Cybersecurity Alert:

Overcoming Vulnerabilities for Stewards of Member Health Data and Information

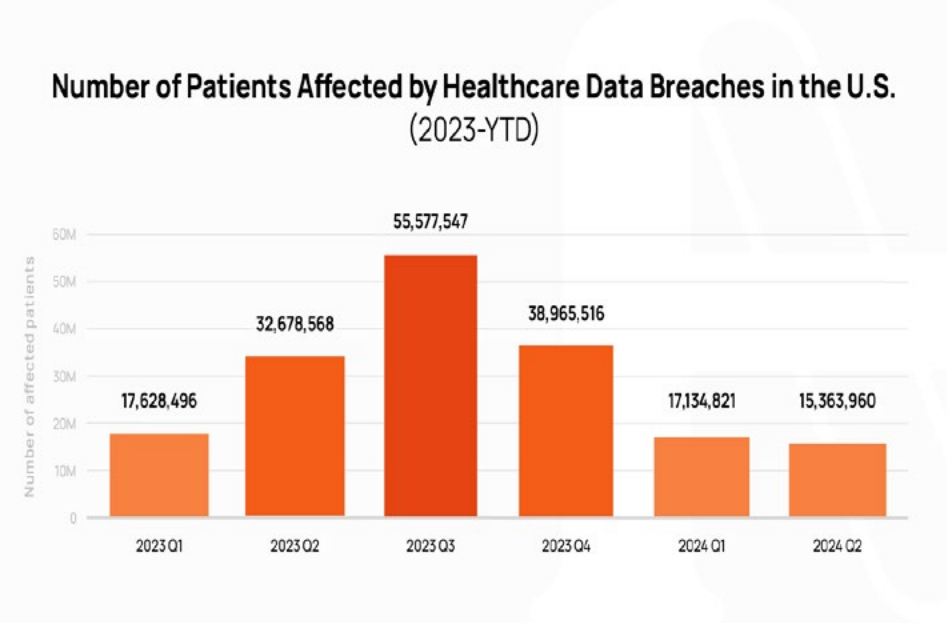
Written By Laura Carabello

It's just mid-year 2024, and the U.S. healthcare industry has already experienced some of the most dangerous cyberattacks in history, with unprecedented breaches in terms of stolen health and personal data. Healthcare organizations nationwide, including self-insured companies, now wonder if they, too, are vulnerable – and how to thwart these criminal attacks. As a caveat, cybercrime can follow each one of us home with devastating effects on our personal lives.

The healthcare sector is increasingly facing cyber threats and over the last five years, analysts report there has been a staggering 256% rise in significant hacking-related breaches and a 264% surge in ransomware incidents reported to the Department of Health and Human Services (DHHS) Office for Civil Rights (OCR). Companies covered by the Health Insurance Portability and Accountability Act (HIPAA) are required to notify HHS of data breaches involving protected health information, such as medical data and patient records.

In response, many advisors recommend that covered entities and business associates subject to HIPAA re-double their efforts and proactively attempt to diminish or prevent this growing menace.

According to Scott Fuller, chief of cybersecurity at CyberPro Partners, a HealthWare Systems company, "No healthcare entity is immune from a cyberattack, and every single person in the organization has the same threats and the same troubles in terms of trying to remain safe with cybersecurity. Today, a third-party audit confirming security is virtually mandatory, especially for small to mid-size organizations that can ill afford to have a full-time cybersecurity specialist constantly looking at their vulnerabilities. This is an underserved, fast-growing market that desperately needs protection from the growing legions of cybercriminals."



Source: Health Day News

In the past, Fuller says that it was considered healthy to have a "penetration test" performed annually. Someone would pose as a hacker and try to uncover vulnerabilities, repeating the test the following year to see if all the holes were plugged.

"Fast forward to today where these cyber criminals are coming out so fast with hacking techniques, monthly testing is a necessity," he says. "Organizations need to be aware of what occurred even in the past week, recognize the weaknesses and determine how to fix it – apply the patch from the software company, restart the server and know that the vulnerability is gone. But if you're not doing that on a monthly basis, it may get to the point where the system needs to be looked at constantly. It's just the ever-evolving world of cybercrime."

The cascade of hacking events this year followed the 725 large security breaches in healthcare reported to the DHHS OCR in 2023, beating the record of 720 healthcare security breaches set the previous year. Even the federal government is vulnerable. The Cybersecurity and Infrastructure Security Agency (CISA) reported that Russian government-linked hackers stole correspondence between a number of U.S. federal agencies and Microsoft in a months-long hack this year. CISA's disclosure in April is the first acknowledgment that federal agency emails with Microsoft were stolen.

DATA BREACH

A data breach occurs when sensitive information is accessed or disclosed without authorization, posing a risk to individuals or organizations. Such breaches can put various types of data at risk, including personal, financial, and medical information.

Source: Health Day News

Here's a snapshot of high-profile healthcare cyberattacks reported thus far in 2024:

January

- Concentra Health Services: Protected health information (PHI) of nearly 4 million patients was compromised in the cyberattack the previous year on Perry Johnson & Associates, Inc. (PJ&A), a provider of medical transcription services to healthcare facilities. The files contained the PHI of individuals, potentially including names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, and dates and times of service.

- INTEGRIS Health reported that 2.4 million patients had been affected in a December 2023 cyberattack. Patients received extortion emails informing them that their data had been stolen in a cyberattack on the healthcare network and that the data would be sold to other threat actors if they did not comply with the extortion demand.

- Eastern Radiologist, Inc., North Carolina, revealed unauthorized access to its network at the close of 2023, affecting data from over 886,000 patients. Some documents were accessed and/or copied from their system containing various patient data, potentially including names, contact information, Social Security numbers, insurance information, exam and/or procedure details, referring physicians, diagnoses, and/or imaging results. As a result,

February

- UnitedHealth Group's (UHG) Change Healthcare was victimized by a ransomware attack, compromising the data from one-third of Americans and now characterized as one of the worst hacks to hit American healthcare as malicious hackers stole compromised credentials on an application that allows staff to remotely access systems. UHG manages 15 billion transactions per year and touches one in every three patient records. UHG conceded both that it had paid the cybercriminals $22 million, and that patient data nonetheless ended up on the dark web -- and information may still remain vulnerable. UHG expects between $1 billion and 1.15 billion USD in direct costs this year as a result of the attack and forecasts a further $350 million to 450 million USD as a result of business disruption, including lost revenue. The State Department is now

offering a $10 million bounty for information on ALPHV or BlackCat, the cybercriminal gang behind the breach. Another hacker group, which calls itself Ransomhub, posted 22 screenshots on the dark web for about a week.

- Lurie Children's Hospital, Chicago, reports cyber criminals took down the electronic health record systems and MyChart online, although these patient-facing systems have since been reactivated.

- Medical Management Resource Group, operating as American Vision Partners and providing administrative support for ophthalmology practices, announced unauthorized access to its network the previous November. Hackers had obtained personal information belonging to patients of American Vision Partners' clients, including names, contact details, dates of birth, medical records, and, in some cases, Social Security numbers and insurance details, impacting approximately 2.35 million individuals.

April

- Kaiser Permanente, which operates 40 hospitals and 618 medical facilities, reported a breach in April, purported to be the largest data breach reported so far this year to the HHS' OCR and impacting 13.4 million current and former plan members. The data breach purportedly stemmed from tracking technology

– which has since been removed from their websites and apps- that unwittingly shared patient information with advertisers and third-party vendors, such as Microsoft, Google and X (formerly Twitter.) These vendors were able to access information -- patient names and I.P. addresses, indicators that they were signed into a Kaiser Permanente account and the ways they navigated different websites or applications.

•City of Hope, a cancer hospital operator and clinical research organization, disclosed a data breach that compromised the personal and health information of 827,149 patients. The suspicious activity began late in 2023 when the organization engaged a leading cybersecurity firm that determined that hackers accessed its I.T. systems. Hackers stole files that may have contained patient names, contact information such as email addresses and phone numbers, dates of birth, Social Security numbers, driver's license or other government identification, financial details (such as bank account numbers and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/or unique identifiers to associate individuals with City of Hope, like a medical record number.

May

•Ascension, the St. Louis-based nonprofit Catholic health system that runs 139 hospitals and 40 senior living facilities across the country, confirmed a hit by Russian-speaking ransomware group Black Basta. This led to a diversion for emergency medical services and interruption in services concerning its electronic health records system (EHR), among other tools. The system is already facing patient class action lawsuits alleging harm from exposure of private information which they claim was "foreseeable and preventable" if Ascension had implemented "adequate and reasonable cybersecurity procedures and protocols."

LESSONS LEARNED

"The lesson re-learned is you don't have to get directly attacked to be affected," says Rob Gelb, CEO, Valenz Health, noting that thankfully, Valenz has not experienced a cyberattack, but leadership at the very top fully supports and backs I.T. Security. "Cybersecurity is a team sport and preventing a breach with reasonable protections and strategies costs far less than getting compromised. Collectively, healthcare information security teams should start collaborating and sharing the best security practices they are implementing."

He recalls an incidence in 1980 following the MGM Grand fire when MGM shared everything they learned from that experience with all the casinos on the strip. They all realized one casino's tragedy was everyone's tragedy.

"Third-party security assurance goes part of the way but lacks team collaboration," says Gelb. "I want a format that inspires companies to help each other openly."

Gordon Thompson, FCAS, FSA, MAAA, actuarial consultant, Amerisk Consulting, shares this response to the Change Healthcare attack, "The attack is being attributed to the absence of multi-factor authentication, which left the remote systems vulnerable. To create a secure environment, you need to include every member of your team as an active participant in your digital security team. Some portions of your risk can

be secured by forced software updates to the most secure versions and patch known vulnerabilities."

According to Verizon's Annual Data Breach Incident Report, 74% of all breaches include a human element, to which Thompson advises, "Frequently educate your employees about the latest data breaches and their causes and how they can avoid them. Empower your entire team by arming them with information and best practices. Knowing what your risks are and constantly working to secure them is only one step in guarding against this type of breach, but it's a foundational one."

He says we all need to make sure we cover at least the basic cyber defensive tactics, warning, "Cyber criminals are frequently one step ahead of the best security practices, innovating and finding new ways to hack into sensitive systems. However, this attack was due to a lack of multi-factor identification, which left a remote access application exposed."

Requiring multi-factor identification is a basic security defense, one that even the most routine security audit would have found and addressed, saving UnitedHealth an estimated $1.5 billion in damages in this one instance.

"Paying attention to the latest tactics attackers are using can help your organization check their cyber defenses and be alerted to potential exposure in your own organization," continues Thompson. "A cyber risk audit to find the potential exposures in your organization is a great place to start."

WHAT IS RANSOMWARE?

Ransomware is malicious software designed to encrypt data on victim computers, allowing bad actors the ability to demand a ransom payment in exchange for the decryption key.

For example, ZCryptor is a ransomware cryptoworm that encrypts files and self-propagates to other computers and network devices. The first victim on the network is infected by common techniques, masquerading as an installer of a popular program or malicious macros in Microsoft Office files.

Fuller says that many organizations want to know if they should pay the ransom and assume the problem is over. "That's not the case," he advises, as demonstrated by UHG where the ransom was paid, and the info remained on the dark web.

Here's another example: Not too long ago, an OBGYN doctor with just a small clinic and five employees was hacked, with the cyber criminals leaving ransomware notes on all the office computers and demanding $15K. Fuller advised the doctor not to pay the ransom since once they know you are going to pay, they will strike again and again.

"They have no idea about who you are or the size of the organization but figure you are an I.P. address and an easy target – low-hanging fruit," recounts Fuller. "They looked at the doctor's QuickBooks and assumed she could probably spare $15K. In this situation, it only took about two days to trace the culprits in North Korea and basically bring her system back. Some pain, but not worth paying a ransom. There's no honor among criminals."

PLAN SPONSOR PREPAREDNESS

Cyber-criminals appear to have a sixth sense that ERISA-covered plans, regardless of their size, are great targets given their financial assets and maintenance of personal data on participants. With a target on their backs, responsible plan fiduciaries have an obligation to ensure proper assessment and mitigate cybersecurity risks.

As the number and sophistication of cyberattacks increase, plan sponsors and participants need to stay current on the Employee Benefits Security Administration U.S. Department of Labor's" Best Practices" for cybersecurity and fraud protection. See below for an overview of the recommendations for plan-related I.T. systems and data, as well as for plan fiduciaries making judicious decisions on the service providers they should hire. Visit this URL for a complete document: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

1. Have a formal, well-documented cybersecurity program.

2. Conduct prudent annual risk assessments.

3. Have a reliable annual third-party audit of security controls.

4. Clearly define and assign information security roles and responsibilities.

5. Have strong access control procedures.

6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.

7. Conduct periodic cybersecurity awareness training.

8. Implement and manage a secure system development life cycle (SDLC) program.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

10. Encrypt sensitive data, stored and in transit. 11. Implement strong technical controls in accordance with best security practices.

12. Appropriately respond to any past cybersecurity incidents.

On an annual basis, plan sponsors should also consider asking their providers for information about their cybersecurity practices. A simple step is to review and document that data and store it in a fiduciary file. With increased utilization of personal digital solutions, plan sponsors can collaborate with their recordkeepers to distribute participant-focused communications that improve "digital hygiene."

Fuller suggests, "There are some things about cyber security that are common sense, and there are issues that simply require education, a framework and some accountability. Think of the Weight Watchers model, where people know how to lose weight but need to be accountable, so they are not embarrassed during the

weekly weigh-in. To ensure fraud protection, having that accountability with an independent cybersecurity check-up every week or month accelerates progress for moving onto a security framework. It's like coaching an athlete to optimize the best performance."

Analysts also warn that a company's third-party vendors are bringing vulnerabilities to the table, especially with self-insured employers now relying heavily upon digital solutions, telehealth and remote patient monitoring. This can also include a payroll service, creating customer portals that give administrative access to everyone in the organization and the ability to see home addresses, Social Security numbers, wages, and other personal information. Someone could get that information and sell it, suddenly creating the HR-related headaches of having everybody know what everybody else earns.

"That's considered an internal breach, but it's still a breach of trust since employees provide employers personal information that they assume will be handled correctly," counsels Fuller. "That's why many organizations are starting to introduce third-party risk management with more checks and balances to ensure that there are adequate sign-offs about who gets access to this information."

Thompson says he thinks it inevitable that every organization will have a data breach, adding, "It's easy to think that an attack of this sort will never happen to you, but if it did, do you have a crisis response plan, so you know how to respond? Which stakeholders are notified first? What resources do you have available to manage the crisis? Do your insurance policies cover cyber liability? To what extent? These are the questions we recommend asking now before you experience a breach."

He advises that a complete risk assessment can help you understand where the risks are in your technology, which can be patched and made more secure, and what the scope of an attack might entail.

"Working with an actuary can help you put numbers around the probability of an incident and the potential costs of a cyber-attack, as well as check your current policies for gaps in coverage," says Thompson.

He further counsels organizations to work with a vendor to secure their data, noting, "Technical and security vendors are a great place to start to identify your technical vulnerabilities. Those vulnerabilities can then be secured or insured. While ensuring your cyber liability is a great step, it's one that many companies have taken, only to be disappointed when they file a claim at how much isn't covered. This is also a vulnerability."

Jakki Lynch RN, CCM, CMAS, CCFA, director cost containment, Sequoia Reinsurance Services, explains, "Beyond firewalls and multi-factor authentication, organizations should have a strategic preventative risk management and recovery plan for business continuity that includes alternative means of performing the operational services required for patient care delivery, revenue cycle management and claims adjudication. Awareness and focus on preventing data breaches should be a top priority for health care providers and payers."

She says that many unresolved downstream concerns for organizations remain, recommending consideration of these issues to address and mitigate risk exposure for potential future breaches:

- How patient care will be impacted due to the economic harm to healthcare providers and how major privacy breaches of healthcare information can be prevented and detected

- Address claim reimbursement concerns, including interest

and penalties due to late claim filing and delayed claim processing – and how providers and plan payers validate that the claim billing and payments processed subsequently by Change HealthCare (or others) are correct.

• How potential breach fines or reduced Medicare payments will impact hospitals and health systems and healthcare costs for payers, as well as access to care for patients.

• How platform organizations can provide a level of assurance that the incident has been contained as well as prevented in the future.

Kurt Smith, Corporate Information Security Officer, Valenz Health, offers this guidance, "Defense-in-depth uses multiple lines of defense to protect against potential threats. Think of a bank's physical security: a lobby where customers can enter, a teller who proxies customer requests for the bank, and a secured vault with controlled entry. The entire bank has security protections. Last but not least, bank policies and protocols enhance a bank's security. I.T. Security's job is to implement the digital equivalent of that kind of security.

Smith itemizes some of the top basic actions an I.T. security team should take:

- Implement multi-factor authentication, especially for Internet-facing resources and privileged access. If you can land on a webpage online, so can a bad actor.
- Separate corporate and production environments—physically and virtually—in terms of network infrastructure, systems, applications, and credentials. Corporate systems allow staff to conduct day-to-day business. Production systems are the products and services the company provides -- they're the engine that keeps a company in business. Separation reduces the attack surface.
- Implement next-generation security tools -- heuristic antivirus doesn't cut it these days. There are too many solutions to list, but the key is visibility in monitoring, containing, and responding to threats. Vulnerability management is also a big part of this, not just patch management but code and application scanning.
- Monthly security awareness training is critical -- e-crime is the top threat. Social engineering attacks are more straightforward and require less effort to compromise a company than by hacking in. Why hack when you can trick someone into giving you their credentials?
- A strong identity management program is imperative because social engineering attacks are so prevalent. Helpdesks remotely support staff, vendors, and customers. You must be able to verify who is on the other end before rendering assistance.

ADDRESSING COMPLIANCE ISSUES

Healthcare systems were put on notice in February to address potential HIPAA compliance issues before they experience a breach or receive notice of an OCR investigation. OCR released two Congressional Reports concerning compliance and enforcement under HIPAA, offering key insights for entities regulated by HIPAA that aim to bolster their compliance strategies. OCR suggests that covered entities and business associates focus on improving compliance with the security management process standard, the audit controls standard and response and reporting requirements.

This includes safeguarding against prevalent attack methods such as phishing emails, the exploitation of existing vulnerabilities, and the use of weak authentication measures. In the event of a successful breach, attackers frequently encrypt electronic Protected Health Information (ePHI) for ransom purposes or steal the data for future malicious activities, including identity theft or extortion.

Attorneys at Bradley Arant Boult Cummings LLP advise that by prioritizing preparedness, resilience, and a culture of cybersecurity awareness, healthcare organizations can not only protect themselves against the financial and reputational damage of cyberattacks but also, and most importantly, safeguard the well-being and privacy of the patients they serve.

Here are OCR recommendations for best practices and strong reminders for healthcare organizations to enhance cybersecurity preparedness, especially with increased utilization of digital solutions.

- Ensuring all partnerships with vendors and contractors are secured by appropriate business associate agreements that clearly outline responsibilities in case of a breach or security incident.
- Embedding risk analysis and management into the core business practices, with regular assessments, particularly when adopting new technologies or altering business operations.
- Establishing robust audit controls to document and scrutinize activity within information systems.
- Conducting periodic reviews of information system activities to identify and mitigate potential risks.
- Adopting multi-factor authentication measures to verify that only authorized individuals access protected health information.
- Securing protected health information through encryption to prevent unauthorized access.
- Learning from past security incidents to improve the overall security management strategy.
- Offering targeted training that aligns with organizational and specific job requirements, emphasizing the essential role of all staff in upholding privacy and security standards, and ensuring such training is refreshed regularly.

U.S. GOVERNMENT AND TRADE ASSOCIATIONS STEP IN

In Q1, U.S. Senator Bill Cassidy, M.D. (R-LA), ranking member of the Senate Health, Education, Labor, and Pensions (HELP) Committee, released a report outlining ways to improve privacy protections for Americans' crucial health data. Including various recommendations to update the HIPAA framework, protect health data not currently covered by HIPAA, and address data that blurs the lines between health and non-health categories, the report points to the value of HIPAA in safeguarding patient information,

The Biden administration has announced a plan to improve cybersecurity at hospitals, beginning with incentives but eventually imposing penalties on hospitals that do not adopt measures to protect patient

data. The Department of Health and Human Services (HHS) research funding agency is promising more than $50 million to developers who can build a scalable cybersecurity platform able to keep hospitals' complex digital ecosystems up to speed. The Advanced Research Projects Agency for Health (ARPA-H), the Universal PatchinG and Remediation for Autonomous DEfense, or UPGRADE, program will offer "multiple awards" to those with the best pitches on ways to detect weaknesses and implement fixes with minimal interruptions to care delivery.

In May 2024, the Federal Trade Commission issued a revised Health Breach Notification Rule aimed at protecting consumer medical information on digital health and wellness apps and requiring them to notify consumers of a breach. According to the announcement, the rule requires vendors that manage digital health records that are not covered by HIPAA to notify individuals, the FTC and, in some cases, the media of a breach of unsecured personally identifiable health data. The agency defines this type of data as traditional health information such as diagnoses and medications, as well as data collected from fitness trackers and "emergent health data."

Organizations throughout the healthcare ecosystem are lining up to advocate for better protection against cyberattacks. The Medical Group Management Association sent a letter to the DHHS OCR seeking clarity on whether providers are responsible for alerting affected patients that their personal health information may have been compromised. Additionally, the Workgroup for Electronic Data Interchange (WEDI) requested that the Department of Health and Human Services (HHS) create an Office of National Cybersecurity Policy led by a "cyber policy czar."

Most recently, the College of Healthcare Information Management Executives (CHIME), the American Health Information Management Association (AHIMA) AHIMA, the American Medical Association, and most state medical associations have sent a letter to OCR to request more clarity around reporting responsibilities related to the Change Healthcare data breach, emphasizing that OCR should publicly state that its breach investigation and immediate efforts at remediation will be focused on Change Healthcare, and not the providers affected by Change Healthcare's breach.

CAPTIVES & REINSURANCE: CONSULTANTS WEIGH IN ON SOLUTIONS FOR MITIGATING CYBER RISK

As healthcare cyber threats accelerate, there is an increased need for self-insured companies to have the ability to assess, manage and transfer the risks associated with a cyber-attack. Cybersecurity firm CYE cautions that the protection afforded by cyber insurance may fall significantly short of the actual costs incurred during cyber incidents. In a recent report, they expose critical coverage gaps that threaten organizational stability in the wake of cyberattacks, revealing that a staggering 80% of insured companies that suffered a data breach did not have sufficient coverage to meet the costs of a breach.

Axa Advisors says captives are a well-established part of the risk management landscape and can give sophisticated clients additional tools to assess, mitigate, retain and transfer both traditional risks and evolving, critically important risks like cyber. They believe that captives will play an increasingly important role in this process, helping businesses to gain not only greater cyber security resilience but greater confidence in their ability to recover from cyberattacks.

They also cite the value of structured reinsurance, which can help captive clients manage cyber risk, giving clients a degree of certainty about the maximum premium payable in any one year while limiting the level of retention on the balance sheet.

Actuaries at AmerRisk Consulting advise that in response to the significant losses of cyber insurers resulting from several high-profile wins for policyholders, companies are either declining to cover cyber risk or have chosen to severely restrict coverage. They say that policies have become so costly that many business owners can't afford to consider meaningful coverage. Plus, cybercriminals innovate more rapidly than the technical solutions to the threats they pose and much faster than any insurer can keep up with.

Thompson points out, "A thorough risk assessment isn't complete without an underwriter/actuary reviewing your market cyber policy and identifying any gaps in coverage. They can make recommendations about how to insure those gaps through self-insurance or by putting them in a captive."

However, the consultants say there may be ways to add cyber risk to an existing captive to solve the problems since a captive can change and respond faster than the traditional insurance market, pivoting to quickly adapt to the emerging risks that cyber criminals pose. While they also point to a limited loss history which makes coverage difficult to price accurately and potential losses difficult to quantify, they advise independent analysis of individual companies and losses that are publicly available can create a blueprint for the types of losses a business may experience.

By adding cyber risk to your captive, these analysts advise an extensive internal audit of the cyber risks of a company and a plan to manage those risks internally. As the company learns more about its own risk to cover it in a captive, it can improve loss control and create a position of risk ownership within the leadership of the company.

Furthermore, since a cyberattack is an immediate threat that requires rapid access to capital, captive coverage can be written to ensure that resources are immediately available to respond. Captive policy language can also be broad and tailored to the benefit of the captive owner, providing better coverage of all the risks associated with a cyber-attack -- including reputational harm, media responses, legal fees, potential ransom payouts and other costs that aren't physical damage to the company as a result of the attack.

Milliman says there are significant advantages to adding cyber insurance to a captive, noting one benefit of adding cyber insurance to a captive is having insurance coverage where coverage may not exist in the commercial market or may be too expensive. They say captives provide their parents with an option to consider when looking for alternatives to the commercial market, and while some cyber policies may have exclusions, like ransomware losses, a captive can help fill the gap in coverage through a difference in conditions policy.

Finally, MarshMcLennan Captive Advisors admit that while a captive is not a silver bullet, using a captive insurer provides organizations with flexibility and options for their cyber risk management strategy. Since the cyber insurance market has become challenging over the past few years, they say risk retention vehicles are helping clients to manage their total cost of risk and increasingly are using existing captives and cells, or establishing new ones, as an integral component of their cyber risk management and insurance strategy.

CYBERSECURITY – AN ONGOING CHALLENGE

Attackers are working overtime to be successful, and security teams must be more aggressive than ever before in assessing their own defenses. While legacy security control investments cost millions in controls, systems and staffing, these traditional fixes often leave gaps in the form of misconfigurations and insufficient protocols.

Tom Kellermann, head of cybersecurity strategy for VMware, who serves as the Wilson Center's Global Fellow for Cybersecurity Policy and sits on the U.S. Secret Service Cybercrime Investigations Advisory Board, explains, "Healthcare security teams are typically overwhelmed with huge lists of potential issues, so they can't easily identify the practical risks in a "pile of theoretical vulnerabilities. Every healthcare organization faces a wide array of potential weaknesses and security flaws that may exist within their systems and networks — such as vulnerable medical devices, unencrypted data transmission or outdated software."

He says organizations often identify these vulnerabilities through cybersecurity tools like security assessments or penetration testing, but due to the sheer volume of these possible vulnerabilities, it can be difficult for healthcare cybersecurity teams to prioritize which weaknesses pose the most practical and immediate risk to the organization's security posture.

Kellerman points to the long recovery time from a cyber-attack, indicating a potentially poor business continuity plan (BCP), which every healthcare organization needs in case of a potential cybersecurity event. The plan must address business continuity in case of crisis or disaster, including technical backups, alternative payment and collection routes and the ability to restore systems in a timely fashion.

One final indication of the demand for vigilance: Blackwell Security, a cybersecurity company, announced in May that it had received $13 million in an undisclosed funding round.

Laura Carabello holds a degree in Journalism from the Newhouse School of Communications at Syracuse University, is a recognized expert in medical travel and is a widely published writer on

Healthcare issues. She is a principal at CPR Strategic Marketing Communications. www.cpronline.com ■