Europe and Russia and are very rarely caught.

Read this guide to learn:

- Why Healthcare Providers and Systems are Ransomware Attack Targets
- What You Can Do to Protect Your Organization

Why are Healthcare Providers and Systems Tempting Targets?

There are many reasons why healthcare providers and systems are such attractive targets. First and foremost is the payday. "Criminals want to make money, and they know that healthcare providers and networks need to get their systems back up and running as quickly as possible to care for patients," explains Jeff Tarte, SVP, Chief Information Security Officer at People's United Bank. They also know that healthcare providers and networks are treasure troves of patient information. Cybersecurity Ventures estimates that personal health information is 50 times more valuable on the black market than financial information. But the other reason that hospital and healthcare networks are such attractive targets is their many vulnerabilities.

Stretched resources: "There's never enough money in the budget for cybersecurity," Stasiukonis said, which makes it difficult for healthcare providers to keep up with the evolving threat. Health systems spend only 4% to 7% of their IT budget on cybersecurity, whereas other industries such as banking or insurance spend three times as much, according to Associated Press reports. COVID-19 has made matters worse. Many hospitals and healthcare networks postponed technology upgrades or cybersecurity training that would help protect them from the newest wave of attacks.

Old technology and complex systems: At most healthcare providers and networks, the backbone systems and technology are outdated and complex, often cobbled together over decades of mergers and acquisitions. This creates gaps in security that cybercrooks can exploit. For example, the anti-virus solutions that worked four years ago can't detect many of today's threats. "You need a different set of tools to keep up with changes in ransomware," Tarte said. "A lot of attackers use technology management tools that make their activity look like legitimate IT administrators doing their jobs."

Medical devices: At large organizations there can be thousands of medical devices connected to the network. It's difficult to monitor all these devices or efficiently upgrade security across the network. Medical devices such as x-rays, insulin pumps and defibrillators lack the security found on other network devices such as laptops and computers. But hackers can use them to attack a server that holds valuable information.

Supply chain vulnerabilities: Cybercriminals don't just look at the healthcare providers and systems for vulnerabilities. They are experts at exploiting security gaps at trusted healthcare vendors to infiltrate hospitals and healthcare networks, and they often focus on payments made by accounts payable. Payment fraud is an increasing threat for financial professionals and the businesses they support, regardless of industry. Before the pandemic, 81% of businesses across industries had been targets of payment fraud. The pandemic has only made matters worse. Companies must now anticipate new vulnerabilities resulting from changed business processes, such as fast-tracking new business partners and suppliers. Among anti-fraud experts, 82% anticipate payment fraud will increase over the next 12 months.

> **98% of cyberattacks across all industries rely on social engineering, tempting employees to click on links that will download malware or to simply misdirect them.**
>
> – ACFE Fraud in the Wake of COVID-19: Benchmarking Report, December 2020

The workforce: An enormous number of people must access hospital and healthcare networks every day, opening up numerous attack vectors. Social engineering that targets employees is on the rise: 98% of cyberattacks across all industries rely on social engineering, tempting employees to click on links that will download malware or to simply misdirect them. For example, cybercriminals will often send bogus payment update information, hoping to trick employees into send legitimate payments to their illegitimate accounts. Again, the pandemic is only making matters worse. Among anti-fraud experts, 77% say that fraud prevention and fraud investigations are more challenging as remote work continues.

What can Healthcare Providers and Networks do to Protect Themselves?

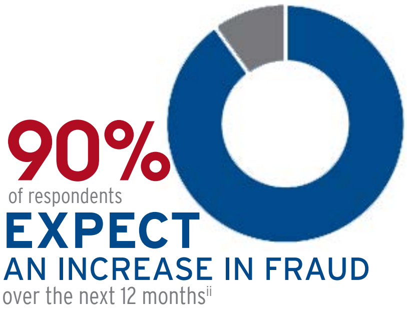
Research by the Ponemon Institute, a consulting firm, has indicated that only about 15% of healthcare organizations have adopted the technology, training and procedures necessary to manage the cyberattacks they regularly face. Ultimately, the goal is to limit the organization's "attack surface," Tarte said, "to minimize customer disruption, reduce financial loss, and speed up recovery." To this end, organizations can follow several steps.

Conduct a security assessment and penetration test. This is a comprehensive scan of all organizational systems, existing security software, Wi-Fi and hard-lined network connections, hardware, firewall devices, and VPNs that healthcare staff might access remotely. By stress testing an exact copy of the entire network the same way an attacker would, it's possible to identify and start closing security gaps, and prioritize critical assets.

Run an application security assessment. This tests the software applications used to keep the healthcare facility up and running. This includes EMR systems like Medent, scheduling software, web applications, patient portals and more. It's also important to test the organization's security credential conventions such as password policies, application permissions, access points and access-controlled computer clusters (such as the pharmacy's software utilities).

Coordinate phishing and social engineering penetration tests. These tests gauge the likelihood that people in the organization will give sensitive information to someone they think is legitimate, give physical access or data access to an illegitimate individual, or click on a malicious link (thereby downloading malware that can give crooks access to sensitive data and/or the ability to lock down critical files). Phishing and social engineering are still the top vulnerabilities at most organizations, and so it's critical these tests are combined with regular, organization-wide training.

Protect supply chain and payment related processes internally, as well as in partnership with your banks and technology providers. Hospital and healthcare network employees should proactively monitor their online accounts, put automated fraud detection tools in place (e.g., Check Positive Pay and ACH Positive Pay), and convert fraud-prone paper check payments to electronic methods. Administrators should also use online entitlement controls to separate duties and enforce "need only" access for employees. But one of the most critical fraud payment prevention tools is also among the most basic. "Always verify account-change requests by picking up the phone and confirming the change with a known contact before sending payments," Stasiukonis said. He explains that criminals have gotten very sophisticated at creating "drop accounts" at domestic banks that look very legitimate, and he knows of several cases where payments in the millions of dollars were sent to such accounts and never recovered.



Even with all these precautions, however, it's still possible to fall victim to a cyberattack. That's why every healthcare organization "needs a realistic disaster response plan in place," Tarte said. Indeed, being able to respond quickly is more vital than ever. The federal government's recent warning to healthcare providers notes that some recent healthcare sector victims have experienced very short periods of time between initial compromise and activation – even under a few hours. Tarte suggests that organizations consider performing a ransomware

> **Research by the Ponemon Institute, a consulting firm, has indicated that only about 15% of healthcare organizations have adopted the technology, training and procedures necessary to manage the cyberattacks they regularly face.**

tabletop exercise to help identify gaps in their response plans or where additional controls may be required. These exercises walk through the chronology of a security incident with key members of IT, security, business, and management to determine how they would respond as events unfold. "This is a real eye opener for some companies," Tarte said.

Besides having cyber insurance, healthcare providers and networks should consider having forensics experts on call that can help respond to ransomware and related attacks, get systems and patient care up and running, and perhaps even act as a ransom broker. Having a ransom broker is especially important since banks are often restricted in their ability to facilitate ransom payments. "It's really important to understand what your bank can't do," Tarte said. Most banks can't transact on cryptocurrency exchanges (the preferred method of payment among hackers), and federal and state laws do not allow ransom payments if the cybercriminal is linked to any of 50 or so groups tied to terrorism or certain other crimes. Stasiukonis, whose firm has acted as a ransom broker, added that banks are understandably cautious. "It's really serious. We've had banks make us certify that we will not negotiate with any of these 50 groups."

While planning for a cyberattack might seem unnerving or even a bit fatalistic, taking these steps is vital given the scope of the problem, the ever-changing nature of the threat and the potential life and death ramifications. Cybercriminals will continue to see healthcare providers and systems as tempting targets, and these organizations need a robust strategic response.

Beyond these tactical steps, cyberattack prevention and response should be an issue that is discussed at the management and board levels, with a focus on how to put appropriate funding in place to implement required plans. ■

[i] 2020 AFP Payments Fraud and Control Survey
[ii] ACFE Fraud in the Wake of COVID-19: Benchmarking Report, December 2020
[iii] Guardian Digital
[iv] ACFE Fraud in the Wake of COVID-19: Benchmarking Report, December 2020

People's United Bank, N.A. is a subsidiary of People's United Financial, Inc. (NASDAQ: PBCT), a diversified financial services company with $61 billion in assets and an A- rating from S&P. Founded in 1842, People's is a premier, community-based bank in the Eastern U.S. offering commercial banking, retail banking and wealth management services through a network of over 400 office locations.

Speak with an
experienced banker today.

☎ 1-800-894-0300
www.peoples.com/healthcare