CISO | information security workshop

The Intersection of Business & Security

Cybersecurity: Building Secure Connected Healthcare Organizations

A Workshop Overview

TH&W

VANDERBILT UNIVERSITY
OWEN GRADUATE SCHOOL OF MANAGEMENT

Center for Digital Strategies
Tuck at Dartmouth

Cybersecurity:
Building Secure Connected Healthcare Organizations

An Executive Workshop for CISOs*

On Friday November 18, 2016, the Center for Digital Strategies (CDS) at the Tuck School of Business at Dartmouth and the Owen Graduate School of Management convened a workshop for information security executives in the healthcare industry. The day-long workshop was designed to foster an open dialogue about information security challenges, best-practices, trends, and opportunities.

The workshop was conducted in "Old Mechanical," one of the oldest buildings (1888) on the Vanderbilt University campus, and the former home of the mechanical engineering school. Twelve information security professionals attended, representing Cerner, Cardinal Health, Community Health Systems, Hospital Corporation of America, Humana, Indiana University Health, Juniper Networks, Kindred Healthcare, Lifepoint Health, Novartis, RCCH Health Partners, Vanderbilt Health, and Willis Towers Watson.

Also participating were Eric Johnson, dean of the Owen Graduate School of Management (co-moderator); Hans Brechbuhl, the executive director of the CDS (co-moderator); Don Castle, an executive fellow at the CDS; David Kotz, the Champion International Professor of Computer Science at Dartmouth College; and Todd Hudson, Special Agent in Charge of the Secret Service's Nashville Field Office.

The workshop was funded by a National Science Foundation grant led by Kotz, called Trustworthy Health and Wellness (THaW). THaW, according to its mission, "to enable the promise of health and wellness technology by innovating mobile- and cloud-computing systems that respect the privacy of individuals and the trustworthiness of medical information." For more information, see thaw.org.

The agenda for the workshop was comprised of four discussion sessions and a presentation by Todd Hudson on the Secret Service perspectives on the shifting cyber threat.

**This workshop was supported in part by the National Science Foundation under award number CNS-1329686. The views and conclusions contained in this document are those of the participants and authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsor.*

Key Insights Discussed in this Article:

- **Perhaps more than any other industry, healthcare requires cyber security** coordination and communication among different business entities. Regional and local hospitals, physician practices, insurance companies, patients, pharmaceuticals, vendors, and patients must all participate.

- **CISOs in the healthcare industry juggle a lot of responsibilities**. CISOs in this sector don't just handle information security; they are often tasked with data retention, protecting privacy, and even maintaining physical security of facilities—all in an industry where individual privacy is paramount and sacrosanct.

- **Common pain points include data, systems maintenance, personnel, and third party management.** The common thread in these challenges is keeping a secure conduit between information, systems, and human beings. Each waypoint represents a security risk.

- **Medical device security is top of mind for 2017.** These devices, if hacked, could injure or kill patients: that's the ultimate healthcare information security threat.

- **Patient portals are a two-sided threat.** CISOs need to secure the front door, where patients log in. But they also need to secure the back door, where the data is stored and where third parties might have access.

- **The Secret Service is a resource for CISOs.** It will discuss the latest criminal trends and tactics with CISOs, and will be responsive to request for assistance with data breach investigations.

- **The Internet of Things (IoT) is a massive risk that the industry doesn't know how to manage yet.** A distributed network of internet-connected machines can become computing power for hackers. Likewise, compromised building controls can disrupt the care delivery process and harm patients.

- **Phishing training programs work.** Sometimes it takes repeated lessons and examples of phishing attacks, but these educational programs are the best tool for awareness and training employees on identifying phishing messages.

- **Board meetings are an important time for CISOs to garner top management support for what they do.** The key is brevity and clarity; the board members don't want to sit through a long, technical discussion of cyber security.

Introduction

The US cyber health ecosystem represents diverse participants including multi-national corporations, small private providers, payers, suppliers, governments, and individuals. Combined with this business layer is the rapidly expanding networked device layer of the internet of things (IoT). The evolution of medical devices has radically transformed the treatment of many acute and chronic illnesses. Intelligent adversaries exploiting vulnerabilities in any part of this ecosystem create incidents that rapidly propagate to unsuspecting members. Hospitals, suppliers and payers alike face risks ranging from theft of private information, hold-ups for ransom, denial of service attacks, and fraud. Individuals face risks ranging from privacy violations to medical identity theft and personal harm. In the increasingly connected healthcare delivery system, innovative solutions are required to ensure uninterrupted communications, service availability, and protection of critical individual, corporate or government data and information.

CISOs in the Org Chart

Across the corporate landscape, CISOs usually report to a variety of C-suite executives. This reflects the increased importance and growing responsibility of the CISO role, as data breaches have been proven to have wide-ranging and costly consequences. Furthermore, the CISO role has been recognized as not limited to technology, because cybersecurity is an enterprise-wide risk management issue, not solely an IT issue.

CISOs in the healthcare industry, as represented by the attendees at the workshop, mostly report to the CIO, and they maintain good relationships with other related parts of their organization, such as the COO, the CFO, the chief data officer, the ethics and compliance department, and privacy and risk management.

Pain Points: Data, People, Third Parties and Outdated Systems

The sheer amount of data being created today is mind-boggling, and more data has been created in the last two years than in the history of the human race. By 2020, it is predicted that 1.7 megabytes of new information will be created every second of every human being's life. So, it's no surprise that managing data is a top pain point for CISOs in the healthcare industry. For one, there is too much data to properly tag and analyze, which means many organizations simply don't know what they have. Furthermore, much of that data is in the cloud, and some of it is being accessed from mobile devices, which makes data security even tougher.

Personnel play a key role in protecting data, because oftentimes hackers' entry point is through people who unwittingly reveal their passwords, click on a phishing email, use a particular device that hasn't (or can't) be patched, or copy data through un-secure USB ports. Among the participants, the best practice for passwords is complex passwords, changed every 90 days. One company requires very complex passwords, changed every

180 days. Some use, or are looking at using, password safes. Another best practice is blocking G-mail (and similar personal email accounts). Employees can send to and receive from Gmail, but cannot load Gmail on company computers. Some organizations configure employee computers to use VPN as the only path to the Internet, so all traffic must come back inside the company firewalls.

Top management can unwittingly be data security vulnerabilities. They are very busy, often believe they do not deal with sensitive data such as patient data, and can actually be targeted individually by hackers. Sometimes top physicians work in remote locations and are less involved in data security discussions. Best practices for managing these "people challenges" include recognizing they are busy people and giving them education in quick bursts, meeting with them individually and showing you understand their pressures, and explaining how they can be a specific target.

Third-party management is another major pain point. Organizations regularly contract with vendors to provide services, and part of that relationship sometimes includes giving the vendor access to the organization's systems and data. Vendors therefore need to be fully assessed and qualified before being given access to an organization's information, but that assessment is difficult and costly. One best practice is to use a short, impactful vendor questionnaire to help identify those current and potential vendors with insufficient security policies and practices. Vendors with excellent practices are allowed to continue working with the healthcare company's data and systems. Those who do not pass are subject to a more in-depth security audit. Finally, whenever considering a new or upgraded application from an external vendor, one best practice is to first download the new application into a sandbox and investigate it for security risks.

Managing systems presents an additional (if obvious) challenge. Some systems are outdated but still in use, which leads to security and reliability issues. Other systems have been decommissioned, but their residue of data must be dealt with.

Phishing Training Programs Work

Phishing scams are one of the most common ways for hackers to obtain sensitive information for malicious reasons. Organizations can combat this activity by educating employees about what a phishing email looks like. For healthcare organizations, this education often takes place through an internal ethical phishing campaign that happens periodically through the year—and doctors and executives should get special attention. These campaigns train users about phishing practices and help the organization identify high-risk users who fall victim to phishing scams more than the general population. These users, in turn, can be educated more intensely or risk being punished if their high-risk behavior continues.

Best practices among the participants include:

(i) Framing the message in terms of personal loss ("Your paycheck could be diverted by a phishing scam") rather than in terms of gain ("Your

information will be more secure if you pay close attention to where emails are coming from");

(ii) Gamifying phishing campaigns and offering prizes for good performance;

(iii) Making the message related to home life ("Here is how to be more secure with your personal computer devices and data at home", or "Here are some practices you should have your children use").

One company even gives away virus protection for employees and their families. Another organization has had good results with a phishing awareness campaign in the form of a comic book. The comic book tells a true story of how hacks have happened, and shows how easy it was for criminals to get data from unsuspecting individuals.

There are other best practices to reduce the success of phishing scams. Some organizations use country blocking—only allowing their servers to receive email from a limited set of countries. Another method is aggressive reporting and the use of an internet proxy server. Outbound throttle control also helps, because it can alert the organization when a compromise leads to large-scale exfiltration of data.

Patient Portals

Patient portals at healthcare organizations are increasingly common, and they represent a huge potential security risk. The threat begins on the front end, where patients use a username and password to log-in to their account. If people use weak passwords, or if the answers to security questions can be easily found on the internet, then the portal can be breached without much effort.

A set of best practices revolves around more patient education. Patients need to be aware of the security risks of using mobile phones to access their data—these devices are often full of security holes and pose a challenge for organizations to secure. Furthermore, patients need to make sure their computers are running the latest operating system, and they need to assent to multi-factor protection (although there is a risk of scaring people off the portal if you push too hard on multi-factor authentication). Unfortunately, patients often believe that the healthcare organization is fully responsible for the security of their data; patients need to understand that they themselves play a major role. Patients must be accountable for their own habits and behavior around information security, and should be aware that it doesn't take a genius to hack their account—the average criminal hacker can do it.

If the patient login is the portal's front door, the back door are the APIs established for access to patient information by mobile apps. Unfortunately, these ports and their APIs are can become a major vulnerability, because hackers can script computers to attack repeatedly via these APIs until they find a path in.

Growing Risks for 2017: IoT, Medical Device Security, Ransomware (and more)

In the healthcare environment, the Internet of Things (IoT) includes a wide range of networked medical devices like CTs, MRIs, and infusion pumps. These devices are remotely supported by the manufacturer, and many times this vendor will embed software into the devices that may not be secure. Because clinical engineers are often in charge of these medical devices, it's important to bring them into the information security conversation before the purchase occurs—especially because rogue vendors have been known to use clinical engineering contacts to get around the IT staff.

Unfortunately, networked medical devices can be remotely compromised, either as a means for extracting personal health information or, in the worst case, loading incorrect treatment parameters that lead to patient injury or death. This would be a nightmare scenario for healthcare security, and would be a transformational event that could cause an incredible amount of damage to people and organizations. Not surprisingly, it's a key concern for CISOs in 2017.

The challenges of IoT go beyond medical devices to include home-care or consumer-grade health and wellness devices. Anything with a camera or microphone can be used to watch or listen, and patient-managed technology is often not well configured or maintained for strong security. Furthermore, IoT also includes infrastructure like power systems, oxygen supplies, and HVAC equipment: a broad category of things that, if hacked, could harm patients or significantly disrupt patient care. The scope of IoT is so large, it's hard for organizations to get an inventory of what exists, which makes it impossible to completely manage the risk.

The IoT risk extends beyond the walls of the healthcare organization. Sometimes patients are sent home with sophisticated devices that can communicate with the hospital via the patient's wireless router. Healthcare organizations need to make sure those devices have a secure way of communicating, without depending on the patient to correctly configure or secure either the device or their home network. These devices are regularly transmitting private data that, if breached, could cause massive disturbances and distrust in the system.

Finally, IoT has the potential to be used as computing power in a denial-of-service attack inside or outside the organizational network. If that happened, healthcare organizations would have no immediate way to stop it, since the attack is coming from a widely-distributed network of unknown size, location, and identity.

Other top-of-mind issues for 2017 include data classification and network segmentation, finding better ways to enable employee and patient self-service, and getting ahead of the next generation of ransomware. Ransomware, if not guarded against, could hold data hostage and is a reportable breach, so CISOs need to proactively monitor for it.

The Secret Service Can Help with Cybersecurity Breaches

Congress gave the Secret Service authority to investigate cybercrime in the 1980s. With the increase of data breaches in recent years, the Secret Service has expanded its outreach to CIOs, CISOs, CFOs, chief counsels, and other C-suite members. The rationale for this is that when boards of directors are actively involved and aware of the cyber threat landscape, companies are much better positioned to deal with it.

Cybercrime is one of the most dominant, fastest growing security threats to businesses. After examining multiple breaches, it has become clear that there are few, if any, perimeter technologies that can guarantee safety from intrusion.

Despite large investments to protect IT networks, U.S. companies are being hacked far more than any other country. There is recognition on national level that we need to do something different. We can no longer rely on the model of individual entities trying to protect themselves in isolation. Not only should information sharing occur across industry sectors, but to the extent possible, sharing of cyber-attack indicators and threat intelligence should also be shared peer to peer.

How do we categorize attackers? Hacktivists are those who want to maximize disruption and cause embarrassment. Criminal hackers are those who are out for financial gain through forcing wire transfers or stealing credit card information. Other times, criminal hackers may steal non-payment related data, such as PII, which can be easily converted into cash. They are selling this information on the dark web. Nation-states represent the most advanced, persistent cyber threat and usually target government and corporations. Their methods tend to be sophisticated which increases time of penetration to time of detection. This translates to more damage and a longer, more difficult recovery. We need to close the gap between when attackers get in and when we detect them.

Criminal investigations have revealed a few cybersecurity trends. First, a surge in ransomware that has led to the choice of losing data or paying the ransom. Second, the lines separating nation-states, criminal hackers, and hacktivists are beginning to blur. Third, business email compromises are on the rise, primarily affecting companies who conduct wire transfers.

CISOs at Board Meetings: Brevity is Best

The security breach at Anthem BlueCross BlueShield in 2015 got the attention of boards of healthcare companies everywhere. Now they understand the importance of a CISO role and what it could mean if a security vulnerability is exploited. For that reason, and others, boards now require CISOs to make presentations at board meetings, sometimes annually and in other cases semi-annually or quarterly. The challenge for CISOs at board meetings is giving board members enough information about the status of the information security landscape at the company, but not so much information that it overwhelms them. How much to present depends on how much time one gets. Some CISOs get just 10

minutes, others get an hour. In any case, the goal is to educate the board about the company's security plan, and to make sure they are confident the plan is being implemented correctly and according to best practices. One best practice is to show the numbers that illuminate how much of the company's activity falls within the acceptable risk range, and how much of it exceeds that range. Another best practice is telling a bit of a narrative around how the company is moving from a *reactive* to a *proactive* to a *predictive* model of security.

Table Top Exercises: Preparing for a Problem

A best practice followed to some extent by every participating company is to do table top exercises to prepare for handling a security breach. It is never a good time to determine what to do when you are going through an actual problem. The frequency varies from twice a year to quarterly, to one hour a month—each time exploring a different situation. Many companies run Red Team / Blue Team exercises, where one team thinks like the hacker trying to thwart the efforts of the company to overcome a breach. One company recently practiced how to deal with a ransomware situation, including the CISO, CEO, legal department, public relations, and more, addressing the technical breach, deciding whether to pay ransom, addressing whether/how to involve the authorities, and discussing what to say to the public.

Conclusion

The healthcare industry requires cyber security coordination and communication among different business entities. Regional and local hospitals, physician practices, insurance companies (payors), pharmaceutical companies and all manner of vendors and facilitators have to engage with each other and collaborate as the stakes are higher than in almost any other industry. And patients have a key role to play in this whether they appreciate that or not.

Participant List

Hans Brechbühl *(co-moderator)*	Executive Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Scott Breece	CISO Community Health
Don Castle	Executive Fellow Center for Digital Strategies Tuck School of Business, Dartmouth College
Paul Connelly	VP & CISO Hospital Corporation of America
Ollie Green	CISO Vanderbilt University Medical Center
Andy Heins	Senior Director, Information Security Lifepoint Health
Todd Hudson *(speaker)*	Special Agent in Charge United States Secret Service
Bart Hubbs	CISO RCCH Health Partners
Terrie Jennings	ISO, HIPAA Security Officer, Infosecurity Integration Director Willis Towers Watson
Eric Johnson *(co-moderator)*	Dean Owen Graduate School of Management Vanderbilt University
Don Kleoppel	CSO Cerner
David Kotz	Champion International Professor Department of Computer Science Dartmouth College
Charles Lebo	VP & CISO Kindred Healthcare

Jeff Moore	Global Head of Security Novartis Institutes for BioMedical Research
Jon Moore	CISO Humana
Mitch Parker	Executive Director of Information Security and Compliance Indiana University Health
Sherry Ryan	CISO Juniper Networks