TREXIN INSIGHT PAPER

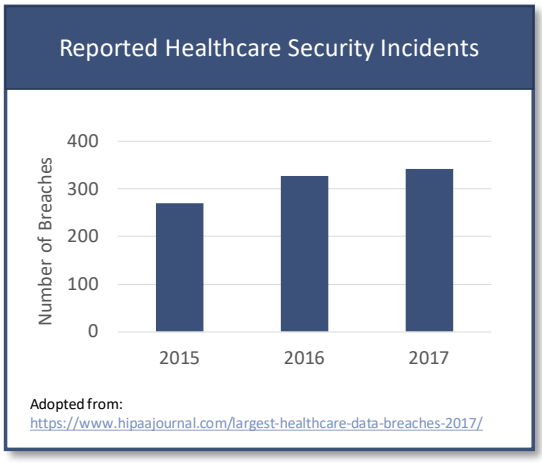
February 1, 2018

HOME HEALTHCARE TRENDS

Exciting opportunity, a significant threat.

In the last five years, healthcare costs have risen faster than the annual income in the United States. In 2016, US healthcare costs were close to $3.3 trillion, or 17.9% of the US GDP, making healthcare one of the country's largest industries. However, a few decades ago healthcare spending costs were not even 5% of US GDP. A recent Journal of American Medical Association study suggests the 63% increase in healthcare spending from 1996 to 2013 is due to a combination of rising charges per service and emphasis on patient quality during hospital stays and doctor visits. While growing inpatient healthcare expenses may not be a surprise, it is also critical to address the upturn in cybersecurity attacks and data breaches costs.

Recently, the healthcare sector was the most attacked by cybercriminals with data breaches costing over $6.2 billion according to the Cybersecurity Intelligence Index by IBM. In 2014 and 2015, eight of every ten health institutions had at least two or more data breaches. Despite all hopes that data breaches would decrease, there were 140 data breaches reported to Health and Human Services Office for Civil Rights (OCR) in 2017 representing a 23.9% increase from 2016. Also, ransomware attacks increased by 89% compared to 2016 and accounted for over half of the top ten healthcare breaches in 2017. Ransomware attacks such as WannaCry and NotPetya—only the first exploits from the NSA tools released by Snowden—have inflicted havoc in small hospitals and biopharma. These attacks consisted of 100 million healthcare records being jeopardized from more than 8000 devices in over 100 countries. Security experts believe the healthcare sector is considered to be a “hacker’s dream” since healthcare is more patient-centric rather than emphasizing IT, as a whole lacking cybersecurity resources, and relies heavily on legacy systems. Despite the rapid increase in costs and cyber attacks, healthcare payers and providers have continued to underestimate the need for a higher degree of cybersecurity vigilance.



While the payers and providers in the healthcare ecosystem increasingly leverage technology to serve patients in home healthcare and clinic environments, this gap with respect to cyber-investment in this ecosystem introduces significant new risk. The healthcare sector’s vulnerability to cyber-attacks primarily due to limited budget allocated by healthcare institutions increase this sector’s attractiveness to the cybercriminal economy. In comparison, the federal government spends 16% of its IT budget on security. Other industries also contribute more to cybersecurity, such as banking and finance which allocate 12-15% of their IT budget on security programs. Going into 2018, security experts predict complex attacks on healthcare Internet of Things (IoT), increased risk from insider attacks, and cracking of passwords and biometrics. Increased patient engagement facilitated by unrelenting development and diffusion of healthcare technologies will continue to transform the ways patients and providers interact. Furthermore, the escalation in the complexity of the ransomware attacks will evolve.

According to a recent study, use of home healthcare and telemedicine technology is expected to grow by over 18% annually through 2020, driven by physician shortages, cost-saving initiatives, patient convenience, and the explosion of connected devices. The risk of potential cybersecurity threads continues to rise as more medical devices use software and are connected to the internet, hospital provider networks, and other medical technologies (one example of IoT). Previous studies suggest that security breach vectors leading to data loss were driven by the external hacking of vulnerability (69%), malware introduced into the system due to human error (60%), phishing emails (39%), and third-

* TOP * 10 Top 10 Tips

1. **Establish a security culture and employee training**
2. **Perform enterprise network assessments and risk analysis**
3. **Control access to PHI and governance body**
4. **Dedicated sec-op teams**
5. **Breach response plan**
6. **Do your diligence to be HIPAA compliant**
7. **Avoid IoT devices that advertise Peer-to-Peer (P2P) capabilities**
8. **Multifactorial authentication**
9. **Check the defaults and update firmware**
10. **Limit network and physical access**

party device product (37%). The cybersecurity threats and vulnerabilities can impact the confidentiality, availability, and integrity of the IT networks, medical devices, and other systems.

As technical advances continue to disrupt home health by providing clinical information through fitness trackers, wearables, and BTLE medical devices, many unprecedented security implications have surfaced—for instance, experts have found that Fitbit wearables could be hacked by focusing on accelerometers and other motion sensors. Currently, no security protection exists for these devices. Most medical devices are not created with built-in. In the next decade, cybernetic implant systems, such as pacemakers or insulin pumps, will be widely implemented and accessed remotely by medical personnel. Smartwatches with LTE connections and pure biometric activity trackers like heart rate monitors leak information over their wireless networking and are susceptible to interception. However, personal connected devices that operate via close-proximity protocols, like BlueTooth Low Energy (BTLE), and piggy-back onto mobile devices are less directly accessible for abuse compared to IoT devices that are connected to the internet via Ethernet or Wi-Fi.

Many experts believe the growing trend toward BYOD (Bring Your Own Device) can put organizations at risk from cyber-attacks. Several healthcare companies have implemented a BYOD policy for tablets, smartphones, and laptops in the workplace. One study suggested that 81% of healthcare providers allow their doctor and medical staff members to use their iPads and mobile devices at work with nearly 46% of those organizations not taking any actions to secure those mobile devices. Another study by BMC medicine indicated that 66% of health apps that send identifying information over the internet don't use encryption while 20% don't have a privacy policy. Healthcare delivery organizations must prioritize minimizing the leakage of personal health information (PHI) via their employees' devices by taking accountability for managing at least the "for-business" portion of those devices, even while recognizing that the software and best practices for this are immature. Certainly, focusing on employee training and awareness of the threats and what they can do will mitigate risks of data theft, ransomware, and other cyber-attacks.

Approximately 73% of corporate executives are deploying or researching IoT devices and are currently facing the gap of addressing ever-changing device security. In 2018, Aon forecasts cybercriminals will leverage this increasingly complex mesh of devices especially in attacking small vendors or contractors using IoT. For example, Texas Children's Hospital manages more than 36,000 devices to provide care, with nearly 6,000 of them connected to the network. The IT security team at Texas Children's Hospital focuses on device identification, access controls, password management, and regular patch updates. The cybersecurity basics of encryption, multi-factor authentication and biometrics, and patching will continue to be the foundation of effective protection in this new world. Internal governance committees provide transparency and bring together department leaders and security professionals to better under the risks of IoT. Many experts believe security threats, such as Wi-Fi hacking or ransomware attacking unpatched systems, have evolved from stolen data to physical hazards that may harm patients such as the forced malfunction of a hospital refrigerator

providing chilled medication. It is critical that organizations institute frequent security assessments for IoT devices to keep up with the evolving security breaches.

As the amount of innovation for medical IoT and wearable technology continues to advance, the relative absence of adequate security protocols by the creators of the applications and gadgets continues to be problematic. Recent studies indicate that only 15% of healthcare respondents had increased or enhanced high-quality staff compared to the 24% who use an all-encompassing strategy to respond to cybersecurity threats. When possible, IoT devices should be segregated on their network and restrict access to employee fitness and wellness data It is fundamental for healthcare delivery organizations to create their HIPAA compliant applications and devices to bridge the security gap. Although the FDA does not conduct premarket testing for medical products, it does need to review changes made to medical devices primarily to strengthen cybersecurity. Organizations must prioritize anonymizing PHI by following HIPAA requirements. However, the Healthcare Industry Cybersecurity Task Force has stated that the NIST frameworks do not offer enough guidance to the healthcare industry. Healthcare delivery organizations need a dedicated sec-op team to handle security, hunt threats, educate staff on latest threats, and perform pen tests. They may also vet business vendors and associates by requiring indemnification provisions, reviewing risk assessments, and associated agreements.

Health Care Industry Cybersecurity (HCIC) Task Force Recommendations:

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity
2. Increase the security and resilience of medical devices and health IT
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase health care industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure
6. Improve information sharing of industry threats, risks, and mitigations

A successful cybersecurity program must go beyond software and build on the three pillars of processes, people, and technology. An effective security plan involves access to medical and billing records as well as contingencies for email and departments reliant upon the network and offices with high-tech equipment like lab, pharmacy or imaging services. Cybersecurity in healthcare must rely on a war-gaming model using real-world threat trends and developing applied sharing mechanisms as used by the US military. War-gaming refers to a simulation where events are affected by decisions of players representing both sides with the red team as the adversary and blue team as the defender (and, in Trexin's variant, also a purple team that represents the Executive Team). By using a realistic scenario exercise as the best information-sharing strategy, cybersecurity staff and leadership should create a quarterly simulation of networks in the virtual world. This military war-gaming model provides realistic scenarios using the typical threat actors in this sector. It also offers leadership an opportunity to work with a multi-disciplinary team to determine the challenges and discuss what worked, what may or may not have worked. Additionally, the model also leads to crowdsourcing best practices among organizations and provides safe mechanisms to share ideas without sharing specifics of one's network. Performing regular war-games with sophisticated threats and new tools in the ever-changing cybersecurity environment offer the opportunity to develop rapid response best practices. Ultimately this will be used to create mission impact models and train teams in a proactive manner.

Cybersecurity requires recurrent continuous testing, authentication safeguards, and adherence. With cybersecurity attacks on the rise, the c-suite executives must integrate risk management with business culture to mitigate threats across all enterprises. Many experts believe the missing element in the healthcare industry is the emphasis on cybersecurity staff. The shift in perception should divert the attention of payers and providers from investing in technology to process and staffing. Healthcare delivery organizations must develop IT departments with cybersecurity specialists with the intent of deflecting malware and creating HIPAA-compliant technology devices. In addition to risk management, cybersecurity professionals must be willing to work with HIPAA protocols, healthcare providers, and IT innovators to transform the healthcare industry. A study by Wombat Security Technologies and the Aberdeen Group

indicated employee training on cybersecurity could reduce the risk of a cyber-attack from 45-70%. It is critical to educate users on multiple platforms with experiential learning and complete a comprehensive overview of the enterprise network. Healthcare delivery organizations need a dedicated sec-op team to handle security, hunt threats, educate staff on latest threats, and perform pen tests. They may also vet business vendors and associates by requiring indemnification provisions, reviewing risk assessments, and associated agreements.

Chief Informational Security Officers (CISOs) must not only know where the devices are located but precisely what they are doing in the network. The CISOs should be looking at targeted areas where they can add to various layers of cyber defense. It is critical to examine the risk of a device's implementation within the facility to mitigate risk. System upgrades and patches must be up-to-date and routinely checked to minimize system vulnerabilities and hacking attempts. An added layer of protection requiring multi-factor authentication and implementing behavioral analytics to identify abnormal patterns of IT access and usage can also prove to be beneficial.

Although healthcare has an open, sharing culture to hold true to its mission, it often complicates the issues of security and privacy. According to Symantec, a leading enterprise security vendor, healthcare companies are notorious for their limited investments in cybersecurity. In a recent report by HIMSS Analytics Healthcare IT Security discovered that healthcare companies are underspending on cybersecurity programs. Cybersecurity is not viewed as a solution to help protect the patient, but historically as an IT challenge and approached reactively in the healthcare sector. Healthcare delivery organizations often lack the infrastructure to identify the threats, the capacity to analyze and translate the threat data into actionable information, and the capability to act on that information. This is why organizations should look for a cybersecurity partner who is experienced enough to be unsurprised by the next vulnerability to be found, and mature enough to work with you on prioritizing a path customized to your industry and strategic needs.

So, Where Are We Heading In 2018?

- Insurance carriers are now deep into preparing 2018 offerings including the development of products, provider networks, and premium rates
- These need to be complete by April or May depending on the state for filing purposes
- They are also adjusting to the Final 2018 Benefit and Payment Parameters published in the Federal Register on December 22, 2016 including:

1. New language requirements for issuers and web brokers
2. New standards for direct enrollment for issuers and web brokers (keeping a customer on the site with a behind the scenes connection with CMS for subsidy calculation and verification)
3. SEP risk adjustment changes
4. Strategies and execution of standardized options
5. Network adequacy changes
6. Out of network out of pocket changes
7. New use of RX data in risk adjustment formula
8. Risk funding changes for high-risk enrollees
9. New risk adjuster issuer data requirement
10. Data validation process
11. RADV discrepancy reporting
12. AV calculator updates

For more information, click **here** to view Trexin's Cybersecurity Practice Area.

This TIP was written by Rushil Desai, a Principal at Trexin, and Glenn Kapetansky, Chief Security Officer. Rushil welcomes comments and discussion on this topic and can be reached at rushil.desai@trexin.com.