SOLIDIFYING HEALTHCARE'S SECURITY POSITION

Provider organizations continue to be prime targets for cybercrime – but adopting the right solutions, as well as a strong cyber-resilience stance, can help protect sensitive patient data.

To meet COVID-19 mandates and still serve their patient populations, healthcare organizations had to quickly pivot to support telehealth and remote work options. While such moves helped providers ensure vulnerable patients could still receive the care they needed outside the four walls of the hospital, they also increased organizations' susceptibility to malware, phishing and other cybercrimes.

"We now know there was a 45% increase in cybersecurity attacks targeting healthcare organizations globally, with the specific intent to disrupt diagnostics, supply chain, therapies and then vaccines," said Daniel Colling, BSN, RN, Global Leader of HP HEALTHCARE Industry Solutions.[1]

"With healthcare working in this new virtual environment, the controls just weren't there to eliminate the risks – and the number of attacks just skyrocketed," he pointed out.

As doctors, nurses and other healthcare personnel started to work from home, connecting to unsecured networks in order to provide telehealth and other healthcare-related services, the number of network endpoints open to potential attack grew exponentially. With so much sensitive patient data shared on these endpoints, it is likely no surprise that, even in the midst of a major public health crisis, cybercriminals took full advantage.

While working to combat the novel coronavirus, healthcare organizations also found themselves having to defend their networks as they were attacked on multiple fronts.

> "We now know there was a 45% increase in cybersecurity attacks targeting healthcare organizations globally, with the specific intent to disrupt diagnostics, supply chain, therapies and then vaccines."
>
> 
>
> **Daniel Colling, BSN, RN,** Global Leader of HP HEALTHCARE Industry Solutions

The impact is significant across the globe

600% increase in malicious emails during the pandemic, according to the United Nations disarmament chief.[2]

Cybersecurity attacks targeting healthcare organizations across the globe have almost doubled during the pandemic, the Associated Press reported.[1]

"We saw that hackers were trying to get into networks through widespread email phishing and social behavioral attacks – much like before the pandemic," said Colling. "But we also saw a shift where cybercriminals started targeting internet of medical things (IoMT) devices – the devices like infusion pumps or respirators that patients needed to receive life-saving care at home. Most of these IoMT devices just don't have the security protocols in place to protect them and it left many hospitals much more open to attacks."

Given the wealth of sensitive patient and financial data healthcare organizations process and store, the increase in targeted attacks was and remains of great concern. Universal Health Services, for example, had to shut down its entire network and move to paper charting after a debilitating malware attack in September 2020 that limited the organization's ability to treat patients in the middle of a global pandemic. Not only do network breaches have the potential to interfere with care delivery – they also come at an overwhelming cost to provider organizations.

According to Accenture and the Ponemon Institute, the estimated cost of a security breach is $13 million, including the information technology expenses involved with ameliorating the resulting network issues and recovering lost data as well as any regulatory fines, civil actions or other costs associated with the loss of patient data.[3]

"The costs involved to deal with a breach are a real challenge for organizations," said Colling. "In 2020, 18 million patient records were impacted by a cyberattack.[4] You have your fines and the cost of identify theft monitoring services for all those patients. But you also have a loss of trust and brand value. It all adds up."

With so much at stake, and the expectation that healthcare organizations will continue to support hybrid care delivery models into the future, it is imperative that hospitals and other provider organizations solidify their cybersecurity position – and implement strategies that promote cyber-resilience, or the ability to prepare for, respond to and recover from cyberthreats. Colling said this starts with educating personnel about cybersecurity protocols.

According to Accenture and the Ponemon Institute, the estimated cost of a security breach is...

$13 million, including the information technology expenses involved with ameliorating the resulting network issues and recovering lost data as well as any regulatory fines, civil actions or other costs associated with the loss of patient data.[3]

"Unfortunately, we can be our own worst enemies when it comes to letting bad actors into the network," he said. "So, educating people about cybersecurity policies and training them to understand your security and compliance protocols is very important."

Colling added that taking a true cyber-resilience stance also includes investing in hardware and devices with built-in security protocols to protect endpoints, the adoption of secure, zero trust log-in and authentication technologies to minimize visual hacking and the utilization of artificial intelligence (AI) algorithms to streamline network monitoring and management. Strengthening an organization's cyber-resilience needs to be a multi-pronged effort.

"You want to have an ecosystem that can support both privacy and security but also improves the efficiency of the nurse and physician as they go about their work," he said. "Unfortunately, it's not a matter of if, but when your network will be attacked. That means you need to move beyond purely defensive strategies with your network and move to a place where you can truly exercise cyber-resilience. When you have the right security posture in place, you know that you can isolate any attack that occurs and quickly recover from it without any disruptions to patient care – even with care continuing to be provided remotely."

Sources

1 Check Point. 2020. *Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again*. Check Point Blog. https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/.
2 Associated Press. May 23, 2020. *UN warns cybercrime on rise during pandemic*. https://apnews.com/article/technology-asia-pacific-latin-america-africa-cybercrime-6ba6af57fd96e25334d8a06fcf999e7f.
3 Accenture and the Ponemon Institute. March 6, 2019. "2019 Cost of Cybercrime Study". https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.
4 AAMC. July 20, 2021. "The growing threat of ransomware attacks on hospitals." https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

Produced by HIMSS