CIRCADENCE

Using Gamification and Cyber Range Learning to Bring the Healthcare Industry Back to Life

Re-prioritizing Cyber Professionals, Processes and Technology

A Brief History of Healthcare Cybercrime

The history of cybercrime in the healthcare industry coupled with recent tech advancements have impacted healthcare operations so much that the industry is now in a state of critical condition in terms of its cyber risk. Several pervasive attack incidences have put constraints on security teams and leaders seeking support for the ever-growing threat of cybercrime. The digitalization of healthcare communication and records has greatly impacted how professionals use medical devices, perform patient care, and conduct internal operations. The rapid race to implement electronic health record (EHR) mandates and widespread mobile adoption and telecommunication tools have all driven cybercrime to accelerate at strides faster than CISOs can keep pace.

> More than 300 reported data breaches have impacted more than 16 million Americans[1] and in 2014 and 2015, the healthcare industry became the most attacked industry[2]. More recently, 62 percent of healthcare organizations have experienced a data breach within the past 12 months, with half of those incidents resulting in the loss of data[3].

While several things can be attributed to these attacks, unencrypted, lost and stolen devices along with outdated systems are some causes. Data thieves are stealing financial and billing information from hospitals—even bank account numbers—on laptops with unencrypted drives through phishing scams—not to mention deploying SQL injections, Advanced Persistent Threats, and Zero Day exploits and ransomware.

[1] Snell, Elizabeth "Report Finds 16.6M Affected by 2016 Healthcare Data Breaches," HealthITSecurity.com

[2] IBM, "X-Force Threat Intelligence Index Report," IBM, Accessed 11 April 2018

[3] Ponemon Institute, "2018 Impact of Cyber Insecurity on Healthcare Organizations," The Merlin International Report, 2018

From 2010-2015, lost or stolen devices became the number one cause of breaches in the healthcare industry. Furthermore, the main threats to confidentiality, integrity, and availability of healthcare data were perceived to be unsecured medical devices (78 percent), BYOD (76 percent), and insecure mobile devices (72 percent).[4]

"Outdated systems, lack of experienced cyber personnel, highly valuable data, and added incentive to pay ransoms in order to regain patient data, are magnetizing hackers to the healthcare market,"

– Steve Morgan, founder and Editor-In-Chief at Cyber security Ventures

According to some studies, healthcare consumers log in to twice as many applications compared to the average user. The frequency of access poses security concerns especially if negligent or unaware employees do not log off systems or lock them after use, which is typical. It is these kinds of instances where vulnerabilities are most present.

> Only 29 percent of healthcare organizations are running a modern version of Windows 10[5], further opening the door for a cyberattack to occur.

While credit cards can be canceled when lost or stolen, if an attack occurs on patient data, medical records can be compromised for years on end. Most companies will offer free credit report monitoring for a year to those affected, but that isn't enough reassurance to quench the concerns of patients whose data is "out there" somewhere being viewed and possibly used by someone they don't know.

[4] HIPAA Journal, "Lack of Security Awareness Training Leaves Healthcare Organizations Exposed to Cyberattacks," HIPAA Journal, 9 April 2018

[5] Donovan, Fred "Older Healthcare OSes Open to Cyber security Vulnerabilities," Health IT Security, 23 May 2018

Healthcare organizations across the U.S. are feeling the cybercrime effects, too. Recent incidents of cybercrime in the healthcare industry include:

SSM Health in St. Louis

A former call center employee accessed 29,000 patient records[6] including demographics and clinical information. The former employee did not have access to financial information, according to the statement.

21st Century Oncology of Fort Myers, FL

An unauthorized third party gained access to a company database, putting 2.2 million individuals at risk[7]. Data stolen may have included patient names, Social Security numbers, physician names, diagnosis and treatment information, and insurance information.

UNC Dermatology and Skin Cancer Center

A stolen computer contained roughly 24,000 patients[8] with records detailing names, addresses, phone numbers, birthdates, Social Security numbers, employment status, and employer names.

Sinai Health System in Chicago

A phishing scam affected approximately 11,350 people[9] of the seven-member hospital system. The investigation reported no financial information was compromised but patient information may have been compromised.

Henry Ford in Michigan

A cybercriminal accessed email credentials from a group of employees to view and steal the data of 18,470 patients[10]. While the email accounts were password protected and encrypted, the hacker accessed patient names, dates of birth, medical record numbers, provider names, dates of service, health insurer, medical conditions and locations.

[6] Rock, Amy "SSM Health Data Breach Exposes 29K Patient Records," Campus Safety, 3 January 2018

[7] Goedert, Joseph "Cyber attack on cancer chain affects 2.2 million," HealthData Management, 7 March 2016

[8] Seaman, Jessica "UNC Health Care: Computer stolen from Triad facility potentially exposes patient information," Triad Business Journal, 8 December 2017

[9] Marotti, Ally "Sinai Health System announces data breach but says risk to patients low," Chicago Tribune, 7 December 2017

[10] Davis, Jessica "Hackers breach Henry Ford Health, exposing data of 18,000 patients," Healthcare IT News, 6 December 2017

In Critical Condition—Monetary and Human Costs of Cyber Attacks

According to an IBM-sponsored Ponemon study, a single health record now yields nearly $402[11] on the dark web – almost twice the average in other industries.

When a hacker attacks thousands, or millions of records, the U.S. Department of Health and Human Services has a maximum penalty of $1.5 million per year for each HIPAA violation[12].

In 2016, "Lucky" ransomware forced California's Hollywood Presbyterian Medical Center to shut down all computers and work from "jammed fax lines" and paper records for several days until they paid attackers to release the systems[13]. And it's not just the employees who are affected when an attack occurs. Pressure and panic is even greater when patient care is in question. In 2016, an NHS hospital had to postpone transplants due to a malware outbreak and during the 2017 Wannacry outbreak, NHS again had to divert care to other facilities. The UK hospitals were at a standstill as doctors and nurses were ordered to immediately turn off all computers and patients were told to only attend in emergencies.

Medical device vulnerabilities are another big risk to healthcare organizations and unique to the industry. All 300 of the medical devices tested by the Department of Homeland Security in 2013 failed security checks and in 2015, the first publicized hack to demonstrate the vulnerability of medical devices occurred—shedding light on yet another threat healthcare cyber security professionals deal with.

Understanding the history of healthcare cybercrime and the associated costs of it is important because healthcare organizations will always stay focused on what they do best—providing patient care—yet they can't effectively do that without access to the necessary data and records to communicate with staff/organizations, operate medical devices, partner with vendors, and ultimately, care for patients. More than ever, cyber security in the healthcare industry faces immense threats and vulnerabilities if not proactively addressed.

[11] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," Ponemon Institute and IBM Security, June 2017

[12] Compliancy Group, "HIPAA Fines Listed by Year," Federal Register, Accessed 11 April 2018

[13] Hackett, Robert "Hackers Are Holding a Hollywood Hospital for Ransom," Fortune, 16 February 2016

Lack of Staffing Remains an Ever-Present Challenge

While several challenges exist within the healthcare industry as it relates to cybercrime, lack of staffing remains an ever-present pain point for CISOs. Existing cyber security professionals haven't undergone proper training to respond to attacks and rapidly remediate breaches.

> More than 60 percent of healthcare respondents from the Merlin International Report believed they didn't have the right cyber security qualifications in-house—and only 51 percent[14] of organizations appointed an official CISO.

While healthcare organizations may be used to doing more with tight budgets, the absence of information security skills and talent proves a major risk. Without people to operate and protect the systems from both an offensive and defensive line, hospitals and providers are, in many ways, knowingly putting their data and patients at risk.

Furthermore, small and mid-sized hospitals are even more challenged, so strapped for funding that some organizations are lacking even one IT security person. And the lack of staff doesn't help when info security departments need to expand but don't have the data to justify existing staff, let alone hire new talent.

[14] Ponemon Institute, "The State of Cyber security in Healthcare Organizations in 2018," Merlin International Report, March 2018

Stringent Regulations Aren't Enough

According to Robert Herjavec, founder and CEO of Herjavec Group, *"The fundamental difference between healthcare and other industries…is that it's not just about money. It's about lives."* [15] Based on the historical incidences that have compromised organizational reputation, patient lives, and individual jobs, companies are more vulnerable than ever.

Healthcare companies have responded by ensuring compliance with privacy requirements and protocols, ranging from HIPAA to a variety of state-level and interdepartmental initiatives. Yet, new stringent incident reporting requirements still has the industry on high alert. The U.S. Department of Health and Human Services Office for Civil Rights – HHS OCR – requires health data breaches of 500 records or more to be reported within 60 days of discovery[16].

Additionally, in its 2017 report, the relatively new Health Care Industry Cyber security Task Force cited that *"while the Framework [NIST Cyber security] provides a high-level description of standards and best practices to help organizations manage cyber security risks, it is not specific to the healthcare industry*[17]*." Now the FDA is beginning to provide specific guidance on medical device cyber security.*

> Only 57 percent[18] of healthcare providers have personnel with the cyber security technical expertise needed to identify and resolve breaches – and far fewer have the resources to proactively address issues before they result in a breach.

It's clear that much more needs to be done on the technical level to prevent attacks in the future.

[15] Herjavec Group, "Cyber security Ventures Global Healthcare Cyber security Spending Will Exceed $65 billion Cumulatively Over the Next Five Years, from 2017 to 2021," Cyber security Ventures, April 2017

[16] U.S. Department of Health and Human Services, "Breach Notification Rule," HHS.gov, Accessed 7 May 2018

[17] Health Care Industry Cyber security Task Force, "Report on Improving Cyber security in the Health Care Industry," Health Care Industry Cyber security Task Force, June 2017

[18] HIMSS, "2017 HIMSS Cyber security Survey," HIMSS North America, 2017

What's Next

Healthcare companies need to prioritize a proactive approach to cyber security—balancing PEOPLE, PROCESS, and TECHNOLOGY to improve protection of the institution's assets and patient information.

People 1: Get a people's perspective

Industry analysts, such as Gartner, advocate moving toward "people-centric security[19]," which lessens organizations' reliance on a massive stack of tools and a compliance checkbox mentality in favor of a more powerful human element in fending off attacks and reducing information security errors. After all, when breaches occur, as we've learned above, there is a human component—people clicking on this or that—and recovery from an attack like that can be rough.

To refocus on people, CISOs can begin by talking with their team to understand their knowledge of cyber security. An online survey or focus group/informational interview setting will reveal a lot about what a team knows and where the gaps in knowledge are. This strategy gives a baseline to work with.

In addition to receiving self-evaluations from staff about their competencies and perceived areas for growth, cyber leaders can back up those assumptions with actual data using gamified cyber ranges to test their abilities and knowledge. Unlike compliance-driven teaching methods, gamified teaching engages practitioners individually and in teams, through modern learning strategies. It works by enabling learners to apply what they know to simulated environments or "worlds," creating a natural flow that keeps learners engaged and focused. Further, it can deploy connected, interactive, social settings that allow learners to excel in competitive, strategic situations. Organizations that offer gamified exercises to teams report that 96% of workers see benefits[20] including increased awareness of weaknesses, knowledge of how breaches occur, improved teamwork and response times, and enhanced self-efficacy.

[19] Pemberton Levy, Heather "Lessons in How to Implement People-Centric Security," Gartner, 11 June 2015

[20] Ashford, Warwick, "Automation and Gamification Key to Cyber Security," ComputerWeekly.com, 3 April 2018.

People 2: Seek out qualified cyber security officers using Artificial Intelligence

Staffing continues to be a challenge for healthcare professionals. Finding qualified candidates is getting harder and harder. However, the best info security response protocols are only as effective as the people executing them. Cyber security leaders can build credibility with human resources departments by setting forth qualifications and processes when onboarding new staff.

For example, require candidates to take cyber security assessments, regardless of their skill level and past professional experience. What's on the resume isn't always reflective when it comes to onboarding a new staff member to a new organization. During the interview process, notify candidates of the expectation that they be "students of the industry" such that they are expected to stay on top of security news and happenings and knowledgeable of the latest threats and opportunities.

Likewise, let new hires know of the consequences of carelessness. If they leave computers unlocked or sensitive data laying around for potential theft, tell them what the ramifications will be. They'll understand immediately the importance of cyber security within the company and understand that they, as individuals, have an active and important role in the matter.

Finally, send out quarterly or bi-monthly roundups of the latest cyber security news and events to keep the team abreast of incidents. Making it as easy as possible for them to be "students of the industry" will lower the barriers to entry and likely, get them more engaged from the get-go.

One way to hire healthcare cyber professionals with confidence is to implement a skills assessment program at the onset of hiring. Artificial Intelligence tools can be used to do that by scoring or ranking cyber activity performance in a cyber range environment. This is a valuable function to help CISOs understand where the skills gaps are within their teams, enabling them to put evaluation programs in place to build stronger, cross-functional teams with the right mix of skills to analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend and securely provision. Further, data from the assessment scores can be used to identify new cyber exercises that can be created to keep learning content fresh—saving time and resources for cyber learning managers who are trying to figure out what pathways to develop to best support teams.

Process: Establish company-wide cyber awareness

All people within the organization should play a role in managing overall risk. This effort helps create a culture of protection and proactive response—rather than reactive. This may sound like a nightmare, as each IT, clinical, engineering, risk management, and purchasing department is touched by security gaps, but it's important that cyber security protocols be widely established so each department purchaser knows and understands the value of ensuring security provisions.

> According to the Breach Barometer Report, in 2016, 43 percent of Protected Health Information (PHI) breaches were caused by healthcare workers[21]. About half were accidents, leaving PHI out in the open on a desk, for example; others were employees intentionally prying into patient records just because they could.

To remedy incidences like this, establish regular IT security analyses and systems probing to know who has PHI access and who's logging on and off without the proper permissions. This consistent effort will allow to mitigate risk head-on versus waiting for an incident to explode. Furthermore, on a quarterly basis, roll out a check-in program that reminds people of the protocols they should be following and reward people for improving their procedures. Making it a visible part of the organization helps everyone "see" that security is a priority. Healthcare organizations that invest in persistent cyber learning programs that are suitable for all knowledge and skill levels will provide the organization-wide awareness needed to ensure optimal safety on medical devices and digital record management. Our product inCyt™ can help healthcare organizations engage their staff in conceptual and hands-on learning needed to hone everyone's security responses. Making cyber a visible part of the organization helps everyone "see" that security is a priority.

[21] Protenus, Inc., "2016 Averaged at Least One Health Data Breach Per Day, Affecting More Than 27M Patient Records," DataBreaches.net, Accessed 11 April 2018

Technology: Train cyber teams in safe environments

When it comes to healthcare technology, systems and applications require constant attending to. As we pointed out earlier, medical devices are some of the most vulnerable assets for hackers to exploit because they are left unlocked, not password protected, not updated. To ensure new and old technologies are secure, cyber teams and healthcare professionals alike can "use" those tools in emulated network environments via cyber ranges to test that technologies are running optimally. Practicing using these technologies in "test" environments helps professionals learn how to manage devices and use them safely so when they are doing their actual jobs, they have practiced the skills needed to ensure technologies are secured properly.

> The ECRI Institute put managing medical device cyber security threats as number one on its 2018 list of top 10 challenges facing healthcare[22].

Our premier Cyber Range-as-a-Service platform allows healthcare institutions the opportunity to train in realistic environments that mirror their actual organization networks. The potential of CyRaaS is limitless, with the ability to modeling for entire healthcare networks to develop living physical and fifth domain environments. Combined with Circadence's Project Ares, Orion Mission Builder™, and StrikeSet™, health organizations can learn and grow without impacting operations. This next generation combination transforms traditional lecture-based cyber earning, taking it out of the classroom and into interactive real-world environments, at any scale, anytime, anywhere.

Look for a training platform that focuses on concepts at all skill levels and maintains existing proficiencies for users. Seek out a solution that utilizes repetitive learning techniques like exercises that detail how adversaries gain access to the healthcare network via the kill chain, common protocols used on the network or hexadecimal to binary conversion used in digital forensics. Finally, find a system that catalogues user actions and skills, so the institution has a permanent record of training and skill set progression.

[22] ECRI Institute, "Top 10 Health Technology Hazards for 2018," Health Devices, Accessed 7 May 2018

The Pain Can Be Minimized

These strategies will go a long way in preventing future attacks and preparing staff and systems to respond when things go astray. Creating a culture change is critical. You can't have privacy without good data security and both have to be a part of everyone's job. If patient care is a priority, taking these steps to proactively prepare for attacks will mitigate risk and deflate costs.

Our own Project Ares® AI-powered learning and assessment platform is a recommended investment to start. This gamified training system can successfully prepare the next generation of cyber security professionals in the healthcare industry by offering such things as: pre-engineered missions for industry-specific attack vectors; computerized advisor, umpire and opponents that use deep learning algorithms and natural language processing; and on-demand help and feedback for all levels to facilitate progress.

For a full in-depth overview and demonstration of how Circadence's next generation training and assessment solutions can amplify human cyber security defenses against existing and emerging threats, reach out to us at https://www.circadence.com/contact/ or 303.413.8800.