Sensitive Health Data

Rising Stakes and Sound Security Practices

In 2000, global spending on Cyber Security was $3.5 Billion. In 2017, the number swelled to $120 Billion. By 2021, it is estimated the market spend will exceed $1 Trillion. There are many reasons for this explosive growth – increased awareness of cyber threats and elevated sophistication of profit driven cybercrime are two of them. The biggest driver however is the sheer number of new devices connecting daily to the World Wide Web and the resulting attack vectors introduced.

There were roughly 15 billion connected devices in 2016. Intel estimates that number will grow to 200 billion by 2020. That roughly translates to 27 per human being on planet earth. A recent article published on ZDNet[1] cites Google Assistant's ability to connect over 5,000 smart home devices (up from 1,500 in January of '18). "Turn on the TV", "Turn off the lights", and "Preheat the oven" – you get the idea. Each device connected by the World Wide Web has the potential to reach any other connected device. Did each of these manufacturers consider security? Will they release security patches in a timely manner? What happens if one of the manufacturers goes bankrupt and can no longer offer support?

These modern conveniences have associated risk price tags and we should all be mindful of them. Are there potential consequences caused by this exponential increase in Internet traffic? Could an Internet connected toaster, toilet or toy serve as part of a bot army or be an avenue for a malicious cyberattack? How safe is protected electronic data in an environment with 200 billion connected devices?

The high dollar costs associated with data breaches is forcing boardrooms around the world to focus on cyber security. The average data breach cost across all US industries was an estimated $7.3[2] million in 2017. If we refine the view to the US healthcare industry, the cost jumps to $12[3] million making it the costliest type of data breach across all industries. There are several common drivers behind these costs (investigations, notifications, remediation costs, loss of business) but fines related to a healthcare data breach are in a class by themselves. HHS handed out nearly $20 million in HIPAA fines in 2017[4].

Consider a few of these recent headlines on the HHS.gov website. "Widespread HIPAA vulnerabilities result in $2.7 million settlement", "$2.14 million HIPAA settlement underscores importance of managing security risk", and "$2.5 million settlement shows that not understanding HIPAA requirements creates risk."

So how can health insurers reduce the high risk associated with a more connected Internet and increased breach costs?

This is the realm of data security programs and Chief Information Security Officers. Before a sound security program can be built and implemented however, all of the issues and variables need to be understood. What are the specific HIPAA and HITECH regulations that apply to my company? How much protected data am I custodian of? Does a business associate or third party handle this data? How is protected data accessed and how is it used? Once the complete scope is understood, a customized security program that flexes with current threats and landscapes can help reduce risk.

Health insurers and managing general underwriters (MGUs) that underwrite employer stop-loss coverage work with very sensitive data. These insurers maintain data on patients who have had rare diseases, expensive surgeries, and perhaps use specialty medications. Not only do these carriers encounter Protected Health Information of cases they have inforce, but also on every case they quote for coverage (approximately 25 times the cases inforce). This means that employer stop-loss insurers see PHI on many millions of lives every year. Do breaches occur in the self-insured health insurance space? Absolutely.

A recent conversation with a former executive at a national employer stop loss carrier painted a frightening picture. They relayed a breach incident in which a server containing millions of PHI records was stolen from a data center. This data would later be used as part of a blackmail extortion attempt. A post mortem review of the incident revealed that secure data center protocols were not adhered to and the server's hard disk drives were not encrypted. While this was a targeted scheme involving a specific network resource, it is important to understand the entire threat landscape. Where are all of the potential breach points?

Fayyaz Rajpari, a technical advisor and intelligence liaison at cybersecurity firm FireEye, says "You need to make sure the entire organization is security aware. It needs buy in from all employees". This can be a challenge at times. Let's face it - SOC2, AICPA, HIPAA, HITECH – these aren't the kinds of subjects that most people get excited to talk about though Rajpari suggests making it a part of a company's culture. FireEye's consulting arm, Mandiant, responds to the largest and most prolific data breaches in the world and recently published their "M-Trends 2018: The Trends Behind Today's Breaches and Cyber Attacks report". [5]

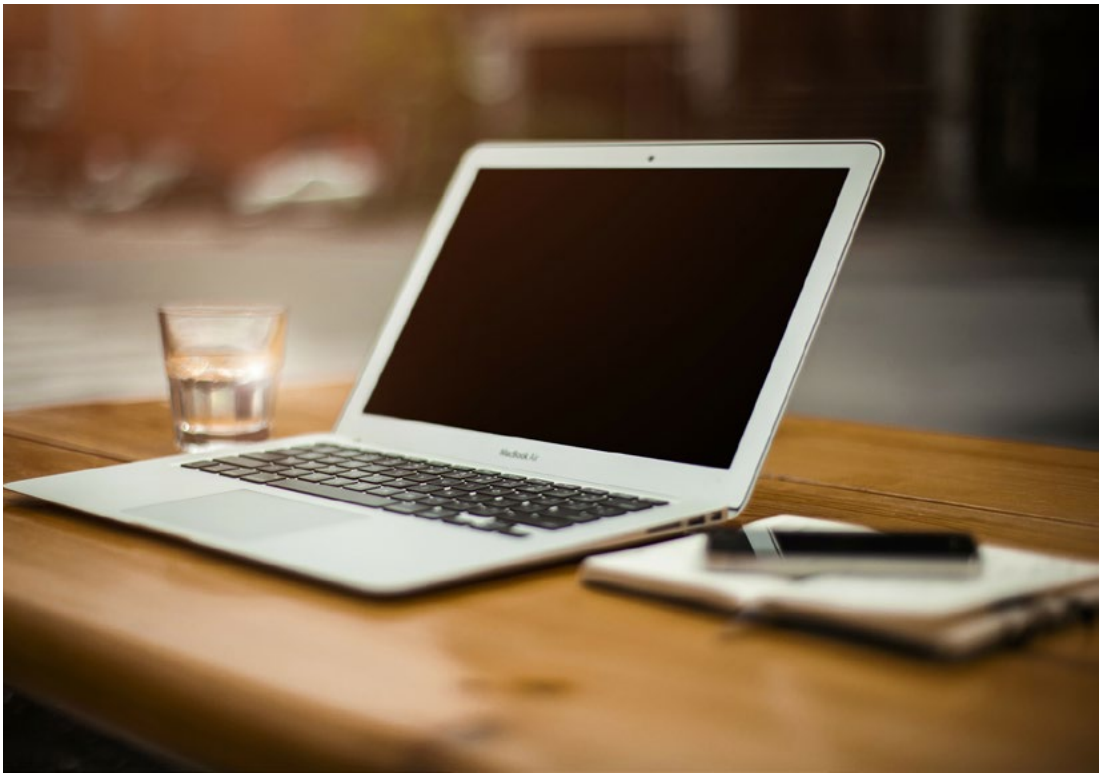
Along with Rajpari, we suggest some common sense principles that all employer stop-loss insurers and MGUs should incorporate into their security program to protect from data breaches:

- ***Continual Employee Training*** - The majority of healthcare breaches are caused by their own employees. Some are careless errors, some are due to ignorance and some are due to malicious behavior. Employees need to understand what the HIPAA/HITECH rules are, what a risky email/website/attachment looks like and what impact a breach could have on their company.

- ***Electronic Data Encryption*** – sensitive data needs to be encrypted at rest and in motion. Operationalizing this effort is key and cannot be taken for granted. It requires knowing how the data is transmitted, where it lives and how it is accessed. These key findings require constant review and adjustments as necessary.

- ***Current security software*** – keep your guard up. Any device and any software that has access to protected data needs to have current security software and patches applied regularly.

- ***Limit exposure, limit the attack surface*** – Only collect data that is needed, and only keep it as long as necessary. Make mindful decisions on who and what is allowed to access the protected data and where it can be stored. For example, many health insurers and other employers do not have a business need to store data on an external device (thumb drive, DVD, etc). Therefore, it is common to implement a group policy that turns off USB access and DVD drives on all PC's. This is not a silver bullet but it reduces possible breach points in a common sense way.



- ***Penetration Testing*** – Hire external consulting firms to poke, prod and test the network. Continually testing, retesting and adjusting is critical to remaining vigilant of new threats.

- ***Garner outside expert opinion about your security program*** – The AICPA has published standards on organizational security controls referred to as SOC 2. It is not uncommon for firms to hire certified consulting firms to perform the necessary audits to document adherence to these standards. A SOC2 Type 2 audit requires producing proof throughout a testing period that the firm has the proper security controls in place. What are your published security policies and procedures? What does your incidence response

Delaware Means ICCIE Trained

The International Center for Captive Insurance Education (ICCIE) has designated the Delaware Insurance Department Bureau of Captive and Financial Insurance Products as an ICCIE Trained Organization. Delaware is one of only four domiciles that has applied for and received this recognition. To qualify as an ICCIE Trained Organization, the captive bureau had to meet the following requirements:

1. At least 20% of the captive professionals in the captive bureau must hold the Associate in Captive Insurance (ACI) in good standing; and
2. At least 30% of the captive bureau's professionals must be ACIs, Certificate in Captive Insurance (CCI) holders, or currently enrolled in the ACI or CCI program.

For insurance regulators, ICCIE maintains strict standards for who qualifies as a "captive professional." The definition of a "captive professional" is someone who spends at least 20% of their time on captive insurance work and is either a licensed professional such as an attorney, accountant, actuary, insurance producer/agent, investment adviser/broker dealer, underwriter, or an equivalent to such a position. It does not apply to those whose work is purely administrative.

ICCIE's mission is to be the premier provider of captive insurance education and to offer the pre-eminent professional designation in captive insurance. ICCIE's program and curriculum have been developed in collaboration with the University of Vermont and reflect the highest standards of a top-tier educational institution.

STEVE KINION, DIRECTOR
Bureau of Captive & Financial Products
Department of Insurance

"This recognition by the ICCIE reflects the education, experience, and professionalism of Delaware's captive insurance staff. One of my objectives is to build upon a staff of highly competent regulators who know and understand how to regulate insurance for the benefit of my fellow Delawareans. I am proud of the hard work and dedication of the individuals in the captive bureau and heartily commend them."

Commissioner Trinidad Navarro

In Delaware, the captive regulators are dedicated exclusively to our captive insurance industry needs, and work under the direction of our Captive Bureau leadership, directed by Steve Kinion.

BUREAU OF CAPTIVE & FINANCIAL INSURANCE PRODUCTS
1007 Orange Street, Suite 1010
Wilmington, DE 19801
302-577-5280
Trinidad Navarro Insurance Commissioner

program look like? What are your disaster recovery plans? What are the logical and physical controls you have in place to protect sensitive data? These are just a few of the critical security subjects touched upon in a SOC2 audit.

Getting out of autopilot and thinking about risk is challenging but critical to the overall security of a network. Too often individuals are lulled into a false sense of reality when they are in front of a computer. They become "zombified". Their guard goes down and their common sense has a tendency to go down with it.

As Rajpari states, "*Security can fail by just one weak link regardless of how much security technology is deployed.*"

Consider how easy it would be for you to write a fictitious return address on an envelope and physically drop it in a mailbox. Now consider this process in digital form. Manipulating the "from" address in an email is vastly easier and it has the potential to reach millions of eyes with a few keystrokes and a click of a button.

Rajpari suggests empowering employees to make cybersecurity awareness both a personal and business goal. Personal training topics such as protecting your children online, shopping online and securing your home network are a few areas that he recommends adding to a security awareness program. If a personal cord can be struck, it is more likely to be embraced. It becomes relevant in a way that hits home and therefore has the tendency to become incorporated into one's everyday actions.

While these are some of the key aspects of a security program, it is important to understand that there is no perfect solution. Being aware of the risks, limiting exposure and designing mitigation plans is not a project that can be completed and moved on from. It needs to be part of the fabric of the company. The more individuals who decide to get out of autopilot and apply a security lens to their digital lives, the more secure that view will become. ■

Mike Hartnett is the head of Information Systems at Medical Risk Managers. MRM is a stop loss consultant, underwriter and actuary. For more information, visit www.mrm-mgu.com.

References

1 https://www.zdnet.com/article/google-assistant-now-connects-to-over-5000-smart-home-devices/

2 Data breach cost estimates gathered from a 2017 IBM sponsored study conducted by Ponemon Institute

3 Data breach cost estimates gathered from a 2017 IBM sponsored study conducted by Ponemon Institute

4 Summarized information gathered from the HHS.gov - https://www.hhs.gov/hipaa/newsroom/index.html

5 https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html?utm_source=lic&utm_medium=social