Cyber risk management in health care

EY
Building a better working world

Why captives are a critical component in cyber risk management for health care organizations

A new digital era

The health care industry is riding a powerful wave of digital transformation of medical services, business operations and the end-to-end patient-consumer experience. Wearable devices are common consumer purchases, and machine learning is providing valuable data insights from them. According to our recent *New Horizons* research, both consumers and physicians believe remote monitoring technologies and artificial intelligence will be central to health care provision within the next 10 years, enabled in part by a proliferation of emerging devices within the Internet of Healthcare Things. The telemedicine market alone is projected to be worth $41.2 billion by 2021, up from $23 billion in 2018.

Data is being shared and combined by connected health care actors across the value chain: providers, hospitals, labs, insurers and pharmacies. Rapid advances in consumer technology are also enabling interactions with patients via virtual agents, which in turn drive the shift in care location to the home. These changes are already happening, and they are happening quickly.

The data generated by this transformation offers great benefits, but also great risk; risk of data breaches, compromised patient information, reputational damage and lost trust. To help manage this cyber risk, health care organizations should consider using a captive insurance arrangement.

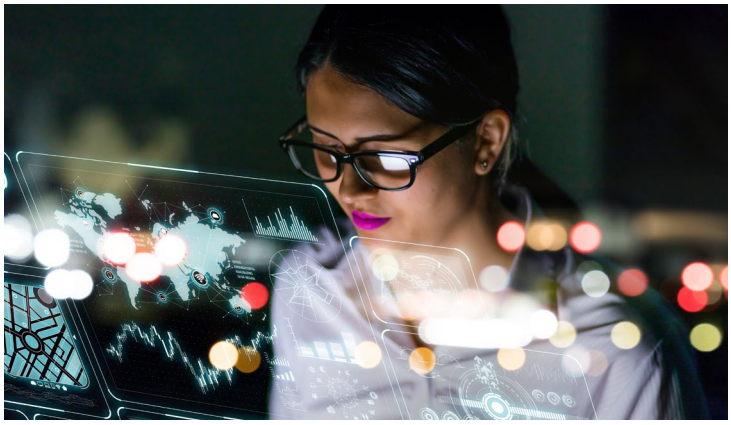
This article examines the cybersecurity risks faced by health care organizations, how a captive may assist in managing those risks and the factors to be considered when creating a captive arrangement for cybersecurity purposes.

Cyber crime in health care

With the health care sector storing an increasing amount of personally identifiable and sensitive information, the illicit sale of medical information has increased. On the black market, medical records are more expensive than credit card information, at approximately $60 per record versus $1 to $3 for stolen credit card details.

Breaches of health care records sharply increased in 2019, with total records hacked exceeding the totals of 2016, 2017 and 2018 combined. Some examples include:

- **July 2019** – A ransomware attack on an Alabama-based dental and optical services organization encrypted a wide range of network files, closing clinics for two weeks.
- **August 2019** – A ransomware attack permanently closed a California company, as widespread encryption and loss of backup data made file recovery and system restoration impossible.
- **October 2019** – Another ransomware attack forced an Alabama company to close its three hospitals for all but critical new patients and purchase decryption keys from the attacker due to the perceived benefits for patient well-being.



Captive concerns

With such potentially catastrophic impacts on the business and such complex underlying risk, many ask how a captive could provide cyber insurance coverage without taking on too much exposure. While no one-size-fits-all approach exists, the lack of choice, the wide variety of policy terms and the high price of primary cyber insurance coverage has made alternatives to traditional insurance attractive. In fact, Aon's Cyber Captive Survey 2019 revealed that health care is the leading industry in the growth of captive cyber coverage, by gross written premium, although the number of participating captives has not grown significantly.

According to Zurich, pooling risks in a captive at a reinsurance level may provide multiple benefits, including flexibility to define customized coverage, assurance that companies pay for what they need without claims falling between the policy gaps, access to a broad data pool to help improve loss management and analysis, and improved claims management at the portfolio level.

Other potential advantages to placing cyber risk in a health care captive include:

- **Raising the profile of cyber risk** — build a sense of urgency around and ownership of cyber risk management at the board level so that decisions are made and change can be delivered
- **Allocating opex and capex** — reinforce accountability for cyber risk management and introduce consistent reporting to C-level executives so that performance can be tracked
- **Demonstrating commitment to risk resilience** — use the captive structure and deductibles to demonstrate what is at stake so that reinsurers gain confidence in the risk management culture of the parent company
- **Investing captive surplus into cyber resilience** — monitor captive performance and guard surplus so that the captive can be used as a source of investment into critical risk management activities
- **Using the full risk management toolkit** — implement an enterprise-wide risk management framework within which the captive forms just one critical tool, so that cyber risk is managed rather than transferred
- **Consolidating pooled captive risk data** — implement an effective risk assessment and mitigation approach leveraging the full data set available to the captive so that the parent company understands its exposure and mitigates appropriately
- **Demonstrating compliance with law and leading practice** — law enforcement and government agencies require a comprehensive, granular approach to cyber resilience that factors in the full life cycle of risk management and risk transfer activities
- **Facilitating cross-industry collaboration** — work closely with insurers and other health care captives to establish cross-industry data standards, shared anonymized data and a common taxonomy

Cyber resilience for the health care industry

Health care organizations are not typically known for combining cutting-edge technology with digital know-how. Recently, however, health care organizations have invested considerable time and effort addressing cyber-exposure concerns; the effectiveness of those efforts is uncertain. As observed in the Global Cyber Risk Perception Survey Report 2019 from Marsh, many organizations plan their cyber defense around technology rather than assessment, risk transfer, response planning and other risk management areas. But cyber risk management is about enterprise-wide risk responsibility, not any single function; the sooner an organization builds a culture whereby everyone is a risk manager, the more effective its risk management will become.

Through a combination of board-level leadership and accountability, investment from captive surplus funds and captive reinsurance risk transfer, health care organizations can comprehensively manage their cyber risk. For health care organizations that don't know how or where to start building their cyber resilience, here are a few key steps:

- **Understand your exposure** — conduct a cyber risk assessment of your data, systems and hardware to understand what is at risk and how critical it is
  - You should be certain that you understand your risk at a granular level, as that meets enforcement agency expectations and delivers positive patient safety outcome.
- **Prioritize mitigating actions** — determine what is most at risk and how this can be mitigated, against a balance of cost, effectiveness, complexity and time
  - Based on your exposure, you may find that risk management training and risk inventory management are more effective than technology in detecting cyber attacks.
- **Maintain and enhance** — continuously implement your mitigating actions, improve your risk management framework and adapt to the cyber risks facing your organization
  - Cyber risk management requires ongoing, proactive attention at all levels of the organization.

Why act now?

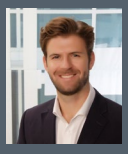
As cyber attacks continue making headline news, health care organizations that fail to focus on their cybersecurity risk being portrayed as negligent. They also risk significant fines for noncompliance with the Health Insurance Portability and Accountability Act and increased scrutiny from government agencies, which reportedly consider email phishing training and simulation exercises critical priorities.

Most importantly, however, failure to focus on cybersecurity risks patient safety and trust.

Engaging a captive in cyber risk will promote a cyber risk management culture across the organization, while also encouraging the organization to take a more holistic and strategic approach to cyber risk. With this engagement, health care organizations will be better positioned to demonstrate proper handling of the data with which they are entrusted. That trust will lead all parties to partner in technology that will benefit the industry and patients.

Contacts

Kerr Kennedy is an IT Risk Advisory associate partner in EY Bermuda Ltd.'s Information Technology Risk practice of the Bahamas, Bermuda and Cayman Islands. Kerr can be reached at +1 441 294 5460 or kerr.kennedy@bm.ey.com.



John Marsden is an Advisory manager within EY Bermuda Ltd. Performance Improvement practice in the Bahamas, Bermuda and Cayman Islands region. John can be reached at +1 441 294 5326 or john.marsden@bm.ey.com.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. 08246-201US
2001-3365212 (BDFSO)

ED None

ey.com