BECKER'S HOSPITAL REVIEW
Guidehouse

The impact of cyberattacks on revenue cycle management: Action steps experts recommend taking now

Healthcare organizations are experiencing a record number of cyberattacks and data breaches that can disrupt clinical operations, negatively impact the patient experience and affect the revenue cycle. As attackers become increasingly sophisticated and enterprises more broadly adopt technology, it's essential that healthcare leaders know how to skillfully navigate increased risk and exposure.

To better understand the impact of cyberattacks on revenue cycle management and what health systems can do to mitigate risk, Becker's Healthcare recently spoke with revenue cycle and cybersecurity experts at Guidehouse: Ian Stewart, partner, managed services; and Erik Pupo, director, commercial health IT advisory.

Former health system executives, Mr. Stewart and Mr. Pupo shared insights and best practices to prevent cyberattacks, reduce risk and respond to potential attacks.

Many healthcare organizations are not prepared for cyberattacks

During the first half of 2024, the healthcare industry experienced more than 300 data breaches, affecting more than 45 million people. These data breaches include costly, high-profile ransomware attacks that impacted major healthcare organizations.

Mr. Pupo said these incidents have proven to be a wake-up call in the industry. "The majority of healthcare organizations do not have as good of a grasp on their cybersecurity posture as they may have thought even six or 12 months ago," he said.

> **"The majority of healthcare organizations do not have as good of a grasp on their cybersecurity posture as they may have thought even six or 12 months ago."**
>
> **Erik Pupo**

Mr. Stewart also noted that recent cybersecurity incidents have revealed many healthcare organizations lack proper processes and response plans for cyberattacks.

"We've seen 'never events,' that we thought would never happen, actually happen four times in a row, back to back," Mr. Stewart said.

> **Recent cybersecurity incidents have revealed many healthcare organizations lack proper processes and response plans for cyberattacks. "We've seen 'never events,' that we thought would never happen, actually happen four times in a row, back to back."**
>
> **Ian Stewart**

Cyberattacks impact patient access, patient experience and revenue

When a cyberattack affects a healthcare organization's back-end systems, significant operational disruptions can occur – from patient scheduling to being forced to turn off entire digital infrastructures. These disruptions impact patients and providers, Mr. Stewart said.

"There are facilities that have lost their scheduling system, their EHR and ultimately their ability to treat patients in real time," Mr. Stewart said. "It's a huge issue."

For example, if a hospital is unable to access and use many of its critical computer systems for a sustained period of time after a breach, they'll likely need to switch to completely paper-based processes. This hinders the ability to understand which patients are scheduled for surgery, as well as access medical information.

Further, a lack of back-up systems can impact patient care, safety and experience – as well as revenue. It also increases an organization's costs, as facilities may need to hire a significant number of people in the revenue cycle to enter information manually.

Investments in cybersecurity can be misguided

Per Guidehouse's 2024 Health System Digital & IT Investment Trends Report, 55% of providers cited cybersecurity as their top investment priority in 2024. However, just spending more money on cybersecurity doesn't lead to better outcomes.

"More money doesn't necessarily mean more security," Mr. Pupo said. "We're definitely seeing a trend that more spending is not going to be the primary solution moving forward."

What matters is how organizations spend their cybersecurity investments.

To maximize outcomes, Guidehouse identified several key action steps:

- **High-caliber talent:** Healthcare organizations need to hire top cybersecurity talent to focus on incident prevention. This will enforce the protection of every possible entry point and minimize risk.
- **Automation and AI:** This includes automating processes, such as data analysis and security alerting of a system's digital infrastructure to be more proactive.
- **Redundancy and back-up systems:** Cloud-based systems especially need redundancy. In the event of a successful cyberattack, an organization's operations might grind to a halt and cash flow can fall to zero. An example of duplication in the revenue cycle is having redundant payment and posting systems.

Actions to manage risk and prevent attacks

Based on Guidehouse's experience working with healthcare organizations, the following steps can help prevent cyberattacks or minimize their impact if an attack occurs.

- **Network segmentation:** This involves isolating different devices and systems on separate networks. That way, if one device or system is compromised, the entire network is not affected.
- **Perimeter protection:** This involves a robust network monitoring protocol and intrusion detection prevention. In Mr. Pupo's view, many providers do not invest adequately in this critical area.
- **Training and education:** Organizations often overlook the importance of robust, holistic training. This includes creating a culture of security involving clinical teams, front-end employees and those who work on the revenue cycle. Everyone needs to understand the best processes and behaviors to prevent a cybersecurity incident. Equally important is the development of a disaster recovery plan where the whole organization must also understand exactly what to do in the event of an incident.

Why training matters

Mr. Stewart observed that most people in healthcare are educated and compliant with all of the rules surrounding HIPAA – but there typically aren't the same standards or vigilance in protecting revenue cycle information. As a result, if there is a call or an email about something on the billing side, organizations often don't have consistent, standard operating procedures and a programmatic way of working. This makes organizations susceptible to data breaches in revenue cycle operations.

"You've got to train everybody, everywhere, all the time to be on the lookout for something that might be suspicious," Mr. Stewart said. "It is necessary to stay vigilant every day to try to identify threats early and often."

> **"You've got to train everybody … to be on the lookout for something that might be suspicious. It is necessary to stay vigilant every day to try to identify threats early and often."**
>
> **Ian Stewart**

Additionally, it's not enough to have prevention and incident response policies and to provide education on these policies; it is essential to constantly test, simulate and repeatedly run incident response exercises. In Guidehouse's experience, preparation and testing enable organizations to respond quickly and minimize damage in the event of a data breach.

AI and the future of regulations in improving cybersecurity

Predictive analytics, AI and large language models can be used to forecast potential security breaches and create preemptive measures. Healthcare organizations can also use AI to identify potential unusual security patterns and anomalies.

In the revenue cycle, AI can help to streamline coding and billing and authenticate information through validated augmented intelligence. "Coders and billers can use AI to validate that they are correctly entering information, which can eliminate some human error," Mr. Pupo said.

In striving to improve the status quo, various regulators are creating cybersecurity regulations that often conflict. Mr. Pupo expressed hope that there will be more uniformity in these regulations to enable vendors to work toward an understandable minimum bar for security.

With deep knowledge of the healthcare industry's operational and financial risks, Guidehouse brings a unique understanding of where processes can be improved and technology can be applied to reduce risks. Guidehouse also has significant expertise helping healthcare organizations resolve incidents by augmenting revenue cycle teams, adding appropriate technology, revising processes and quickly developing effective workarounds.

To learn more about Guidehouse's cybersecurity and revenue cycle expertise, visit: **http://www.guidehouse.com/RCM** and see the article: **The After effects of Large-Scale Healthcare Ransomware Attacks.**

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. Guidehouse Health helps providers, government agencies, life sciences companies, employers, payers, and other organizations modernize and innovate healthcare services, finances, and operations. By combining our public and private sector expertise, we assist clients with addressing their most complex challenges and navigating significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Ranked 2023's 3rd largest healthcare consulting and healthcare IT consulting firm by Modern Healthcare, Guidehouse has earned 19 Best in KLAS® awards. For more information, visit www.guidehouse.com/industries/health.