MITIGATING CYBERSECURITY RISK: IS CYBER INSURANCE THE ANSWER?

Authored by:
Colin Konschak, FACHE, Divurgent
Shane Danaher, MBA, Divurgent

INTRODUCTION

Until recently, healthcare executives tended to ignore the need for cybersecurity, as it was perceived to only be a consequence affecting data, which can be replaced. However, since 2014 when cyberattacks against healthcare began ratcheting up, the industry leaders have been forced to acknowledge the increasing cyber threats and consider cybersecurity protection.

Though cybercrime is increasing at a steady rate as technology becomes more pervasive, there has been a dramatic rise in cybercrime in the past eight years, with no sign of slowing down. Still, healthcare systems see cybersecurity as more of an IT challenge with a relatively reactive approach to IT breaches. This leaves the health system significantly unprepared for cybercriminals and makes the system ill-equipped to mitigate cyber threats, despite the economic importance of medical records. Health organizations are therefore beginning to turn toward cyber insurance providers as internet threats increase.

Is cyber insurance a good cybercrime strategy, just one component of an overall strategy, or is cyber insurance even unnecessary?

Leaders in all business sectors are realizing cybercrime can make virtually every business risk a reality, including reputation loss, business interruption, breach of privacy, liability for regulatory penalties, and even outright business failure. Throughout this cybersecurity whitepaper series, we have delved into steps organizations can take to protect their network, software and human attack surfaces. But what about insurance against attacks? Do healthcare organizations need cyber insurance? If so, what kind of coverage should they choose? In this whitepaper, we examine the kinds of business risks healthcare organizations face, the ways they can guard against those risks becoming realities, and how to blunt the impact if they do, including coverage with cyber insurance.

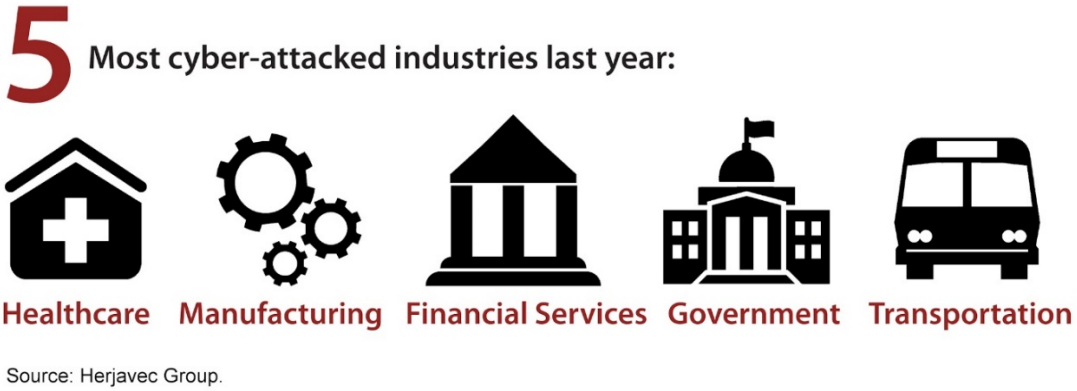
VIEWING THE RISK LANDSCAPE

The first step in considering any type of insurance is determining what the risks are and the potential damage they can cause. In its 2017 Cybercrime Report, which was sponsored by global cybersecurity firm Herjavec Group, Cybersecurity Ventures Editor Steve Morgan emphasized a startling prediction about cybercrime:

> "Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined" (Morgan, 2017).

In 2016 and 2017 healthcare led the top 5 industry sectors targeted by cybercrime, according to the Cybersecurity Ventures 2017 Cybercrime Report (see Figure 1).

Figure 1: Most Cyber-Attacked Industries 2017



Source: Herjavec Group.

In the report, Herjavec Group Founder and CEO explained the cybersecurity imperative for healthcare leaders. “In 2017 we have seen more focus on cybersecurity investment from healthcare providers,” said Herjavec. “They’ve felt the pain of their antiquated systems and have had to step up out of necessity to do more to protect their infrastructures and patient data.”

With the mounting threats of cyber extortion, denial of service attacks and the growing amount of personally identifiable information and protected health information for sale on the Dark Web, boards and members of the C-Suite in healthcare are being held accountable by law for cyber breaches. Still, many do not recognize cybersecurity as a primary component in their risk management strategies (Mangelsdorf, 2017).

CYBERSECURITY RISKS MOVE TO THE FOREFRONT

In its 2018 Risk Barometer report, insurer Allianz Global Corporate & Specialty (AGCS), noted that cyber incidents are now the top risk in 11 countries, including the United States, where cyber incidents supplanted business interruption as the top risk in 2018 over the previous year. Business interruption still ranks as the highest risk globally, with cyber incident risk maintaining its steady climb to the number 2 spot. Fifteen years ago cyber incidents weren’t even in the top 10, ranking only 15th (AGCS, 2018). It is important to note that business interruption is one of the key components of cybersecurity insurance package because it is one of the top risks of cybercrime.

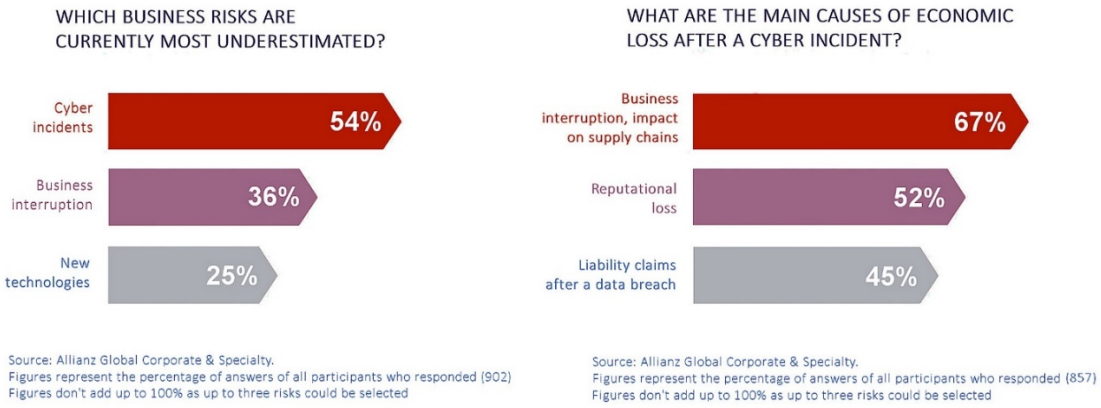
“Cyber is a 24/7 365-day-a-year risk that is evolving at a rapid pace,” said AGCS CEO, North America Bill Scaldaferri. "Cyber losses can span many risk areas, such as loss of reputation, business interruption and new technology. In addition, it is not limited to being an external risk

exposure, as the actions of employees can impact a company's risk of data breaches or other forms of cyber incidents" (AGCS, 2018).

AGCS Global Head of Cyber, Emy Donavan, also noted that more than 50 percent of Risk Barometer responses rank cyber incidents as the risk most underestimated by businesses (see Figure 2 below).

"Every company has been or will be impacted by cyber risk. It is not over-hyped," says Donavan. "If anything, it is under-appreciated because the threats are not always well understood. There are now multiple cyber threats to a company's digital presence" (AGCS, 2018).

Figure 2: Underestimated Business Risks and Main Economic Losses



THE BUSINESS CASE FOR CYBERSECURITY

The AGCS report noted the multiple threats to a company's digital presence. The threats come under three major headings:

- Cyber Attack
  - Extortion
  - Cyber theft
  - Network liability
  - Data restoration and forensics costs
- Cyber Business Interruption
  - Employee error
  - System failure
  - Regulatory requirement
- Data Breach
  - Any breach of privacy legislation
  - Regulatory action
  - Client data in care, custody and control (AGCS, 2018)

COUNTING THE TRUE COSTS OF CYBERCRIME

The direct and indirect costs of a breach can be staggering, and recovery from it can be challenging. Direct costs in recovering from breaches include data forensic services to restore and clean up your systems, credit monitoring services, labor and material expenses for public relations and patient notification, attorney fees, and regulatory fines. Indirect costs can include effects of business disruption, lost productivity, reputational harm and degradation of financial performance, and all of these indirect costs can be hard to quantify.

Because of all of these very real business threats, mitigating risks of cybercrime should be a high on the list of organizational priorities. But is it? What are the consequences of not making it a priority?

According to a survey of 10,000 consumers worldwide conducted in 2017 by technology sector market research firm Vanson Bourne for the digital security firm Gemalto, 69 percent of consumers feel businesses don't take the security of their data very seriously and 67 percent believe their online personal information will be stolen at some point. However, perhaps the most consequential finding from the survey is this—a majority (70%) of consumers say they would take their business elsewhere if an organization that holds their personal information digitally suffered a data breach (Gemalto, 2017).

That is a scary thought from a customer/patient-retention standpoint when it comes to healthcare and many other business sectors, but consumers also need to be looked at as part of the human attack surface problem when it comes to cybercrime risk management. In this world of electronic health records and online health accounts, consumers can be just as sloppy and pose just as much of a cyber threat to your organization as your own employees.

"Consumers are evidently happy to relinquish the responsibility of protecting their data to a business, but are expecting it to be kept secure without any effort on their part," says Jason Hart, CTO, Identity and Data Protection at Gemalto. "In the face of upcoming data regulations such as GDPR, it's now up to businesses to ensure they are forcing security protocols on their customers to keep data secure. It's no longer enough to offer these solutions as an option. These protocols must be mandatory from the start—otherwise businesses will face not only financial consequences, but also potentially legal action from consumers" (Gemalto, 2017).

The Security Rule in the Health Insurance Portability and Accountability Act (HIPAA) has a direct nexus with cybersecurity and cyber risk management for all entities subject to it, because, in total, the administrative, physical and technical safeguards cover incident prevention, identification, response and mitigation. The Office of Civil Rights of the Department of Health and Human Services (OCR) particularly emphasizes the security risk management requirements, including the performance of regular risk analyses and the development of a risk management plan. A risk analysis involves reviewing and determining the location and types of data, potential

sources and likelihood of each risk, and potential effects and the magnitude of each risk if it does occur.

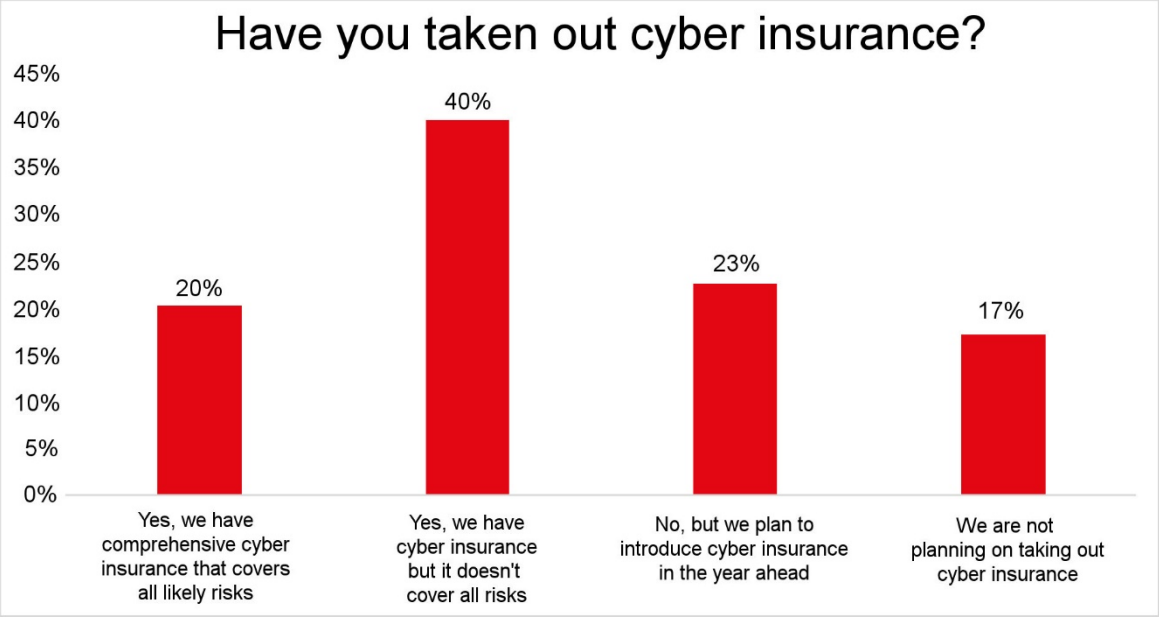
Once the risks are fully evaluated, the risk management plan serves as a guide for the development of an entity's cybersecurity program and the adoption of security measures designed to account for or mitigate those identified risks. OCR considers these requirements fundamental to all other Security Rule measures, and, as such, these measures frequently are noted as an area of non-compliance in many recent OCR settlements, which can range in the millions of dollars.

WHERE DOES CYBER INSURANCE STAND?

Despite all of the risks out there, apparently not everyone in the business world is convinced that cyber insurance is necessary. In a survey released in May 2017 of 350 companies, conducted by research firm Ovum for Silicon Valley analytics firm FICO, the following was found (FICO, 2017):

- 50 percent of U.S. executives surveyed say their firm has no cyber insurance, compared to 40 percent in other countries surveyed
- 27 percent of U.S. executives say their firms have no plans to take out cyber insurance, despite 61 percent of executives stating they expect the volume of attempted breaches to increase in the next year
- Only 16 percent of US firms surveyed have cybersecurity insurance that covers all risks

Figure 3: Take-up Rates for Cyber Insurance



Source: Ovum

Most notably for the purposes of this whitepaper, the survey found the healthcare sector to be particularly lagging in full protection with cyber insurance. None of the healthcare organizations represented in the survey have insurance that covers all risk, while 74 percent have no cyber insurance at all (FICO, 2017).

WEIGHING THE RISKS AND THE BENEFITS

If you work in healthcare, you have either been a target of cybercrime or you eventually will be. Most general liability policies, and errors and omissions policies will not cover a cyber incident or data privacy or security breach. So, when the breach happens, will cyber insurance help mitigate the damage? To determine whether cyber insurance is right for your organization, there are many factors to consider and much research to be done to figure out whether the investment in premiums will outweigh the risks.

In a 2017 *HealthITNews* article, Steven Gravely, a partner and healthcare practice lead at Troutman Sanders, was interviewed about considerations regarding cyber insurance for healthcare organizations. "Providers must treat cybersecurity as an enterprise risk that will affect the entire organization rather than simply an IT issue," Gravely said. "The dollar amount of coverage is certainly one important factor, but as important is the scope of the coverage. What is included under the policy as a covered loss and what is not." (Siwicki, 2017, August 4).

Gravely also noted that all policies are not equal, with some not covering the costs of preparing notifications to OCR and state regulators or paying their penalties, and others not covering services being suspended during a cyber-extortion attack. For this reason, careful analysis is needed—not only of what the policies cover, but what is the level of your organization's threat response capability and ability to proactively guard against attack.

WHAT SOME CYBER INSURANCE POLICIES COVER

Risk transfer is the commitment of a cyber-insurer, and here are a few expenses insurers cover, depending on the policy:

> ***Investigation***: A forensic examination is essential to define what occurred, how to repair damage and how to avert a similar type of breach from taking place in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI. Accurately conducted research reaches the source of the attack, devices used, and helps to educate hospitals' IT experts on projected sophistication in that route.

Business losses: A cyber insurance policy may include similar items that are covered by an error policy, as well as monetary losses experienced by network downtime, business interruption, and costs involved in crisis management, which may include fixing reputation damage.

Privacy and notification: This includes data breach warnings to customers and other affected parties–warnings which are required by law in many jurisdictions–and credit monitoring for consumers whose information may have been breached. The insurers should notify all health payers of a breach and assist them in taking the necessary steps to secure their data while making reports to essential authorities.

Lawsuits and extortion: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also cover the costs incurred in an attack, such as ransomware.

Standalone policies contain some of the coverage explained above, but they may go by various names from insurer to insurer. Event management insurance can cover the cost of a breach, such as a forensic investigation, public relations, notifying patients and credit monitoring. Network business interruption insurance can reimburse for lost income and operating expenses. Liability insurance can cover third-party claims, such as fines, defending a lawsuit and an imposed judgment. Cyber-extortion insurance can reimburse for ransom payments.

All of these different types of coverage relating to cybercrime need to be explained in full, and as always, the fine print must be carefully examined to have a full understanding of coverage and exclusions, and what is being expected of your organization in mitigating some the risk of cyberattacks.

WHAT A HEALTHCARE ORGANIZATION SHOULD ASK A CYBER INSURANCE PROVIDER

There are similarities in the general policy and cyber insurance, but most cyber insurers want coverage with systems equipped with updated IT infrastructure and are therefore careful in coverage. Here are a few questions to ask an insurer:

- **Is there more than one type of cyber insurance policy, and is the policy customizable?** Cyber insurance is evolving, and it is better to employ strategies that are tailored to your clinics as organizations vary in budget, patient size, and Internet of Things connections.
- **Are there deductibles, and how do they fare against those of other insurers?**
- **How do coverage and limits apply to both first and third parties? For example, does the policy cover third-party service providers?** On that note, find out if your service providers have cyber insurance and how it affects your agreement.

- **Does the policy cover non-malicious actions taken by an employee?** This is part of the Error & Omission coverage that applies to cyber insurance as well. If after investigation, the discovery details that an employee was a significant cause of the breach, what will the risk coverage be like?
- **Is the cyber insurance policy operated by you (the insurer), or a third party?** It is always better to deal with a team who handles cybersecurity and recovery themselves. It saves business downtime and manages crisis in a superior fashion.
- **Does the policy include time frames to which coverage applies?** Because advanced persistent threats take place over time, which can be months to years, you need to be clear as to when you are covered, and when you are not.

CONCLUSION

A cyber insurance policy is measured by the business scale and data sensitivity, because of the difficulty in quantifying and accurately predicting the extent of cyber incidents. Cyber insurance demands budget analysis and modern-day attack-resistant infrastructures before policy purchase, creating a win-win situation for the client and insurer.

If you have a cyber insurance policy, it will contain an obligation for you to notify the insurer of a security incident. Failure to timely notify your insurer could adversely impact your ability to receive coverage under the policy. If you do not have established relationships with third parties, such as legal counsel, monitoring companies or mailing companies, your insurer may require that you use their chosen vendors. Even if you do have an established relationship, if you have not obtained permission from the insurer to allow you to use your chosen third-party vendor, you may still be required to use their vendors.

Cyber insurance will undoubtedly increase public trust, as consumers acknowledge safety of their data and quality care. Cyber insurers can determine the routes of attacks, assisting in better resistance for such future violations. Cyber insurance tames the high costs of data breaches by offering coverage in areas of breach notification, lawsuits and forensic investigation among other things.

No matter how good your systems and procedures are, there is no way to guarantee you will not be attacked and breached, so cyber insurance should be considered. In any case, healthcare stakeholders should start by creating security awareness—technology updates alone will not win the battle against cybercrime. Healthcare organizations must deploy security-centric strategies, and plan from the cyber attacker's point of view. The security strategy will use interactions with employees and vendors, and how they interact with high-value information and the Internet of Things devices.

The goal is to apply a comprehensive approach to help the system prepare for ongoing cyber-attacks. Health organizations should also raise awareness training for every staff member and for patients who are handling medical records, becoming familiar with cybersecurity best practices. Some companies are approaching cybersecurity training in ways that are similar to training for ethics and regulatory compliance.

And although cyber criminals are continuously looking for new ways to launch an attack, organizations should also get better at the enemies' strategies. Companies should keep abreast of, and continuously monitor, compliance and new cyber-attack mechanisms, through alliance and security awareness. Whether for old threats seeking vengeance or new malware, health systems should ensure their defense mechanisms are up to date.

REFERENCES

Allianz Global Corporate & Specialty. (2018). *Allianz Risk Barometer: Top 10 Global Risks for 2018*. Available at: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2018/

Gemalto. (2017). *Data Breaches and Customer Loyalty*. Study conducted by Vanson Bourne. Available at: https://www.gemalto.com/press/pages/majority-of-consumers-would-stop-doing-business-with-companies-following-a-data-breach-finds-gemalto.aspx

Mangelsdorf, M. E. (2017). What executives get wrong about cybersecurity. *MIT Sloan Management Review*, *58*(2), 22.

Morgan, S. (2017). *Cybersecurity Ventures 2017 Cybercrime Report*. Sponsored by Herjavec Group. Available at: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Ovum. (2017). *What the C-suite Needs to Know About Cyber-readiness*. Sponsored by FICO. Available at: http://www.fico.com/en/latest-thinking/white-paper/what-the-c-suite-needs-to-know-about-cyber-readiness/.

Siwicki, B. (2017, August 4). What to know about risk, coverage before you buy cyber insurance. http://www.healthcareitnews.com/news/what-know-about-risk-coverage-you-buy-cyber-insurance