The Healthcare Industry's Biggest Cybersecurity Threat Is Internal

Cybersecurity Series

By Gary Lynch, Chief Technology Officer, Healthcare, Verizon Business

While external threat actors targeting medical devices like infusion pumps and pacemakers can have devastating consequences, these incidents are relatively not as common compared to other network intrusions and data breaches. Surprisingly, the most significant cybersecurity threat the healthcare industry faces isn't from external hackers – it comes from within their own walls.

The (non) malicious internal actor

The majority of data breaches (70%) are the result of an internal actor's actions, both malicious and non-malicious, according to this year's Data Breach Investigations Report. Malicious internal activity had been on the decline since 2018 until last year, when the five-year trend began to reverse itself. Privilege misuse, which didn't crack the top three last year, holds the second-place spot this year.

It's difficult to pinpoint the cause of this regression. It may be that there is a growing demand and a larger financial motivation for obtaining a medical research facility's sensitive information, for instance, or it may be that the rise of private 5G and MEC within the healthcare space has made it more difficult for threat actors to break into hospital networks. The latter would compel threat actors to seek accomplices that might help them bypass security. Whatever the case may be, we would all do well to monitor this trend in the coming years.

And yet, innocent mistakes surpass ill intent, with miscellaneous errors emerging as the top pattern this year within the healthcare sector. The most common error is misdelivery, which refers to sending information to an unintended recipient, whether by electronic or physical correspondence. Loss, which refers to the misplacement of paper documents, is the second-most common miscellaneous error.

verizon business

The growing interconnectedness of the healthcare ecosystem
It's clear that hospitals face a major challenge internally, but that doesn't mean they can neglect external threats, which account for almost a third of data breaches in the healthcare industry. The external threat is exacerbated by the growing complexity of the data ecosystem.

In today's healthcare system, hospitals engage a variety of third parties in order to outsource work, ranging from billing to lab work. A hospital may deal with multiple labs for a range of tests. Labs collect an array of data, including patient information, insurance, payment details, and so on. Every time a hospital communicates with one of these third parties, opportunities arise for threat actors to exploit. Sometimes the data breach may not even be malicious, instead the result of a software glitch that replicated across interdependent systems.

The rise of telehealth over the last five years has further extended the distance confidential patient information must travel. According to this year's Mobile Security Index (MSI), almost two-thirds (64%) of healthcare respondents said their organization allowed remote access to electronic patient records. This practice is increasingly common. It can also be seasonal, as in while doctors are on vacation. Smaller practices are less likely to have strict cybersecurity practices. The more distributed patient records are across the data supply chain, the greater the risk of compromise.

The importance of access controls and shared responsibility
The reality of today's data supply chain, regardless of industry, is that it's increasingly interdependent. This reality ratchets up the urgency of the dynamic between an organization and the partners, vendors, and other third parties it chooses to work and share data with. In other words, your cybersecurity is only as strong as the weakest link within your network. This is doubly urgent for hospitals, which deal in highly sensitive information.

Most of the data breaches hospitals experience, whether precipitated by internal or external actors, are the result of errant data, that is, the wrong person gaining access to and sharing the wrong information. This could be a corruptible employee that procures valuable data in order to sell to an external party. It might be the head of a department innocently emailing sensitive research to an unintended recipient. It could be a medical laboratory outsourcing data processing or medical billing to a vendor that gets hacked.

Hospital networks are becoming more robust and more secure with private 5G and Edge configurations. The vulnerabilities of such a network have much less to do with the network itself and more to do with the processes in place with sharing data internally and externally. Hospitals must implement more rigid access controls to minimize malicious and non-malicious internal actors, and they must invest in shared responsibility agreements in order to keep their partners' information handling processes to an acceptable standard.

At the end of the day, it doesn't matter if a breach is caused by a malicious or a non-malicious actor, or whether the breach was intentional or caused by a simple mistake. The damage is malicious. The key to cybersecurity in the healthcare sector is to ensure strict guardrails are in place to help protect people from themselves.

verizon business