COLLECTIVE INTELLIGENCE

Healthcare Cybersecurity Incidents: What We've Learned

Mark Seifert and Siobhan Gorman
October 2024

Healthcare organizations reported more ransomware attacks than any other critical infrastructure sector in the last year. Healthcare also had the highest average data breach costs: approximately $10 million per incident. Drawing on our experience responding to numerous incidents affecting healthcare providers, insurance companies, payment processors, pharmacies, hospitals and more, here are our top five recommendations for executives in the sector.

Calibrate incident response plans to your role in the healthcare delivery chain

Your organization's proximity to frontline patient care is a key factor in your incident response strategy. Ensuring patient safety and access to care are critical considerations in any cybersecurity incident affecting the healthcare sector. Even if your organization does not have a direct role in patient care, your incident response strategy should anticipate potential downstream effects and the needs of providers so they can address patient concerns as effectively as possible.

Align on the recommended cascade of information in advance, and pressure test it through crisis simulations

Complexity of relationships within healthcare systems adds to the challenges of providing updates. During a breach, organizations are judged on their ability to get accurate information to key audiences quickly. However, healthcare systems are built on extremely complex relationships. Inside a hospital, for example, you need to consider the order in which you communicate with department chiefs, attendings, residents, nurses, support staff, and vendors—in line with the hospital incident command system. Third-party vendors and service providers that support healthcare infrastructure also need to map their network of customers, so they know when and how to reach them in the event of an incident.

Create more redundancies and workarounds for accessing your critical systems and data

Interdependencies exacerbate operational disruption. No one organization is responsible for healthcare. The dependencies among organizations mean the entire system is only as strong as its weakest link. Healthcare systems bring together organizations of all sizes and technical maturity levels. Even if your organization has taken measures to strengthen network security and resilience, your ability to provide critical services could be at risk if there is a cybersecurity incident anywhere in the healthcare delivery chain.

Review the steps your organization is taking to protect patient data before a crisis hits

Breaches of patient data can have severe consequences. Patient data is deeply personal and varies widely—from payment records to diagnoses, treatment plans, and medical imaging. Data breaches can result in significant emotional harm to patients and reputational harm to institutions. Recently, a US-based hospital network paid $65 million to settle a class action lawsuit following a data breach where cybercriminals published nude images of cancer patients on the dark web. Examples like this one demonstrate how cybercriminals are weaponizing health records and other sensitive data. As more patient data is leaked, the risks of intentional and unintentional misuse increase. Traditional support resources such as credit monitoring and identify theft protections do not address the emotional toll of a breach. Regularly review the data your organization holds and encrypt sensitive data at rest and in transit.

Engage with government as both regulator and customer

Keep an open line of communication with government agencies during the investigation and regulatory notification process and prepare for extensive one-on-one engagement.

Governments are not only responsible for regulating the healthcare industry but also play a critical role in financing public health programs and providing care to government employees, military members, and veterans. While there are important differences between the US system and consolidated national healthcare systems around the world such as the UK National Health Service, all organizations in the health sector should be prepared to engage with many government authorities at the national and local levels during a breach. Direct engagement tends to lead to fewer surprises in how agencies and their leaders characterize cyber incidents publicly.

To continue the conversation

Mark Seifert

Partner, Cybersecurity, Data and Privacy Global Co-Lead, Washington, D.C.
mseifert@brunswickgroup.com

Mark helps clients prepare for and respond to cybersecurity incidents. A certified privacy professional and a former regulatory attorney, Mark offers insights and practical advice on addressing complex cybersecurity and privacy issues from preparation to response to recovery.

Siobhan Gorman

Partner, Cybersecurity, Data and Privacy Global Co-Lead, Washington, D.C.
sgorman@brunswickgroup.com

Siobhan concentrates on crisis, cybersecurity, public affairs and media relations. She works on corporate crises and corporate reputation projects across a range of industries. Tapping her longtime journalism experience, she regularly advises clients on media relations issues and conducts media training for executives.