BY BRAD KADRICH

THE COST OF DOING CYBER BUSINESS

INSURANCE POLICIES ARE BECOMING MORE PREVALENT IN FENDING OFF RANSOM ATTACKS

The prevalence of data breaches and cybersecurity hacks on companies of all sizes is not only not changing, experts say it's getting worse.

Some reports say the number of publicly reported data compromises increased by 78% in 2023 compared to 2022, and that the average cost of the ransom on a data breach hit an all-time high — some $4.45 million — last year.

Small businesses, large businesses … they're all getting hit, and one thing that is changing is the prevalence of — in some cases, requirements for — cybersecurity insurance.

Rich Miller, the president and CEO of Livonia-based STACK Cybersecurity (which recently rebranded from AM Data Service), said two things are true: The size of the business does not matter, and attacks "aren't slowing down at all."

In fact, he said, he tells existing and potential clients the fact of an impending attack is not a matter of "if," but "when." And, as statistics show, a breach could be expensive.

"When you get attacked, it could cost you ransom, it could cost you lost business, it could cost you downtime," Miller said. "If they … lock out all your files and you can't access them, you may be able to restore from a backup and not pay the ransom, but it might take a week.

The answer to that problem, more and more often, is the purchase of cybersecurity insurance. Miller warns that such insurance – like sewer backup insurance in a homeowner's policy – doesn't usually come with a business owner's policy.

"You need a separate cyber policy to do it," he said.

It's getting to the point where there are becoming requirements to carry cyber insurance and requirements to be able to

continued on page 52

get cyber insurance.

Take big businesses like the auto industry, who depend on several tiers of suppliers to make the cars. According to Miller, because big businesses such as the automakers are susceptible to hacks through their suppliers, they're requiring those lower-level suppliers to carry cyber insurance of their own.

"Bigger businesses are starting to demand that their suppliers carry (insurance) so that they're covered," Miller explained. "And … there's a lot of two-way indemnity going on where a bigger business says, 'Hey, if you get a cyber breach and you lose some of my data, you need to indemnify me because you are doing business with me,' and vice versa.

Rich Miller is president and CEO of Livonia-based STACK Cybersecurity.

"We're seeing it more and more, and when you get hit, you need these coverages," he added. "But it's expensive and a lot of businesses don't want to do it."

That kind of decision can cost a company, according to Justin Myers, the president and CEO of the California-based Glenn S. Caldwell Insurance agency.

According to Myers, a supplier who doesn't have insurance and gets breached, and causes a breach in the larger third-party company, has nowhere to go.

"If that client … didn't have cyber liability coverage on their policy, so they really didn't have anyone to turn to," Myers said. "They immediately turned to their IT company and said, wait a second, this individual or this compromise or shut down our system through the cyber-attack, came through your system. So, this manufacturer was kind of left high and dry to deal with it, their system was shut down for several days and they weren't able to conduct business.

"They actually had, in order to get their system back, they had to pay a ransom … several hundreds of thousands of dollars," he added.

Until the last couple of years, companies like STACK left that decision up to their clients, and Miller says perhaps as many as half of them balked.

"There's becoming more demand on the business to have cyber insurance from outside forces," he said.

Miller recalls pitching the idea of cyber insurance to a client, but the client declined. A week later, that same client got hacked. So Miller – trying to help the client – again pitched getting some insurance, and the client again declined.

That couldn't happen now, because STACK requires its new clients to have insurance, or sign a waiver — "I'm not going to pass up a huge contract if they don't, but I'll make them note that they've chosen not to do it," he said — saying they don't want it.

"With us shifting toward the cybersecurity focus when we really dug in and kind of figured everything out, that was one of the shortcomings that we realized we had. We never required it," Miller said.

Having cyber insurance would seem to be a no-brainer, considering these statistics, developed by secureframe.com, a platform that helps companies get and stay compliant to various security and privacy standards:

- The number of publicly reported data compromises increased by 78% in 2023 compared to 2022.
- The average cost of a data breach reached an all-time high in 2023 of $4.45 million, a 15.3% increase from 2020.
- It takes organizations an average of 204 days to identify a data breach and 73 days to contain it.
- Breach notification costs rose to $370k in 2023, a 19.4% increase over 2022.
- Cyberattacks using stolen or compromised credentials increased 71% year-over-year.
- 74% of all breaches include the human element.
- 12% of employees took sensitive IP with them when they left an organization, including customer data, employee data, health records, and sales contracts.
- 98% of organizations have at least

one third-party vendor that has suffered a data breach.

Still, companies often have to be convinced that insurance is a good thing to have.

"We're doing a lot … of educating," said Mitchell Prevost, an agent with Glenn S. Caldwell. "A lot of people are under the assumption that their general liability is covering that with that cyber endorsement. So, we're going out and we're trying to go after businesses that are doing well or may not know the risks that they have."

Prevost recalls a client that specializes in wholesaling – "You wouldn't think right off the bat that there's a high exposure for cyber (attacks)," he said -- but almost 95% of their business is done via email credit … purchasing is done online.

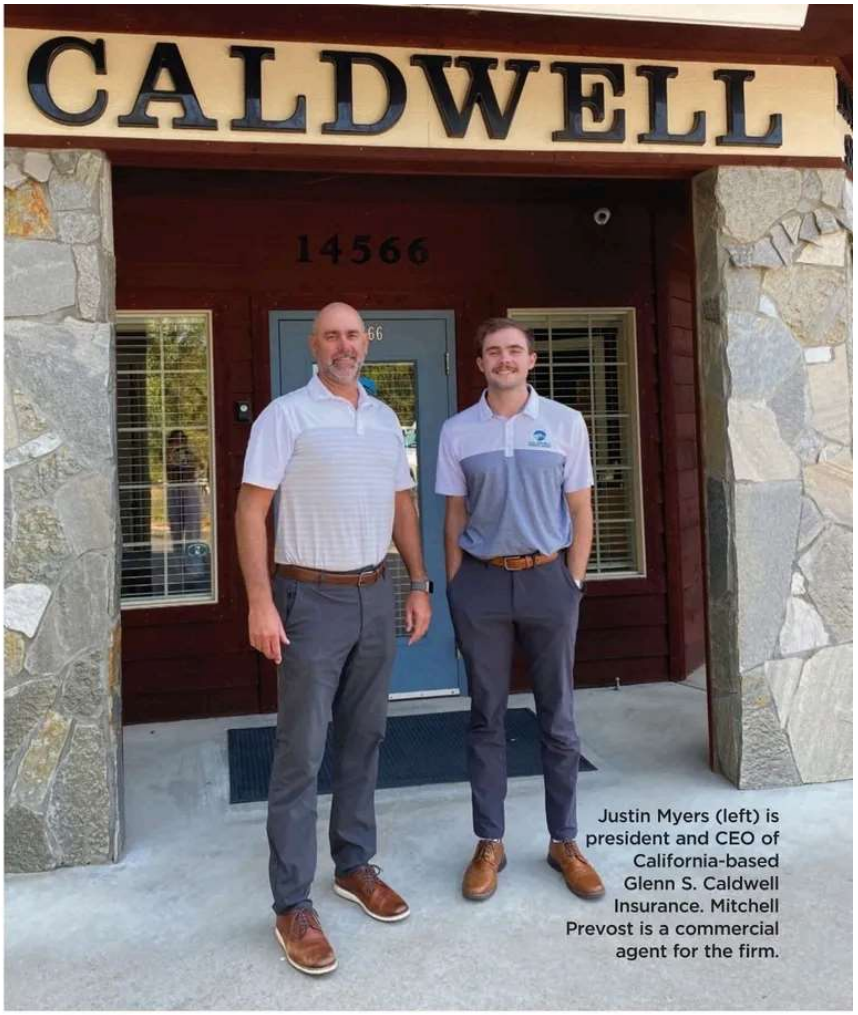
"So, they were happy that I reached out and offered them a cyber policy," he said.

The policies, though, are coming with a growingly stiffer set of requirements themselves in the complexity of the questionnaire most clients have to fill out in order to obtain the insurance in the first place.

The complexity of the questionnaires — they can be as small as a couple of pages or they could be 25 pages or more, according to Miller — depends on the level of policy businesses are seeking. There hasn't always been that requirement — "It used to be something you just had to think about," he said – but now insurance companies are starting to push more and more, requiring businesses to comply or to have different types of protections and processes in place.

The questionnaires seek to detail what kinds of cyber protections companies have in place and, in the beginning, companies would have their IT agents — such as STACK — fill them out or just do it themselves.

"They don't really know what they're answering," he said. "It takes a cybersecurity professional to understand and interpret these questions."



Justin Myers (left) is president and CEO of California-based Glenn S. Caldwell Insurance. Mitchell Prevost is a commercial agent for the firm.

For instance, STACK has a client that does business with Ford Motor Company, and Ford wanted the client to fill out a 60-page questionnaire.

"It's taken right from the National Institutes on Standards and Technology," Miller said. "And they're pushing those requirements down to their vendors."

While everyone agrees getting cyber insurance is a good idea, determining what level to purchase can be a bit daunting and, according to Glenn S. Caldwell's Myers, depends on a variety of factors.

"For example, if you have a company that is strictly online and they're doing $10 million in gross revenue, you would try and protect them for at least half of their assets," Myers said. "If they have $10 million, you would want to get them a $5 million policy to protect them for as much as possible.

"Whereas if you have a large construction company and they're hardly doing anything online and they're doing $10 million, they don't necessarily need that %5 million policy," he added. "It is dependent on the nature of business, the likelihood of the attack, the revenue that's coming in, and just the necessity for a larger limit or not."