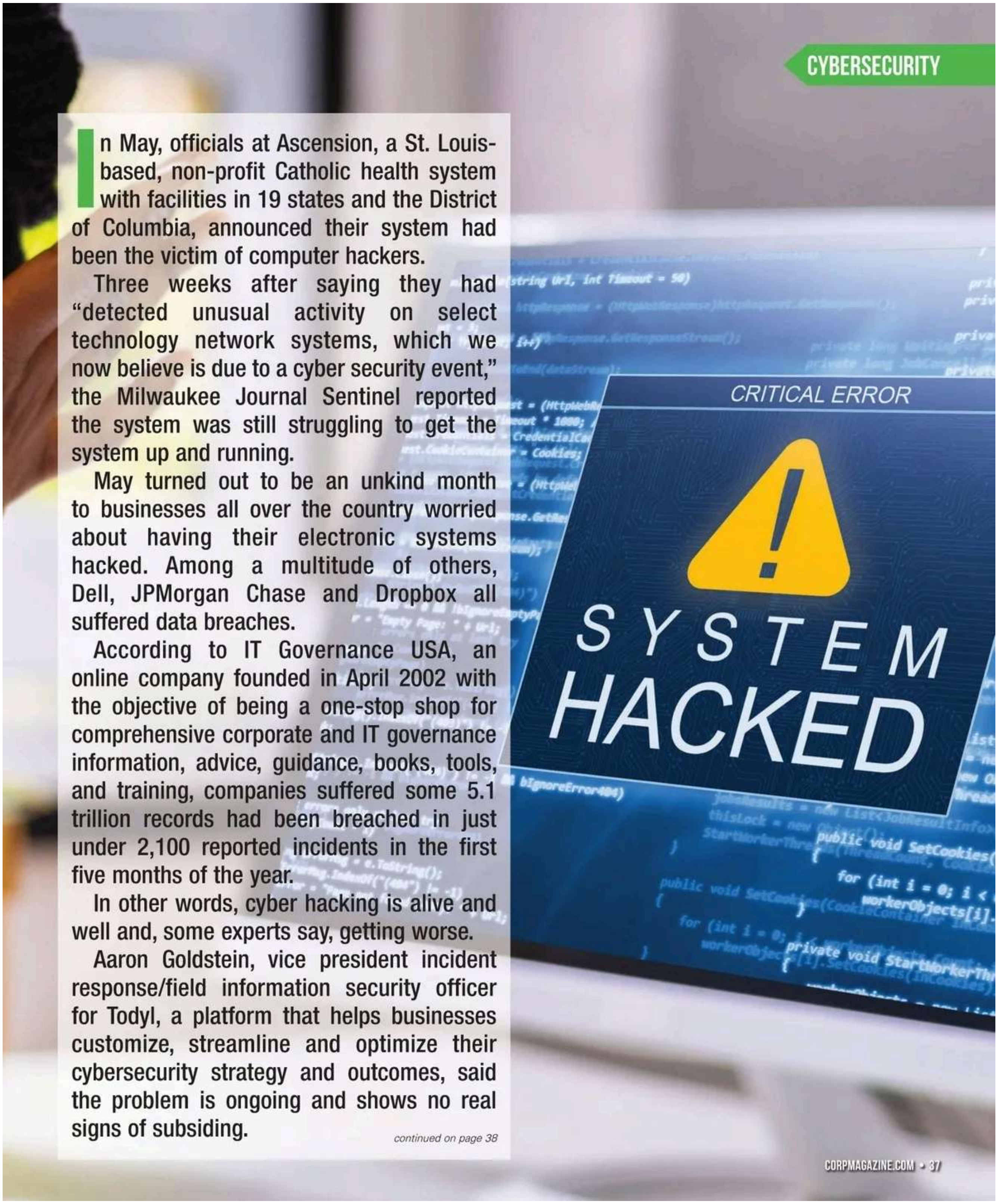
CYBERSECURITY

BY BRAD KADRICH

NOT GOING AWAY ANY TIME SOON

CYBER ATTACKS HAVE DOUBLED SINCE 2015 AND ARE STILL A TOP SECURITY PRIORITY FOR BUSINESSES



In May, officials at Ascension, a St. Louis-based, non-profit Catholic health system with facilities in 19 states and the District of Columbia, announced their system had been the victim of computer hackers.

Three weeks after saying they had "detected unusual activity on select technology network systems, which we now believe is due to a cyber security event," the Milwaukee Journal Sentinel reported the system was still struggling to get the system up and running.

May turned out to be an unkind month to businesses all over the country worried about having their electronic systems hacked. Among a multitude of others, Dell, JPMorgan Chase and Dropbox all suffered data breaches.

According to IT Governance USA, an online company founded in April 2002 with the objective of being a one-stop shop for comprehensive corporate and IT governance information, advice, guidance, books, tools, and training, companies suffered some 5.1 trillion records had been breached in just under 2,100 reported incidents in the first five months of the year.

In other words, cyber hacking is alive and well and, some experts say, getting worse.

Aaron Goldstein, vice president incident response/field information security officer for Todyl, a platform that helps businesses customize, streamline and optimize their cybersecurity strategy and outcomes, said the problem is ongoing and shows no real signs of subsiding.

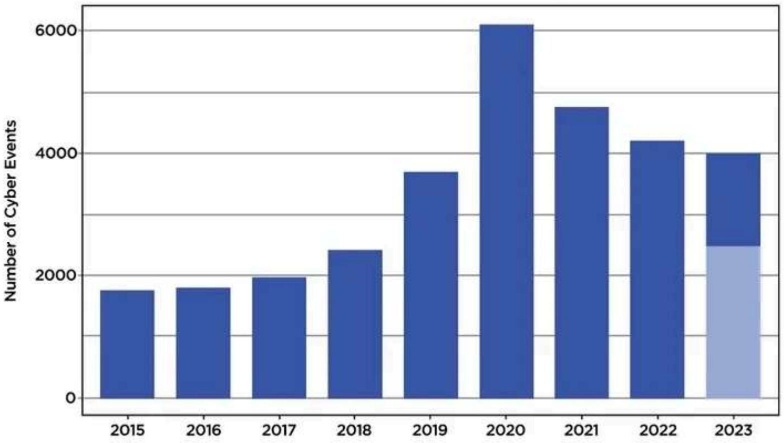
continued on page 38

"(Hacking) is trending upward, probably for the last 10 years at this point," Goldstein said. "The amount and volume of the attacks, as well as the value of what's being stolen and compromised, is astronomical."
Goldstein, who earned a bachelor's degree in information technology-security from the University of Central Florida, said that, while ransomware attacks are still prevalent, coming up on the outside are business email compromises.

It's an incident where a user gets their credentials stolen and the threat actor uses them to log in as the user.

"They might do a couple things ... send a fraudulent email to another member of the company and ask for a wire transfer or payment," Goldstein said. "We've seen them create fake employees and sometimes they'll even act as a fake vendor for a bigger attack where they've compromised multiple companies.

Rising cyber-attack trend – reported events have doubled in the past 5 years



Note: Publicly disclosed cyber events dataset contains data from Jan 2015 to March 2023. Number of events in 2023 is projected based on the average monthly observation on the first quarter of the year and demoted in a lighter shade of blue. Source: Moody's

"And then that new email that's compromised is just added to the email chain and a CCC to just make it look more legitimate, like, 'oh, well, you know what? Allison's been added to this email chain, it must be legitimate.'

"And so, we see a lot of that type of activity where users are just getting their credentials stolen in a lot of different advanced ways, and the threat actors perpetuate fraud almost immediately."

It's happening a lot more than it used to. Moody's published a report in September that showed reported cyber events more than doubled between January 2015 and March 2023, from some 1,800 in 2015 to some 4,000 in the first three months of 2023 (that includes a peak of more than 6,000 at the height of the pandemic in 2020, according to Moody's).

"The increased digitization of business and its reliance on IT infrastructure has exposed virtually every aspect of the economy to cyber risk," the report read, in part.

The "golden oldies" of cyber-attacks – data breaches, company information, patient information, etc. – like the ones that hit Ascension, Chase and the others are still popular.

The healthcare industry remains a popular and often-hit target.

"Healthcare is a huge target, absolutely. And we've seen that with Ascension," Goldstein said. "Healthcare is a target rich environment. That data is super valuable."

But, increasingly, it's not the only target. Rich Miller says there's a new kind of hack moving up the charts.

Miller, the president and CEO of Livonia-based Stack Cybersecurity, a rebranding of the company he founded in 2006, AM Data Services, said companies now have to worry about "cyber extortion."

It's more of a lay-in-wait process, where threat actors gain access to a company's system and then simply wait for something they can monetize.

Rich Miller is president and CEO of the recently rebranded Stack Cybersecurity, founded in 2006 as AM Data Services.

"They will watch your mail traffic for any unknown number of days. It could be two or three months. And once they finally see something of value come across … waiting for information to come around about trade secret or figuring out what's the secret sauce to your business, what makes it tick," Miller said. "What they're doing now is … saying, 'We have your drawings, pay us this much money, or we're going to send them to your competitor."

Miller tells the story of a client that manufactured ladders, and the tread pattern on their staircase ladders was proprietary information.

In that scenario, he said, the threat actors would lie in wait in the company's email system and wait to find the secret to the pattern.

"Perhaps they find the drawing data for that, and what they're doing is instead of just locking out their system, they're saying, 'Pay us,'" Miller said.

It's something of an evolution from previous patterns of attack, Miller explained. It used to be that the attack would come through ransomware, and cybersecurity firms like AM Data Services, who can create backup systems to thwart such an attack, would urge a company not to pay.

So the threat actors would then lockout the backup system, so companies found a way to protect those. Now, they're frequently doing the cyber extortion.

"Now they're just kind of working their way through," Miller said. "They're going after stuff that has more value."

And it's not just businesses who can fall victim to such scams. With the ever-increasing popularity of social media, individuals can be preyed upon in much the same way.

Miller pointed out threat actors can gain access to personal email just like they can a business email. They can discover personal details such as browsing activity and social media sites.

For instance, in July 2015, the dating site Ashley Madison was hacked, and the hackers threatened to release user data (they did, in fact, release the data of at least 2,500 users).

"So, they find out (the individual) goes to Ashley Madison and threaten, for instance, to reveal all the details to the victim's spouse unless they pay $15,000," Miller said. "And people pay it."

The Moody's report points out that the "rapid digitization" of the economy and business' reliance on it "moves cybersecurity to the forefront of risks to be actively managed."

This trend has prompted investors, market participants, consumers, and regulators to address this emerging risk with greater urgency, the study shows.

"Understanding a company's financial and technological exposure to cyber threats can help these market participants better prepare for potential cyber events and related financial losses," the study finds.

Experts says companies should back up all their data so systems can be rebuilt in case of a hack. Companies like Stack Cybersecurity and Todyl are available to provide assistance with such efforts.

But Todyl's Goldstein recommends yet another helpful measure: Cybersecurity insurance, something he said can be "an absolutely lifesaving thing" in the event of a catastrophic incident.

"You think about an incident, 'okay, well maybe my systems are down for a week or two,' but you don't think about having to rebuild all those systems," Goldstein said, "Not only do you have to be down for that time, but you also have to have new systems to rebuild onto.

"A lot of times people underestimate what a true incident costs between the IT personnel who are rebuilding, the negotiators and the professionals who are doing the security investigations, the lawyers and everything else," he added. "It adds up very, very quickly and it's not a cheap process."

Miller agrees "one hundred percent."

"(Companies) need full cybersecurity (insurance) policies, not just riders," he said. "A lot of times if you have a rider on your policy, it is a low coverage. So, if you've got a million-dollar business owner policy and they add a cyber rider, it may be $100,000 of cyber coverage or maybe $50,000 per incident and $100,000 in aggregate, whereas a regular full cyber policy will be a $1 million policy on its own."

The Moody's study made the same point, saying the "results of our empirical analysis" emphasizes the importance of cybersecurity "as a key component" of security for companies.

Aaron Goldstein is vice president incident response/field information security officer for Todyl.

"Developing a risk-aware culture and supplying risk managers with the tools and data required to assess, monitor, communicate, and respond is needed," the report said. "Our findings here indicate that those goals are both urgent and achievable."

Stack Cybersecurity's Miller said those kinds of cybersecurity efforts are what often (though not always) keeps the good guys one step ahead of the bad guys.

For a long time, threat actors depended on ransomware. Then security firms like Stack and Todyl helped companies build backup systems. When they found a way to compromise those, security professionals came up with what Miller called "immutable backup systems" he said protected the data.

That forced the threat actors to shift course again.

"As we combat those things, (threat actors) come up with new stuff that hasn't been beat yet," Miller said. "When (aggressors) realized they couldn't change the backup anymore, they had to come up with something different.

So they shifted their method because security managers were beating them at their own game?

"Yes," Miller said. "Yeah, absolutely." ■