NAVIGATING HEALTHCARE THROUGH TODAY'S CYBERSECURITY LANDSCAPE

Authored by:
Colin Konschak, FACHE – Chief Executive Officer, Divurgent
Shane Danaher, MBA – Chief Operations Officer, Divurgent
Gavin Tong, MBA – Associate Managing Partner, Gevity

INTRODUCTION

Nearly every day we hear on the news and in social media about some type of cybersecurity issue. Terms once arcane to the public—malware, viruses, hacking, computer breaches, ransomware, to name a few—are now understood on some level by most everyone who uses a computer, whatever their line of work. However, for leaders responsible for providing effective cybersecurity in every business sector, general awareness is not nearly enough. They need to appreciate the level of potential threat and its implications not only for their organizations, but for the future and perhaps even the lives of everyone their organizations touch.

These days, IT security professionals are not facing small-time hackers probing for a hole in a firewall to commit a prank or steal a few passwords or account numbers. In the cybersecurity landscape of today, they are up against highly skilled professionals that include criminals, terrorists and spies, often with significant funding from criminal syndicates and even governments. The cybersecurity environment of today is no longer about hacking—it is about warfare.

On March 15, 2018, the United States announced it would impose long-delayed sanctions on Russian individuals and entities for cyber-meddling in the U.S. 2016 elections, along with other major cyberattacks. During that announcement a startling new disclosure was made: Russians had been caught recently attempting to penetrate portions of the U.S. energy grid. While it is not clear how widespread the attempt was, it shows how seriously we need to take cybersecurity. Major shutdowns in the U.S. energy grid perpetrated with the help of a hostile country would be an unprecedented act of war, and have the potential to be deadlier than any other wartime act or terrorist action the world has ever seen.

LOOKING BEYOND THE NUMBERS TO THE HARM

Highly targeted cybersecurity breaches with big numbers and big names tend to make headlines— Yahoo, Target, Equifax, JP Morgan Chase—but perhaps nowhere is cybersecurity more critical than in healthcare, not only because of distinct inherent vulnerabilities we will explore later, but because of what can be stolen.

Consider the following. When Equifax, one of the largest credit bureaus, was penetrated in 2017, the personal information of 145 million people was taken. The breach was shocking because of the amount of information the thieves gained, including addresses, birthdates, social security numbers and other information that could be used to steal identities.[1]

On May 12, 2017, in a global ransomware attack thought to have been perpetrated by a group with ties to North Korea, tens of thousands of computer systems in more than 100 countries were infected with ransomware, and their data held hostage.

The National Health Service (NHS) in the United Kingdom was hit hard, with at least 40 of its hospitals locked out of their systems while the attackers demanded payment in the form of the untraceable Bitcoin currency.[2]

Hospitals were forced to cancel surgeries and to treat patients without access to their medical records, x-rays, blood tests, and vital information such as allergies. As one doctor told a reporter: it would be a "miracle if no one comes to harm."[2]

Data piracy from healthcare organizations is where true harm comes in because of what can potentially be stolen and what can be done with it. When cybercriminals or cyberterrorists breach hospitals, health systems, medical practices and health insurance companies, they trespass far beyond addresses, birthdates, and social security numbers to some of the most intimate and potentially damaging information about people ever to be logged into a computer system.

Identity theft is big business today and a medical record is worth two or three times what a credit card number goes for on the Dark Web. Healthcare records contain at least 18 protected personal health identifiers, including name, social security number, address, phone, and, often, financial information like credit card numbers. As one expert said: "Your hospital has a greater and broader amount of your private data than your employer or your bank does."[3]

According to a 2016 report from the Institute for Critical Infrastructure Technology (ICIT), the cybercriminals breaching healthcare systems are not only looking for personal identity information, but are sometimes targeting specific high-profile patients or seeking potentially harmful information about healthcare providers.[3] Imagine an attacker steals an HIV patient's medical record and then threatens to share the information about the condition with the patient's employer unless the patient pays the attacker a ransom.

Patient information also contains one extremely valuable asset: health insurance information. This data can be used to create fake insurance credentials, and thieves can get the medical care they need, including prescription drugs, on the patient's dime.

Many leaders responsible for healthcare cybersecurity in the past have been lulled into a false sense of security, many believing healthcare system breaches are lower priority than the high-profile intrusions into commercial and governmental institutions. The breach statistics of the past few years are beginning to tell a different story. These days the U.S. healthcare industry is considered the most vulnerable sector in the commercial economy.[3]

Stories in the news media generate great consternation over attempts to penetrate government systems, such as voter rolls and the IRS, to steal personal identification information. However, healthcare networks are a better source of this and other information because they provide cybercriminals with a bigger pool of potential victims.

According to the 2016 ICIT report, "The vast majority of human beings are in at least one healthcare system, while only a fraction of the population is included in government systems." ICIT adds that, "In general, healthcare breaches have a higher impact and greater fiscal return than government breaches."[3]

Experian's 2018 Data Breach Industry Forecast noted that 233 healthcare system cybersecurity breaches were reported to the U.S. Department of Health and Human Services, the media or state attorneys general just from January to June 2017. That is 52 more healthcare breaches reported than the 181 healthcare breach incidents reported in all of 2016 by Experian's 2017 breach study.[4,5] Table 1 highlights the 10 biggest healthcare data breaches of 2017-2018.

TABLE 1: THE 10 BIGGEST HEALTHCARE DATA BREACHES IN 2017-2018

Business	State	Covered Entity Type	Individuals Affected	Submission Date	Type of Breach	Location of Breached Information
AccuDoc Solutions, Inc.	NC	Business Associate	2,652,537	11/27/2018	Hacking / IT Incident	Network Server
Iowa Health System dba UnityPoint Health	IA	Business Associate	1,421,107	7/30/2018	Hacking / IT Incident	Email
Employees Retirement System of Texas	TX	Health Plan	1,248,263	10/15/2018	Unauthorized Access / Disclosure	Other
CA Department of Developmental Services	CA	Health Plan	582,174	4/6/2018	Theft	Paper / Films
CNO Financial Group, Inc.	IN	Health Plan	566,217	10/25/2018	Unauthorized Access / Disclosure	Other
Health Management Concepts, Inc.	FL	Business Associate	502,416	8/22/2018	Hacking / IT Incident	Network Server
Airway Oxygen, Inc.	MI	Healthcare Provider	500,000	6/16/2017	Hacking / IT Incident	Network Server
AU Medical Center, Inc.	GA	Healthcare Provider	417,000	8/16/2018	Hacking / IT Incident	Email
SSM Health St. Mary's Hospital – Jefferson City	MO	Healthcare Provider	301,000	7/30/2018	Improper Disposal	Paper/Films
Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300,000	7/15/2017	Hacking / IT Incident	Desktop Computer / Network Server

Source: Department of Health and Human Services

In all of the 413 breaches from 2017 - 2018, approximately 13 million individuals were affected, and not all of those healthcare breaches were targeted at the big systems.[6]

Experian is currently predicting that two trends will continue:

- While big healthcare hacks will continue to get the greatest publicity, the small breaches will cause the most damage.
- Healthcare organizations will be targeted more than any other industry sector, and they will be hit with new, more sophisticated attacks.[6]

The attacks are widespread. In its survey of 91 healthcare organizations, the Ponemon Institute found that 89 percent of healthcare organizations had at least one data breach involving the loss or theft of patient data during the past 24 months, and 45 percent had more than five breaches.

In addition, 61 percent of healthcare business associates, defined as persons or entities that perform services for a covered entity that involves personal health information, had at least one data breach involving the loss or theft of patient data in the past 24 months. A third said their organization had more than two breaches.[7]

In 2015 and 2016, half of healthcare organizations said data breaches were criminal attacks, while another 13 percent said breaches were due to malicious insiders, but there is another reason data disappears; 36 percent of healthcare organizations and 55 percent of their business associates said unintentional employee action had allowed the breach.[4]

The attacks put an added burden on already razor-thin margins on which most healthcare entities operate. The average cost of a data breach on healthcare organizations is about $2.2 million, according to the Ponemon Institute, with estimated total annual costs of $6.2 billion.[7]

By 2021, it is estimated that those damages will rise to $6 trillion.[8]

WHY IS HEALTHCARE SO PARTICULARLY VULNERABLE?

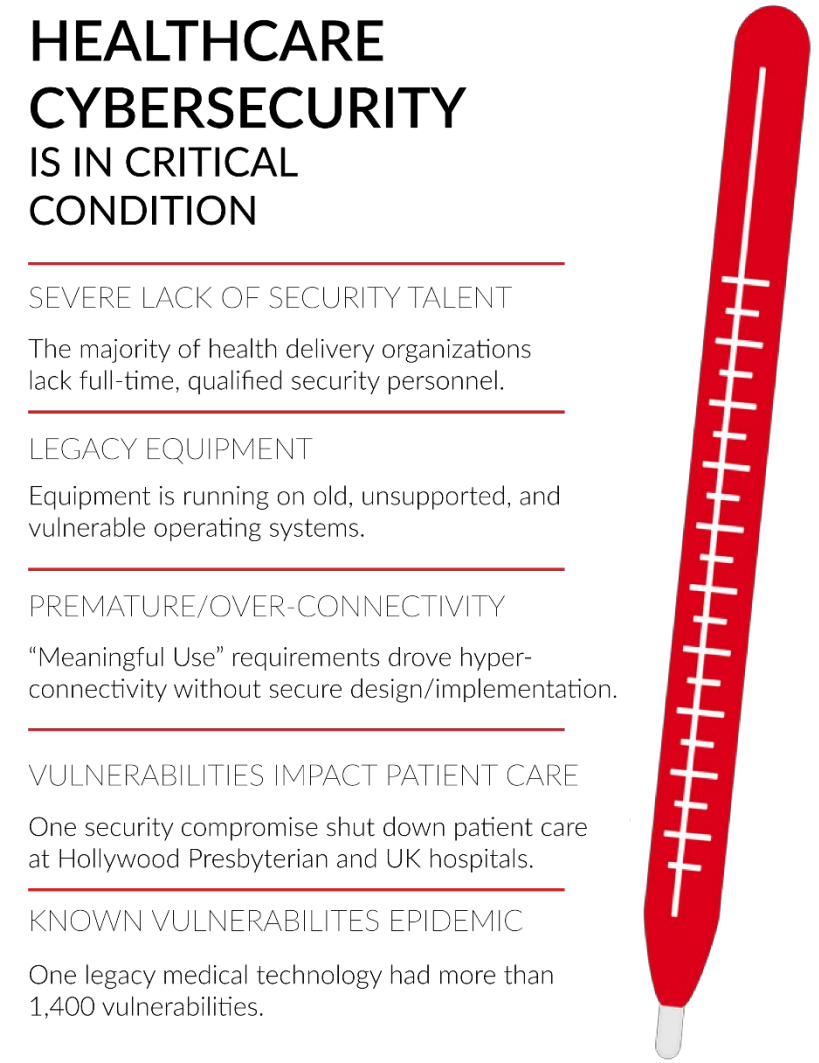
Digital connectivity is critical to the delivery of healthcare today. Yet this digital infrastructure is also one of healthcare's greatest vulnerabilities, putting not just the industry at risk, but every patient who enters a hospital, undergoes a surgery, walks around with an implanted medical device, or takes a drug. A tightrope needs to be walked between secure connectivity, and the hyper-connectivity induced in the pursuit of providing information to both patients and providers.

A 2017 report from the Health Care Industry Cybersecurity (HCIC) Task Force, a committee created as part of the Cybersecurity Act of 2015, concluded healthcare cybersecurity is in "critical condition," identifying five high-level challenges (Figure 1):[3]

- A severe lack of security talent
- Legacy equipment
- Premature over-connectivity
- Vulnerabilities that affect patient care
- Known vulnerabilities that are not corrected

The task force also noted healthcare, which is decades behind other business sectors in protecting information systems, is putting patients at serious risk. Indeed, it concluded, cybersecurity in healthcare needs to be viewed as a patient safety consideration, rather than an information technology issue. Task force members wrote, "Our nation must find a way to prevent our patients from being forced to choose between connectivity and security."[3]

FIGURE 1: HEALTHCARE CYBERSECURITY ENVIRONMENT



Source: Health Care Cybersecurity Task Force. (2017, May). Report on Cybersecurity in the Health Care Industry. Washington, D.C.: Department of Health and Human Services.

HOW WE GOT HERE

As mentioned before, many leaders in hospitals and other healthcare entities have been living in a world of denial. The lack of investment in IT cybersecurity infrastructure has left most healthcare institutions to be better prepared for a zombie attack than a cyber one.

Following the NHS attack in 2017, the New York Times reported, "The ransomware attack on the NHS never should have happened." Over the prior year, the agency had been warned numerous times that its computer systems were outdated and unprotected from attack. That's because the hackers exploited a flaw in newer versions of Windows software used by a great number of business and government entities.

Microsoft issued a patch for these newer versions of the software, but many companies hit by the attacks had never installed it. The NHS, however, was in a worse situation. It was running Windows XP— an ancient version of Windows that Microsoft stopped supporting in 2014. On May 17, 2017, just days after the attack, Microsoft created a patch for Windows XP.

This sounds like an extreme case, but the reality is healthcare IT infrastructure today is riddled with complexities and security gaps. Part of this is due to the piecemeal way in which these systems evolved, with software and hardware purchased from various vendors and jury-rigged to work together.

Thus, today's healthcare organizations have hundreds of systems, with some, like the NHS, still running antiquated applications on legacy hardware. The Centers for Medicare & Medicaid (CMS) Electronic Health Record (EHR) Incentive Program, the Merit-Based Incentive Payment System (MIPS) of the Medicare Access and CHIP Reauthorization Act and other IT adoption financial incentives spurred increased adoption of more robust hardware and software, but it has not been enough to keep pace with technology developments.

The complexity of these systems is such that, often, no single person within the organization has a holistic understanding of how the system operates. Indeed, healthcare IT professionals report that the most common security incident they experience is the exploitation of existing software vulnerabilities.[9]

In addition, the average hospital has thousands of devices and machines with computer chips, ranging from wireless blood pressure cuffs that transmit data into the EHR, to computerized tomography (CT) scanners, magnetic resonance imaging (MRI) machines, and even surgical robots. In a survey of 535 IT practitioners in healthcare organizations, 59 percent said their organizations had more than 300 network-connected devices.[9] But it was the growth of EHR that became healthcare's "Superstorm Sandy." In 2008, less than 10 percent of hospitals had even a basic EHR; by 2014, nearly all of them did.[10] The rush to install the systems is one reason for the mess we find ourselves in today.

Today, attackers can infiltrate the EHR from numerous entry points and, in addition to stealing patient data, they can rewrite the records, changing the patient's medical history. If anything happens to the patient as a result, the hospital or physician is responsible. Yet in a 2016 survey of 91 healthcare organizations, just 19 percent said they had a process in place to correct errors in a hacking victim's medical record.[7]

Other, not-so-obvious targets in healthcare organizations offer additional entry points for attacks. These include closed-circuit television systems, webcams, remote door controls, digital video systems, and video conferencing systems.

Attackers could install malware on all security cameras then watch as an employee punches in an access code for the EHR, locked drug cabinets, or an MRI machine. Increasing the vulnerability of these systems is the fact few fall under the purview of the IT security team, so they are not included in routine system scans or protections.[11]

FINDING GOOD PEOPLE TO FILL THE CYBERSECURITY SHORTAGE

Even as the healthcare industry reluctantly wakes up to the risks of cyberattacks, it faces another challenge: finding qualified people to fix the problems and protect the systems. In fact, nations across the world are grappling with a severe shortage of cybersecurity professionals. In the United States alone, which employed nearly 780,000 people in cybersecurity positions in 2017, about 350,000 jobs were open, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. Experts estimate a projected shortfall of 3.5 million cybersecurity professionals by 2021.[12]

The shortage is particularly acute in the healthcare industry. It's never been viewed as a "sexy" industry for IT cyberheroes, who have traditionally been wooed by Wall Street and corporate America to guard intellectual property and corporate secrets, or by the government to protect national security. Next to those options, the local community hospital looks about as exciting as watching paint dry.

The low salaries and antiquated systems security experts would find on the job also don't help recruitment. Blame budget gaps for that; yet another drawback of IT and cybersecurity not being seen as a priority in organizations where delivering medical care is viewed as the primary mission. People are now waking up to the fact that without computer systems and data, it will be impossible to deliver care in the future.

So, is it any wonder that even today about half of all healthcare organizations say they have little or no confidence they can detect patient data loss or theft? As the Ponemon Institute noted in a 2016 report: "Although there's been a slight increased investment over last year in technology, privacy and security budgets, and personnel with technical expertise, most healthcare organizations still don't have sufficient security budget to curtail or minimize data breach incidents."[7]

Those budgets aren't budging, either. Ten percent of healthcare entities reported their security budgets had been cut, and 52 percent reported they remained the same as the previous year. As the authors of the report noted: half of healthcare organizations still don't have the staff or the budget to detect or manage data breaches.[7]

EXPANDING THE VIEW OF HEALTHCARE CYBERSECURITY

Most healthcare leaders still do not understand the word "hacking," and the image it brings of a 20-something computer wiz playing around is no longer relevant. Rather than nerdy techies, these attackers are highly professional, highly skilled operators. They are part of sophisticated networks, even city-states, bent on not just demonstrating they can get into a system, but on destroying an organization from the inside out, and reaping millions in revenue as a result. They are, in effect, the Special Operations of the hacking world. Again, we are at war. Today, we need to go beyond the thought of "hacking" to the reality of "attacking."

Our attackers fall into three realms: cyberterrorists, who are motivated by ideology and a desire to bring attention to and win their cause; cybercriminals, who are motivated by financial gain; and cyberspies, who are sponsored by a nation-state and operate similarly to an intelligence agency but are, nonetheless, independent.

The organizational sophisticiation of these different types of attackers is reflected in their ability to deliver advanced persistent threat (APT) attacks. APT attacks use multiple methods to gain access to networks and remain undetected for long periods. This allows attackers to learn more about the network and design additional attacks that will support the removal of large quantities of data undetected. The move to cloud based solutions has contributed to the rise of APT attacks. The US Department of Homeland Security issued an alert in October 2018 regarding the rise of APT attacks "attempting to infiltrate the networks of global managed service providers (MSPs)" and that the attackers had targeted Health Care and Public Health among other industries.[14]

Hijacked patient and employee data can be sold on the black market, used to commit fraud and manipulated to change important medical information that could lead to severe harm or death. Theft of research and development materials could be used to manipulate a company's stock; and, most alarming, disruptions in patient care can result from cybercriminals directly manipulating a hospital's information technology network.[3]

As US News and World Report noted: "Hospitals are dinghies in a sea of hacker sharks."[13] Some of our prior practices to make operations more efficient and convenient have in fact caused vulnerabilities, as suggested by the following quote.

> *"There was a time in healthcare that the balance between 'ease of use' and security tilted towards easy access," said Jerry Kevorkian, Chief Technology Officer of Sentara Healthcare. "That tilt is no longer possible in this digital world. Proper security has now taken on the role of ensuring proper care for the patient by guarding clinical data and ensuring that it does not get modified without the proper controls in place."*

In our next whitepaper, we will look at cybersecurity threats that come from the inside of your organization and how you can take proactive measures to educate and enlist your employees in the war against cyberattack.

ABOUT THE AUTHORS

Colin Konschak, FACHE – Chief Executive Officer, Divurgent

Colin is the Chief Executive Officer at Divurgent. He is a highly accomplished executive with over 20 years of experience with extensive experience in healthcare operations, P&L management, account management, strategic planning and alliance management.

His broad healthcare sector experience encompasses pharmaceutical, provider, payer, information technology and consulting. He is a registered Pharmacist, possesses an MBA in health services administration, is board certified in healthcare management and is a Six Sigma Black Belt. Colin is a Fellow in both the Healthcare Information Management System's Society (HIMSS) and the American College of Healthcare Executives (ACHE).

Colin is the author of numerous industry papers and textbooks, most recently co-authoring "Hacking Healthcare: Understanding Real World Threats"; the healthcare industry's only text on the topic of cybersecurity. Colin has been an adjunct professor in both Old Dominion University and William and Mary's MBA program, teaching courses in Healthcare Operations and Strategy.

Shane Danaher, MBA – Chief Operations Officer, Divurgent

As Chief Operational Officer, Mr. Shane Danaher's vision and leadership are intrinsic to his ability to successfully deliver creative, effective, and efficient solutions that challenge and outdo the status quo for healthcare organizations nationwide. As an executive leader of Divurgent, innovation has been a key component of Shane's drive to help providers evolve in payment and delivery reform, as well as patient engagement, providing higher quality of care, lower cost of care, and healthier communities.

Competencies as an analyst have allowed him to utilize research, data, and technology in various ways including: critical access hospital surveys related to hospital IT metrics and correlation and causation with various financial metrics, creation of a tool to maximize quality while reducing cost for hospitals and physician practices implementing an EHR at "go-live" time, and other database technologies to create efficiencies in presenting to and collecting data from physician practices.

As Past President for the Virginia chapter of HIMSS and Senior Member of HIMSS, Shane plays an active role in industry thought leadership. In his membership with CHIME, Shane has attended several CIO forums, and has spearheaded, organized, and attended multiple Focus Groups as a CHIME Foundation Member. Shane also resides on the Board of The Association for Executives in Healthcare Information Security (AEHIS), where he provides his expertise and leadership in cyber-security to other Board members and AEHIS members.

Gavin Tong, MBA – Associate Managing Partner, Gevity

Gavin is an industry thought leader in Health Informatics. He has spoken at numerous conferences and has published dozens of articles in industry journals, trade magazines, and newsletters. Gavin is passionate about the creation of secure, interoperable systems that provide the information needed to achieve the triple of aim care – improving the patient experience of care, improving the health of populations, and lowering the per capita costs of care.

As the Associate Managing Partner for Architecture and Standards, Gavin has been accountable for numerous Threat and Risk Assessments (TRA) on highly integrated healthcare systems. He has helped organizations harmonize their security requirements and has assessed numerous EHRs against hundreds of controls from ISO and CIS.

Gavin routinely applies principles and best practices from TOGAF 9.1®, ITIL, Prosci®, COBIT 5, and PMBOK® to his engagements. Gavin is highly adept at communicating complex concepts in simple, easy to understand terms applicable to the audience. These skills allow him to generate consensus and support from stakeholders at all levels of an organization.

REFERENCES

1. *Larsen, S. (2017, December 20). The hacks that left us exposed in 2017. CNN Tech. Retrieved from http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html*
2. *Bodkin H, et al. (2017, May 13). Government under pressure after NHS crippled in global cyber attack as weekend of chaos loom. The Telegraph. May 13, 2017.*
3. *Institute for Critical Infrastructure Technology. (2016, January). Hacking Healthcare IT in 2016: Lessons the Healthcare Industry Can Learn From the OPM Breach. Washington, DC: ICIT*
4. *Experian. (2018). Data Breach Industry Forecast.*
5. *Experian. (2017) Data Breach Industry Forecast.*
6. *Health Care Industry Cybersecurity Task Force. (2017, May) Report On Improving Cybersecurity In The Health Care Industry. Washington, DC: Department of Health and Human Services.*
7. *Ponemon Institute. (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data.*
8. *IT Strategy Inc. (2017). New Threats in Healthcare Cybersecurity: 2017.*
9. *Ponemon Institute. (2016). The State of Cybersecurity in Healthcare Organizations in 2016. February 2016.*
10. *Office of the National Coordinator for Health Information Technology. (2017) SAFER: Safety Assurance Factors for EHR Resilience. Washington, DC: ONC.*
11. *Filkins, B. (2014). Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. North Bethesda, MD: SANS Institute.*
12. *Herjavec Group. (2017) Cybersecurity Jobs Report.*
13. *Yaraghi N. A Health Hack Wake-Up Call. (2016, April 1). US News and World Report. April 1, 2016. Retrieved from https://www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call. Accessed June 19, 2017.*
14. *US Computer Emergency Readiness Team. (2018) Alert (TA18-276B) Advanced Persistent Threat Activity Exploiting Managed Service Providers. https://www.us-cert.gov/ncas/alerts/TA18-276B*