Healthcare: Providers Protect Patient Data and Their Reputation

Cybersecurity Series

By Gary Lynch , Chief Technology Officer Healthcare, Verizon Business

The consequences of healthcare data breaches can be severe, including compromising confidential information, such as patient records or intellectual property (IP). Breaches can lead to compromised care, significant financial losses and reputational damage. The impact of a breach can even be life-threatening in the event hackers are able to gain access to systems needed for the administration of care, forcing caregivers to tend to their patients without the life-saving systems they may typically use to perform their duties. As such, the specter of healthcare breaches looms large in an industry that is rapidly driving towards digital transformation and changing how and where care is provided. Healthcare providers must implement cybersecurity protocols to protect their patients, their IP, and their reputation.

People make a lot of mistakes

Miscellaneous errors are among the most prevalent patterns in healthcare, according to Verizon's 2023 Data Breach Investigations Report (DBIR). A common miscellaneous error is misdelivery, an action type in which data is mistakenly sent to an unintended recipient. Misdelivery, a common error type in this sector, may not be so harmful in other settings, like a corporate environment that sees a marcomm email go astray, but in healthcare settings, the consequences can be more serious.

Misdelivery might be an email with a spreadsheet containing sensitive employee or patient information being sent to a much wider distribution than originally planned. Another example of misdelivery is a mailing error in which paper documents are placed in such a way that sensitive information appears in the envelope's clear window. Information could end up in the wrong hands without the need for tampering. At the

very least, patients might be upset, which could affect a healthcare provider's reputation.

It's worth noting that the human element, the reason misdelivery takes place, makes up the overwhelming majority of incidents, and is a factor in almost three-quarters (74%) of total breaches. It's one of the most significant cybersecurity considerations, if not the most important, and has a bearing on most action types, including the following.

Holding machines hostage

The cost per ransomware incident more than doubled over the past two years, creating huge financial burdens for victims. The 2023 DBIR reports on how 95% of incidents that experienced losses as high as $2.25 million to rectify. Recent years have also seen a marked rise in frequency: the number of ransomware attacks in the last two years was greater than the previous five years combined.

The healthcare sector in particular is plagued by ransomware gangs, a group of threat actors who work in concert in order to execute a ransomware attack. Increasingly, healthcare providers have become targets for ransomware, as they are in possession of sensitive information as well as critical systems and devices that can fetch large sums of money for hackers. Medical devices connected to the network, such as X-Ray machines and heart rate monitors, can be targets. Once one device is infected, lateral exposure can become a risk. If a group of infusion pumps are hacked, it may be easier to pay the ransom than operate without potentially life-saving medical devices until they're successfully reconfigured.

People are the problem, but they're also the solution

As mentioned above, the human element plays a role in the majority of incidents and breaches. Humans are responsible for misdelivery and are often a factor in ransomware attacks, since social engineering tactics are typically used to plant malware in an endpoint or wider network. Training can help staff identify common phishing and social engineering techniques that often lead to ransomware deployment.

Keeping staff apprised of updated security policy can also help reduce misdelivery. Training staff with regular tests on how to spot and report common phishing or social engineering threats can help reduce future incidents. A security policy should explain how employees should handle critical data, how it should be shared, if it can be shared externally, and who can access it.

Zero-trust strategy is a philosophy

Training employees can be effective at minimizing the impact of the human element, but it's unrealistic to expect to eliminate all human errors. A zero-trust cybersecurity strategy, which seeks to authenticate, authorize and continuously validate users, acknowledges that security threats can come from anywhere, including within an organization. This model can be effective at thwarting breaches and preventing

incidents from becoming much larger events. This can be useful for containing threat actors who use pretexting, masquerading as a trusted user, to spread throughout a network.

Secure while digitizing

As medical facilities continue to digitize, more medical devices and equipment will be connected to networks via IoT technology. Connected devices offer tremendous advantages, including maintenance and resource utilization. Unfortunately, they can also create new points of entry for threat actors.

Healthcare providers should continue to connect their systems and devices, but they need to invest in cybersecurity as they do. The cybersecurity of these devices in particular has not matured proportionally to their implementation. To benefit from smart healthcare, they must prioritize protecting devices and systems as they connect them.