



Beyond Data Breaches: High Stakes in the New Threat Environment

Why healthcare organizations can't simply rely on technology to guard their data

As Mike Milliard, Executive Editor at *Healthcare IT News*, can tell you, cybersecurity isn't just about protecting patient data anymore. While guarding privacy and keeping protected health information (PHI) off the dark web remain top priorities, the stakes are now even higher. A cyberattack can take a hospital offline for days, weeks or even months. And the subsequent delays and disruptions to care pose serious risks to patient safety.

"I've been covering this space for more than 12 years, and as recently as 2014, we were not talking about ransomware. But this year, *Healthcare IT News* has already covered at least two stories of patient deaths linked to attacks," said Milliard in a recent HIMSS webinar, "Beyond Data Breaches: High Stakes in the New Threat Environment," sponsored by 11:11 Systems and Veeam.

Milliard was joined by Hazel Chappell, Founder and Digital Managing Partner at ishca health and Brian Knudtson, Director of Cloud Market Intelligence at 11:11 Systems, in a conversation around the new threat environment. They discussed how healthcare organizations can protect against various cybersecurity scenarios, build resiliency, respond to attacks effectively and recover as quickly as possible when necessary.

While each speaker brought a unique perspective to the conversation, the trio was completely in agreement on this point: careful planning and a multilayered approach to prevention and response are essential for defending against healthcare's mounting cyber threats.

Arriving at the current landscape

In a career spanning more than 25 years supporting organizations around data intelligence, cybersecurity and change management, Chappell has watched "digital transformation" grow from a buzzword to a vital force in the healthcare sector. And with it, she's seen the value of healthcare data skyrocket.

Still, she would describe 2020 as a year of twin pandemics: "Healthcare organizations weren't only combatting the COVID-19 virus, but also fighting off a tsunami of related cyberattacks."

The COVID-19 pandemic was an overall accelerator: it pushed organizations to adopt telehealth and remote patient monitoring devices *en masse* and to lean on automation to mobilize their remote workforce. In terms of digital transformation, these changes were a long time coming – and necessary to ensure that organizations could maintain patient safety and business operations during an unprecedented time.

Still, these changes exponentially increased healthcare organizations' threat surface. "Not only did we create more data, but we created more ways to attack that data," said Knudtson. "The pandemic made it easier for attackers to slip in unnoticed – or directly through the front door."

But if there was a silver lining to this period, Knudtson noted, it would be that organizations have a newly heightened awareness of the issues. They've seen cyberattacks that paralyze healthcare providers and jeopardize patient care, and now they're looking for the appropriate technology to keep their data safe. "We just need to pair people with the right tech to execute change," he emphasized.



It's not if, it's when. Bad actors only have to win once, but you have to win 100% of the time. So it's best to assume you are going to be breached.

BRIAN KNUDTSON | Director of Cloud Market Intelligence | 11:11 Systems

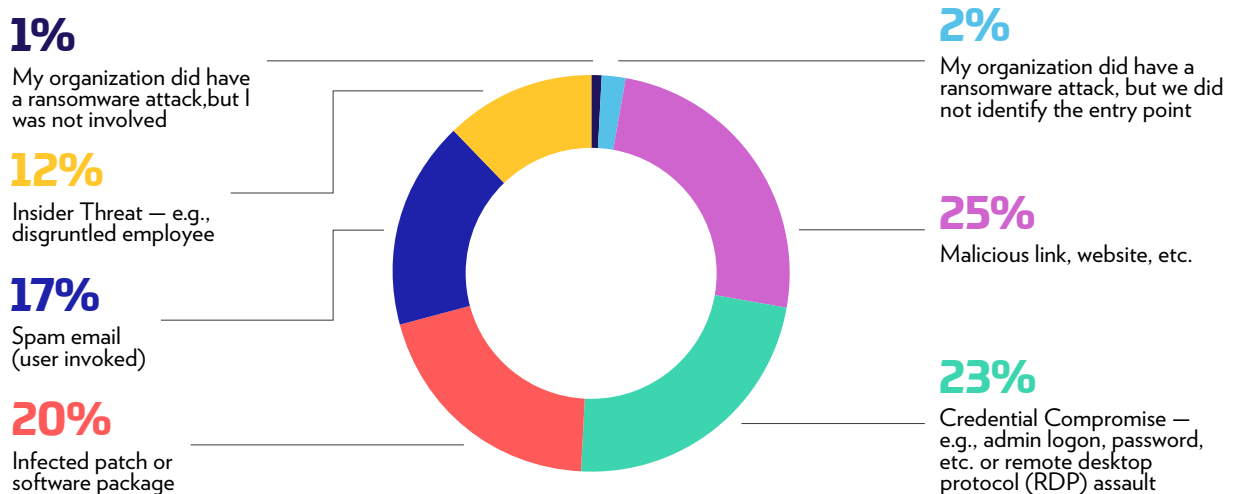
Bouncing back from an attack

As healthcare becomes increasingly cloud-based, Knudtson reports that it's critical to help clients understand where a cloud provider's responsibility ends and where their responsibility begins. "It's important to cover everything: who's in charge of a restore versus who's in charge of a backup," he said. "What level of security settings are we each going to set?" With so many opportunities for attack, it's no longer realistic for organizations to assume they won't experience a breach. "It's not *if*, it's *when*. Bad actors only have to win once, but you have to win 100% of the time. So it's best to assume you are going to be breached," he said.

To that end, Knudtson offered three strategies that organizations can employ when experiencing an attack:

- **Work to identify the breach.** You can't assume your employees will avoid every phishing attempt, so it's important to ensure you can quickly identify an attack (Figure 1). A security incident and event management (SIEM) system can help correlate red flags across the environment, but IT teams must stay mindful of alert fatigue. It can be helpful to work with a managed security service that employs both AI/ML tools and human intelligence to cut through the noise.
- **Know your response.** What is your shutdown plan? "The more automated you can make the process, the better," Knudtson said. But it's a tricky balance. If organizations shut things down too quickly, they may do so in a false-positive situation. In these situations, it's crucial to make these decisions beyond the IT department: what are the needs of other stakeholders, and how will the shutdown affect them? The best response is one that's aligned throughout the entire organization.
- **Establish a disaster recovery plan.** "A security incident can be as disruptive and dangerous as a tornado or hurricane, so your organization's business continuity and disaster recovery plans need to account for cyberattacks," Knudtson advised. For example, 11:11 Systems leans into its partnership with Veeam, a backup and disaster recovery (DR) software vendor. "It may seem like you're duplicating effort, but these two approaches have very different goals in the end," he said. "Backups should not be relied upon to get hundreds of machines back up and running. That is the realm of replication and DR."

Figure 1. Thinking about the most significant ransomware attack your organization suffered in the last 12 months, how did the ransomware enter your organization's environment?



Source: 2022 Veeam Data Protection Trends Report



People need continuing support and guidance to understand the landscape and to employ the right technology for undertaking risk.”

HAZEL CHAPPELL | Founder and Digital Managing Partner | ishca health

Building a culture of security

While innovations in cybersecurity technology can offer organizations protection from incoming attacks, Chappell argued that technology can only go so far without the correct people in place to implement change.

Since 2015, Chappell has been part of the HHS 405(d) Program and Task Group, a collaborative effort between industry and the federal government to provide consensus guidelines, practices and methodologies that can strengthen any healthcare organization's security posture.

“My biggest takeaway from this work is that we're all in it together. This isn't an IT issue. It's about embedding cybersecurity within the culture. Your organization must stay informed and work as a team through various approaches to mitigate cyber risk,” she said.

Chappell recommends establishing internal communities within your organization that collaborate on response and recovery plans and review these methods for improvement after any incidents. She hopes that the work accomplished by HHS 405(d) can guide this process. Quoting a colleague in the program, Chappell added: “We've designed a cookbook for organizations to select their controls from.”

Finding resiliency

Milliard observed that no single solution can shield an organization's entire environment from incoming cyber threats. Increasingly, the same innovations used in defenses – such as

new AI/ML tools – can also provide the arsenal for an attack. Instead, Milliard said, “it will take technology, people and effective change management to maintain resiliency.”

Chappell agreed that healthcare organizations of all kinds shouldn't approach cybersecurity as a tick-box education exercise, but as an enterprise-wide conversation. Ultimately, she believes an organization's biggest threat may be the same as its biggest defense: the workforce. “People need continuing support and guidance to understand the landscape and to employ the right technology for undertaking risk,” she said. “We hear about quantum computing and blockchain use for data security – but how do we know these solutions are suitable for any given organization?”

What works for a hospital may not be the same for a doctor's office, which may not be the same for a health insurance provider. To that end, Knudtson offered this advice: “As you craft your incident response and recovery plans, make sure you understand which tools will work best for your enterprise. The right vendor will architect solutions that consider both your organization's culture and business objectives.”

To learn more about 11:11 Systems and Veeam, go to 1111Systems.com.

11:11 SYSTEMS

VEEAM

About 11:11 Systems

11:11 Systems is a managed infrastructure solutions provider that holistically addresses the most pressing cloud, connectivity, and security challenges of today while preparing businesses for tomorrow. The 11:11 model empowers customers and partners to “Rethink Connected,” by providing fully integrated, fully automated services, activities, and data, powered on a unified platform, that ensures their applications and data are always running, accessible, and protected. 11:11 delivers increased performance and savings to organizations, while freeing up IT resources to focus on the core business. Learn more at 1111Systems.com.

About Veeam

Veeam is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects 450,000 customers worldwide, including 82% of the Fortune 500 and 69% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) and Twitter [@veeam](https://twitter.com/veeam).

