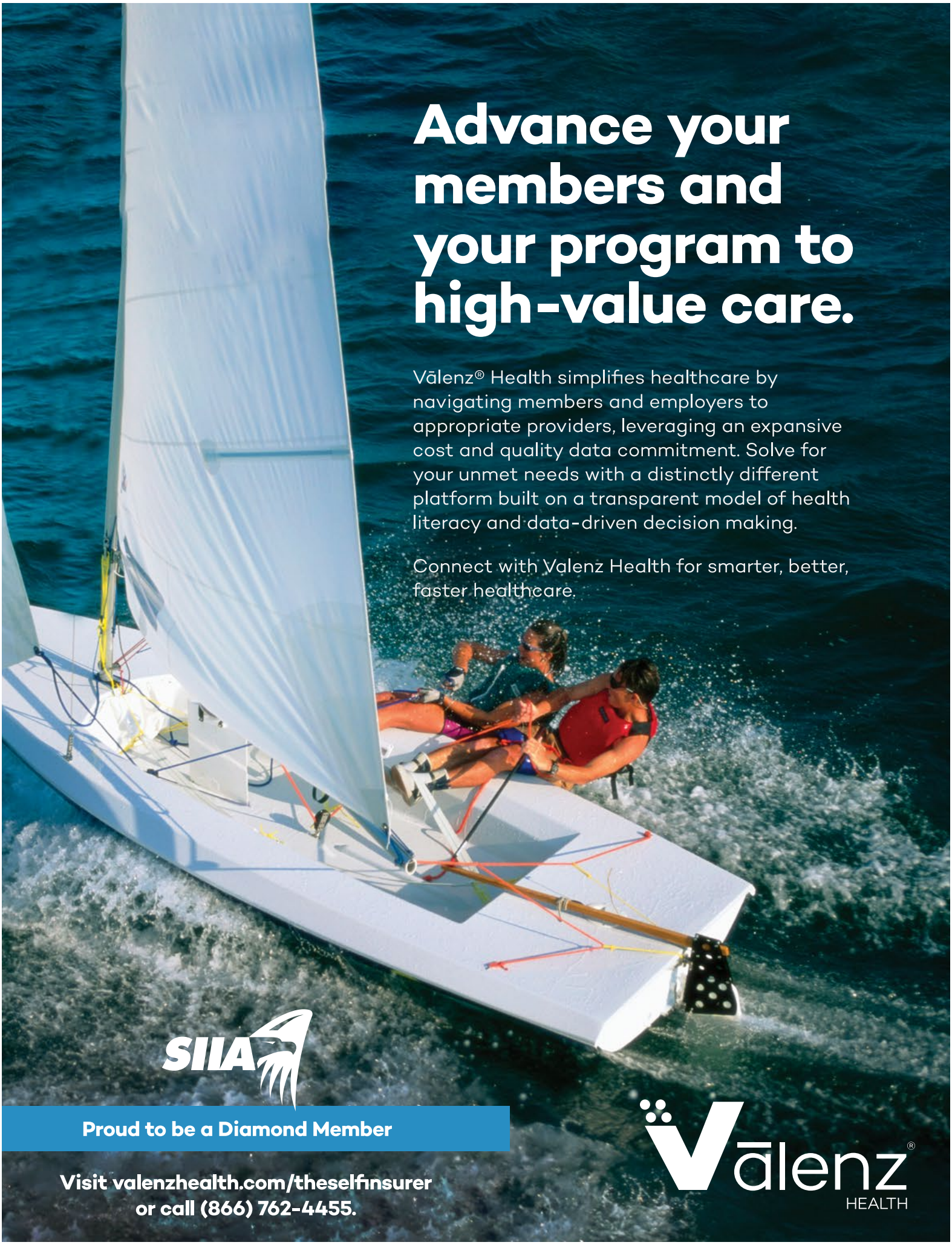
NAVIGATING IN THE NEW AGE OF CYBERSECURITY THREATS

Written By Bruce Shutan

Panic set in at 6 a.m. last July 8 when Phia Group, LLC CEO Adam Russo was contacted by his head of IT, who reported that the healthcare cost-containment firm had been hacked. "The first reaction I had was one of pure despair," he recalls. "It's a company I built from scratch. I didn't know how long we'd be down or if clients would terminate our contracts because they were just nervous about potential liability and breaches down the road."

His company quickly identified a serious cybersecurity threat and shut down all systems across the entire business within two hours of discovering the hack to limit any potential exposure from stolen data. Clients were immediately informed about the incident and the steps that were taken.


Advance your members and your program to high-value care.
Vālenz® Health simplifies healthcare by navigating members and employers to appropriate providers, leveraging an expansive cost and quality data commitment. Solve for your unmet needs with a distinctly different platform built on a transparent model of health literacy and data-driven decision making.
Connect with Valenz Health for smarter, better, faster healthcare.
SIIA
Proud to be a Diamond Member
Visit valenzhealth.com/theselfinsurer or call (866) 762-4455.
Vālenz®
HEALTH

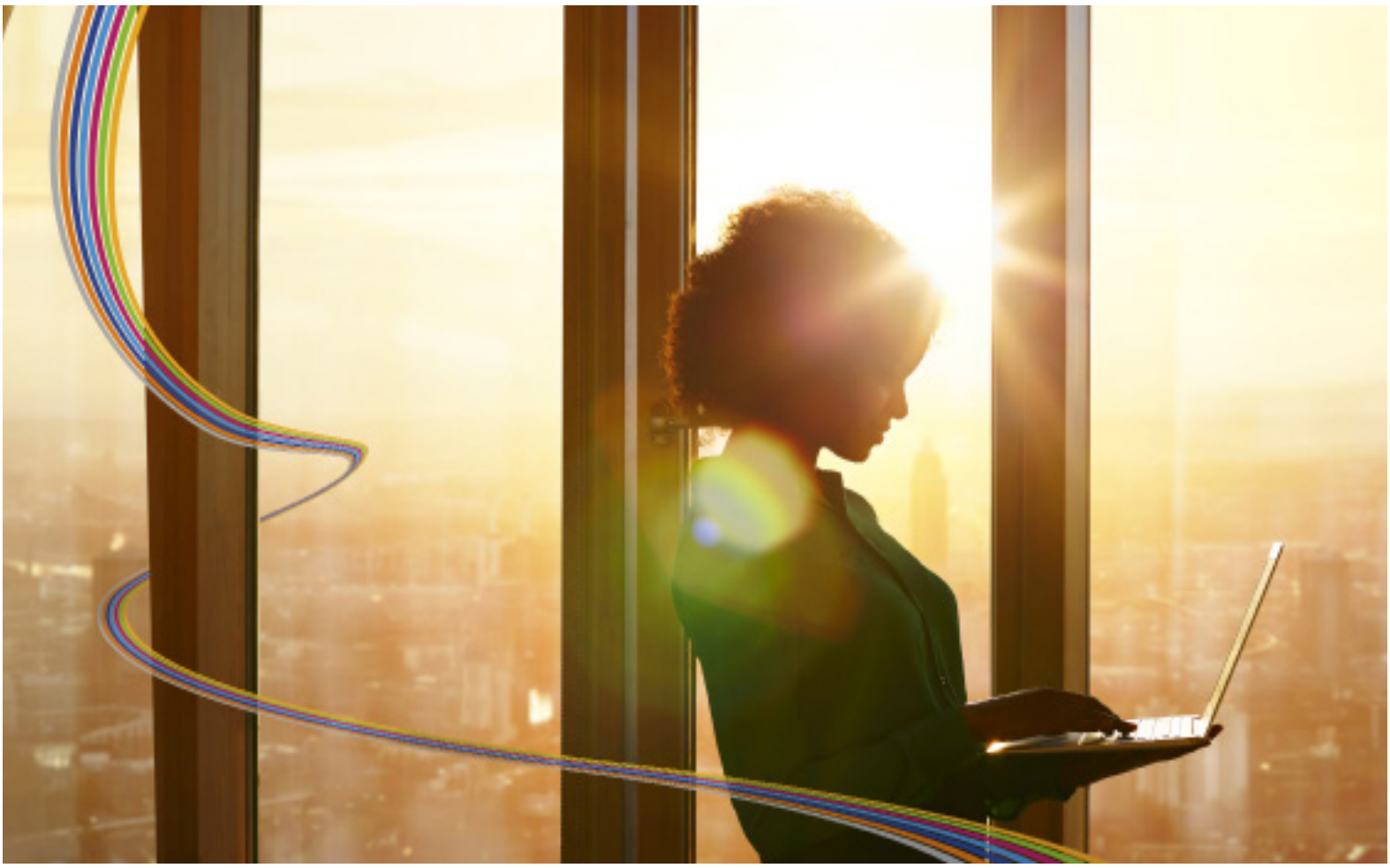
Of course, The Phia Group is not alone in experiencing such a breach. In the past year, 92% of healthcare organizations reported experiencing at least one cyberattack, which was up from 88% in 2023, according to a recent survey by Proofpoint and Ponemon Institute. Of those cyberattacks, 69% reported disruptions to patient care as a direct consequence. Ransomware attacks on this sector rose 128% in 2023, while the April 2024 attack on Change Healthcare compromised information on an estimated 100 million Americans.

Considerable damage has been wrought by large data breaches, which affected more than 167 million Americans in 2023 and set a new record. These large breaches caused by hacking and ransomware skyrocketed 89% and 102%, respectively, since 2019.

FINDING PHISHING EXPEDITIONS

One huge cybersecurity concern involves phishing, fraudulent emails that appear to be from a legitimate source whose aim is to trick the recipient into providing sensitive personal information that may include passwords or credit-card details by clicking on malicious links to download malware to steal data or money. Scores of employees have been duped by this popular scam over the years as methods of deception have become increasingly sophisticated.

"They have become so realistic, looking exactly like you're getting emails from Amazon, FedEx, UPS or any of the major companies, especially during the winter holidays," observes Michael Carrara, CEO of Hi-Tech Health. "Someone may unknowingly click on one of these links, and next thing you know, your internal system and network is compromised."



We Know ... Risk

We study it, research it, speak on it, share insights on it and pioneer new ways to manage it. With underwriters who have many years of experience as well as deep specialty and technical expertise, we're proud to be known as experts in understanding risk. We continually search for fresh approaches, respond proactively to market changes, and bring new flexibility to our products. Our clients have been benefiting from our expertise for over 50 years. To be prepared for what tomorrow brings, contact us for all your medical stop loss and organ transplant needs.

Tokio Marine HCC- Stop Loss Group
A member of the Tokio Marine HCC Group of Companies
TMHCC1242-01/2025

Mike Carrara

His firm has a subscription to KnowBe4, which sends out emails with phishing-scam addresses that the company's internal network is able to detect if employees click on deceptive content. Those random tests are done monthly all year long in addition to a security monitoring report that is reviewed on a weekly basis to detect malicious threats.

It didn't take long for Russo to realize the enormous scope of cybersecurity breaches. "You'd be shocked how sophisticated these criminal enterprises that do phishing are," Russo says. "They are international and earn billions of dollars. The Dark Web has these guys all over the place, and what they do is find just one little crack, and once they're in, they could potentially have the ability to steal data files with personal health information or literally shut down every single thing in your company from your phone system to your network drives, backups, you name it."

What's equally surprising is that it isn't necessarily a random individual on the phone, he explains. It's an entire industry, complete with a sophisticated call center that has its own hold music. "You're given a number," he adds. "They literally treat you as if you're the client, even though they're the ones who hacked into your system."

RESPONSES INSIDE THE BELTWAY

Given that cybersecurity breaches are top of mind for businesses across all industries, legislative and regulatory changes are afoot to address such concerns. For example, the Health Infrastructure Security and Accountability Act,

HCAA's
EXECUTIVE FORUM '25

Deep Roots, Bold Leaders & Soaring Success

The HCAA as an association germinated from the tiniest seed of an idea – that TPA education and advocacy is crucial in nurturing the self-funding industry.

Our Executive Forum continues that tradition, propagating innovation from daring visionaries, and helping our members sprout, grow, and flourish.

REGISTER TODAY!

February 10–12, 2025 | #HCAAExecForum

Bellagio, Las Vegas

S. 5182, introduced in the U.S. Senate in September and referred to the Committee on Finance, includes several important steps to strengthen healthcare cybersecurity. Chief among them: establishing minimum and enhanced standards as well as incident response and recovery plans, expanding risk analysis requirements, holding C-suite executives accountable for complying with security standards, conducting third-party and annual Health and Human Services audits, and funding rural and urban safety net hospitals to implement better cybersecurity practices.

In addition, the U.S. Department of Health and Human Services (HHS) recently proposed a rule that would modify the Health Insurance Portability and Accountability Act (HIPPA) to require health plans and healthcare clearinghouses, as well as most providers, their business associates and other third parties, to strengthen cybersecurity protections for individuals' protected health information.

Greg Garcia

In strengthening the cybersecurity of electronically protected health information, HHS notes that group health plan documents would need to be revised to comply with administrative, physical and technical safeguards.

"Payers were always subject to HIPAA security because they handle protected and electronic health information," explains Greg Garcia, executive director of cyber security for the Health Sector Coordinating Council. "Much of the enhancement references what was published earlier this year as voluntary cyber performance goals, which are now moving to a mandatory status." He says it's difficult to predict how a second Trump term would handle enforcement of regulatory action such as this one, particularly as the public comment period was extended 60 days to March 7.

BREACH VS. INCIDENT

Meanwhile, one of the biggest challenges for businesses is determining the difference between a breach and an incident, according to Carrara. Whenever a cyber threat is brought to someone's attention, he says it's often classified as a breach. But if an email was sent internally with some personal health information, "it isn't really a breach," he explains. "It's an incident, and that's confusing to someone like me. When I hear the word breach, I panic, and usually, after troubleshooting, it's found not to be a breach."

There are several steps Carrara's firm takes once a threat has been identified, which are part of incident-response policies. For example, he says the parties involved may need to be retrained to avoid certain pitfalls or encrypt emails with private health information.

Hi-Tech Health also contracts with a cybersecurity company called Secure Compliance Solutions LLC that filters every transaction that happens on company servers and produces a monthly report. If there are any intermittent or regular attacks that are registered on the server, he says "we might make changes to our firewall policies."

Self-insured clients might compare their internal IT to what his company is doing and come up with their own set of best practices. Carrara notes that statistics on security flaws in software or hardware that have been assigned a unique identifier, known as Common Vulnerabilities and Exposures or CVEs, define the scope and critical nature of cyber threats in security reports, whether it's Windows 11, a server, firewall, patch or something similar, and suggest corrective actions. Examples of less-critical vulnerabilities might involve older servers or software whose patches take a little longer to put in place.

echo
payments simplified

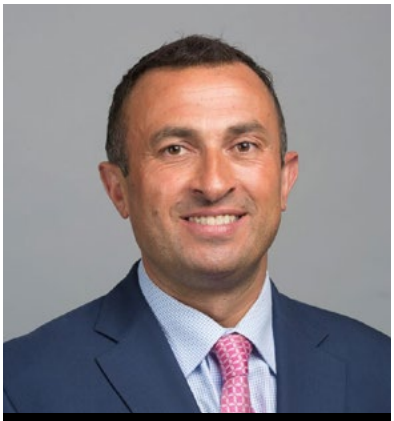
Payment solutions that give you more.

As a leading provider of innovative payment solutions, we deliver payments backed by 25+ years of expertise, enabling **more connectivity, more payment accuracy,** and **more bottom-line savings.**

Learn more at **echohealthinc.com**

Each year, attorneys provide Hi-Tech Health staffers updates on HIPPA rules and regulations, including schooling new employees on clean-desk policies and requirements designed to safeguard sensitive personal information that HIPAA places on third-party administrators (TPAs) as well as his own firm. TPAs and some health insurers use the Hi-Tech Health system to process group health insurance claims.

A related issue that's likely to garner considerable attention is the role of artificial intelligence (AI) in creating more problems as much as solving them. "I think AI is going to present a lot of new challenges for both thieves and the good guys, particularly private information when AI has the ability to reach out and touch so many different sources and pull together that information," Carrara notes.



Adam Russo

His company is exploring AI use for internal customer service for education and training on how to use its proprietary claim system and other issues that don't necessarily require using employee data or private health information.

PREPARATION BEGETS PROTECTION

As Russo unpacked his cybersecurity breach, he was surprised to learn that only about 10% to 20% of clients had a robust team in place that knew what to do, and most of the bigger companies had actually seen potential breaches on a daily basis.

"What I noticed was across our industry, it's a topic that's almost taboo because so many people don't want to talk about their experience. No one wants to say, 'yeah, we got breached,'" he says, adding that there's no standard checklist on how self-insured employers and their partners should identify and respond to a security breach or notify and communicate with clients.

The same applies to something as simple as deciphering how strong passwords should be and how often they need to be updated. "You got people who haven't changed their password in three years, and then you have others who've chosen a sophisticated phrase with 20 characters, some numbers, letters and symbols," he notes.

Ironically enough, preparing for a cybersecurity attack was one of Russo's priorities when he was named chairman of SIIA's board of directors in 2019. Little did he know at the time that those steps, which included devoting sessions to this emerging topic at the annual national conference, would benefit his own company five years later.

It also helps to have the right insurance coverage in place. For example, Phia Group had every imaginable policy prior to its cybersecurity breach that covered anything from cybersecurity and ransom threats to terrorism and hacking – even bribery. If not for those coverages, the company easily could have incurred several hundreds of thousands of dollars in expenses.

What's critical is to quickly identify the perpetrator(s), suggests Russo. Some clients told him they work with vendors who experienced similar breaches that were not resolved for as many as six to nine months, whereas his firm had the right forensic team and processes in place to respond, investigate how the breach occurred and prevent it from happening again.

Many people don't realize that a lot of times, it could be an internal person whose need to pay off gambling debts or other personal problems make them susceptible to selling personal information, according to Russo. "So, you look at everything in your hiring process to avoid an inside job," he suggests. For example, reinforcing the need to establish stronger trust with new hires could mean not granting access or permission to certain information until they're on the job for a certain period of time.

One silver lining in the aftermath of his harrowing brush with a cybersecurity hack is how it elevated his company's standing among prospective clients and

partners. "We took what would be deemed a negative in our industry and actually have used it as a promotional marketing piece on how fast we were able to eradicate the threat and communicate to our clients," Russo says. "I was very proud of my team and how quickly we're able to identify, respond, and get things back online the way they used to be pre-incident."

Bruce Shutan is a Portland, Oregon-based freelance writer who has closely covered the employee benefits industry for more than 35 years.