CISO | information security workshop

The Intersection of Business & Security

Digital Transformation: A Secure Connected Healthcare Ecosystem

A Workshop Overview

TH&W

VANDERBILT UNIVERSITY
OWEN GRADUATE SCHOOL OF MANAGEMENT

Center for
Digital Strategies
Tuck at Dartmouth

Digital Transformation:
A Secure Connected Healthcare Ecosystem

An Executive Workshop for CISOs

The Owen Graduate School of Management and the Center for Digital Strategies (CDS) at the Tuck School of Business 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 threats, best-practices, trends, and opportunities.

The workshop was conducted in “Old Mechanical,” one of the oldest buildings on the Vanderbilt University campus, and the former home of the mechanical engineering school. The participating organizations were Avadyne Health, Cardinal Health, Change Healthcare, Community Health Systems, Emory University, HCA Healthcare, Juniper Networks, Kindred Healthcare, LifePoint Health, Parkview Health, Premise Health, RxBenefits, and Vanderbilt Health. M. Eric Johnson, dean of the Owen Graduate School of Management and Hans Brechbuhl, executive director of CDS co-moderated.

The workshop was funded by a National Science Foundation grant called Trustworthy Health and Wellness (THaW). THaW, according to its mission, “tackles many of the fundamental research challenges necessary to provide trustworthy information systems for health and wellness, as sensitive information and health-related tasks are increasingly pushed into mobile devices and cloud-based services.”

Key Insights Discussed in this Article:

- **Information security threats are coming in new forms, from new directions.** From data tampering to BYOD issues, risks are proliferating.
- **Vendor security is becoming more difficult and more important**. Vendors are accessing data in more ways than ever, and the number of vendors is growing.
- **Medical devices are a growing security risk and a real worry for CISOs.** New medical devices are still being built without a strong security mindset, and being used more often in locations outside of care facilities including patient homes.
- **New devices, software and strategies are emerging to keep information more secure.** Solutions are coming in many shapes and sizes, representing a fragmented approach to information security problems.
- **There’s no consensus on where information security lands on the org chart.** Most agree it depends on the corporate structure and culture at each organization.
- **CISOs are working to share ownership of information security risks across the organizations.** Creating buy-in outside of a traditional security roles and documenting responsibility for the people closest to the risks is imperative.
- **There isn’t a talent gap in the information security workforce, but a skills gap.** The challenge is to train people to apply their talent in a security role.
- **Getting sufficient resources for information security is about showing ROI and total cost of ownership.** CISOs are wise to frame information security costs in terms of their role in responding to and reducing risks.

The workshop was funded by a National Science Foundation as part of a project called Trustworthy Health and Wellness (THaW) - CNS-1329686.

Introduction

The health ecosystem represents diverse participants from large corporations to individual practices: Care providers, outsourced service providers, pharmacies, pharmaceuticals, claims processors, payers, device manufacturers, and other suppliers/vendors. Arguably more than any other value chain/network in any industry, these healthcare players must be able to share information and provide services securely in a world undergoing digital transformation. 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, denial of service attacks, and fraud. Providers and device manufacturers face risks from device compromise. Individuals face risks ranging from privacy violations to medical identity theft and personal harm. In the increasingly connected health delivery system, innovative solutions are required to ensure uninterrupted communications, service availability, and protection of critical individual, corporate or government data and information.

New Threats from New Directions

There is general agreement that information security threats are morphing and becoming more creative and destructive. It makes a CISO want to close and lock all the doors.

A newer threat vector is health care data tampering, which requires a restructuring of the data architecture to address. There's also unconscious tampering, like when people share their Fitbit with a friend. A challenge with this threat is that it's hard to tell when data has been manipulated.

Another threat, which became more evident after the Nuance hack, is memory-based credential harvesting. The Nuance hack leveraged credentials that were in the memory of the compromised machines, then used those credentials to spread the hack. "Not many of us have things in place to prevent that," one CISO said. "I think credential harvesting is going to be a threat going forward. It spread from a tiny finance company in Ukraine. That's my disaster scenario."

BYOD continues to be a concern for CISOs, as it allows all sorts of unsecured devices onto networks.

Finally, phishing emails are extremely complex and realistic—some CISOs admitted they had a hard time discerning some phishing emails. Phishers today will engage in social engineering, pulling personal information from social media, LinkedIn, and even local newspapers to impersonate an email that the reader would be drawn to click on.

Vendors and InfoSec

Healthcare vendors are often critical to patient health, but they are also a large and growing information security risk. Some healthcare organizations have hundreds or thousands of vendors connecting to their network, accessing patient data, sending it out, and then feeding it back in with treatment recommendations. Another common concern is the lack of visibility into cloud providers. CISOs are dealing with these sorts of risks in a variety of ways. Some are systematically studying how many tunnels lead to vendors, and then monitoring those tunnels to see what information is going in and out. In some cases, healthcare orgs are putting up firewalls between themselves and their vendors, and working on establishing standards for building segmented connections. Organizations are also examining their list of vendors to see which ones are still valid. As one CISO put it, "you need to constantly reevaluate the vendors' risk to your company."

Medical Devices Continue to be a Security Risk

In the evolution of information security awareness, many medical devices today are where SCADA devices were 15 years ago: they're designed without significant security safeguards. Regulators are starting to realize this, but it will take a time for regulations to work their way through the supply chain, and more significant risks will be coming soon.

Some medical devices stay inside the walls of a hospital, so the task there is to identify the devices and secure them. But as healthcare extends into the home (and into bodies, with implantables), and telehealth becomes more pervasive, security risks from medical devices will spiral upward. Some organizations have done risk assessments on telehealth vendors, and the results have not been good. The risks associated with medical devices can come from aging infrastructure, negligent design, as well as user ignorance (or ambivalence) about security.

Some solutions are bubbling up:

- One organization is testing a product that can find USB-connected devices on the network and tell you more about them. Then the organization can work with the device manufacturer directly to learn how their device works and what its weaknesses are. The product also allows the organization to lock the device so it can't be inappropriately activated. "It's been a big win for us," the CISO of the organization said. "It has given us a lot of visibility and helps separate what infosec owns versus what other departments own."
- Another product has been developed that sits between the medical device and the network, acting as the gatekeeper between the two. One challenge with this product is not disrupting patient care.
- Another organization puts its materials management team in charge of securing medical devices. These workers are certified to work on medical devices, and they have helped gather data about the devices and contribute it to the database.

New Strategies are Improving Security

Despite the ever increasing security threats, some measures are working to reduce risks. There is general agreement that two-factor authentication is an effective protection. One CISO recounted how his entire organization switched to two-factor authentication 18 months ago. It took six months to roll out, but it decreased the volume of compromised accounts by 98 percent. Many organizations are using Duo for their two-factor authentication management.

Another effective strategy is a blue team/red team pen test, where a third party tests systems in a sandbox. There are two hackers, one from each side, and a third person monitoring it from the SOC to see how the resources are handling the attack.

On the vendor front, organizations are trying to standardize their vendor questionnaires, which can increase transparency and the timely discovery of potential problems.

Anti-phishing campaigns are also very popular and seem to work. Sometimes, they work too well, making people afraid to open email at all. A solution has been to flag external senders and make it obvious when emails are from internal senders. Some organizations are adding a way for people to more easily report suspected phishing attempts, such as a “PhishMe” button that sends the email to the infosec team for their review. One CISO recommended software called Triage for phishing management.

When employees don’t heed warnings about phishing, some organizations are implementing graduated consequences. For example, after the second violation, they need to watch a 10 minute video; after the third violation, a 30 minute video; subsequent violations can lead to temporary or permanent suspension of internet access.

Many organizations are phishing their board members to test to vulnerability. Other strategies for board member security are to create special email accounts for members (with multi-factor authentication) and creating a board-specific portal for sensitive corporate information.

CISOs wish there was a way to prevent threats from even getting into the environment, but they acknowledge that it’s a non-stop problem, in some cases especially for staff at the VP-level and above who are most likely to open phishing emails. The advances in phishing add to the reactionary nature of many of the CISOs’ responsibilities. They feel they are constantly addressing ever-changing threats and can’t take a proactive approach to predicting future security gaps.

One CISO commented that he examines cloud service providers and endorses the ones he likes. “Does the provider give you the right knobs to fiddle with? If yes, you need to actually fiddle with those knobs and inform people how to use it. Sometimes you have to have user constraints on certain types of data. It works, but doesn’t stop someone from using unsupported solutions.”

Spreading the Responsibility for Cyber Risk

Many CISOs are noticing and implementing a more integrative approach to information security. One way this is happening is by addressing risk responsibility in the specific teams that are creating the risk. The infosec team, for example, is teaching other departments how to build security into their systems and automate security measures. “That takes the infosec team out of the position to stay on top of it, and that’s a good thing happening from this tech revolution,” one CISO said. Another CISO spends a lot of time on infosec agreements, training hospitals how to participate and teaching the legal team how to understand security risk. A CISO of an organization with call centers thinks a lot about how to help employees authenticate callers, to make sure the caller has the authority to obtain patient data. “We spend a ton of time on credential management with staff,” the CISO said.

CISOs are in agreement that responsibilities for infosec should not only rest on the infosec team. The risks affect the entire organization, and many departments contribute to the risk, so the responsibility and awareness should be broadly spread across the organization. Many CISOs are forming (and sitting on) risk committees, along with the CIO and chief risk officer. These committees are reviewing cyber risks across the company.

“That’s helped us get a seat at the table in strategy conversations,” one CISO said. “As they change business units and re-organize, we are visible early in the process, where we used to be the last step.”

Other organizations convene a security governance meeting every month and maintain a risk register. This register assigns each risk to a specific team or staff member. That staff member (or business owner) speaks at the governance committee each month, giving updates on the risk they are in charge of. For example, one organization has a clinical application that has been exposed to the internet through an acquisition. It’s a vulnerability and the infosec team has witnessed some activity behind it. They’ve tried to get it behind a firewall, but it’s tough. The business owners of that application have been giving updates to the governance committee every month. In addition, the CISO has been sending a monthly executive dashboard to the CFO, COO and board of directors, showing the top risks and what the company is doing about them.

This type of arrangement can help CISOs be change agents in their organization, or act like the Navy SEAL team: identify risks and get help to take them out.

CISOs agree that the higher you can get the risk exposure in the org chart, the better. Make sure the board knows the biggest risks—it helps get resources and programs in place.

Where Does InfoSec Fit in the Org Chart?

About half the CISOs said their department reports to IT, while the other half report to other departments. Reporting to the CIO is fine if (s)he is a security-minded person, but if not, it's probably better to report to someone who can let you be more influential. One CISO said his organization moved infosec out of IT a few years ago. It ended up creating an "us versus them" mentality between IT and security. But to maintain a security voice outside of IT, that organization has separate teams for technical infrastructure and the non-technical components (the side that works with operations, clinical, legal). "That's driven a lot of efficiencies," the CISO said. Where InfoSec sits within an organization is important as many teams move to create company-wide awareness of risk. "The right choice for security to report to depends on company culture."

A Skills Gap, Not a Talent Gap

There's an urgent need for smart and effective infosec workers, as the security risks are proliferating and becoming more complicated every day. One CISO recruits from local colleges, where he gives presentations and works with professors and deans to get connected with top students. The top couple students are usually scooped up by Fortune 50 companies, so it's hard to compete for them. When he recruits new employees, they go through an extensive internal training program, and there are more junior people in positions of responsibility than usual. This CISO doesn't just target computer science graduates, but mechanical, civil and biological engineers. A lot of their talent lies in critical thinking.

There is a general consensus that there's not necessarily a talent gap, but rather a skills gap. A company can train talented people to have the requisite skills. As companies start to take advantage of cloud offerings, the skills necessary are changing. Recruits need to be security/development/operations minded, with the abilities to orchestrate and automate, and code with Python. Companies also need people who can operationalize what they're good at and turn their skills into procedures that others can follow.

At least one company is adding a new type of worker: a business security officer, who works with non-security personnel to help them understand security requirements. Another CISO accomplishes the same goal, but in a different way. She asks someone from each business unit to act as a liaison to the security team, which helps address risks that exist outside of IT. "No one is addressing these risks until these liaisons come into the fold and identify risks and put them in the matrix," she said. "Resiliency is one example of non-IT risk." Some companies are hiring specialists to focus on Amazon Web Services cloud security. Everyone agrees that if you reward people for security, they will focus on it more intensely.

Making the Case for Security Resources

It can be difficult to show the return on investment of security dollars, because it's hard to quantify the cost of events that were prevented. One CISO told the group what he does: His team identifies areas where the company needs to spend money—maybe 18 different items. Then he goes through each one with the CIO and shows how much it would cost in current and recurring dollars and resources. They then take the list to the president's cabinet with their priorities and ask the cabinet to decide which items to fund and which items *not* to fund. "That gets buy-in right up front," the CISO said.

Another approach is to have private auditors do risk assessments, and then the CISO comes up with a total cost of ownership of the preferred risk reduction measures. When the CISO does a presentation that combines the upward trajectory of the risk, and the total cost of ownership, it provides valuable context for the budget requests.

Closing Thoughts

Just before the end of the workshop, the CISOs each mentioned some of their personal takeaways from the day. Broadly speaking, the idea of the CISO as a change agent in the organization resonated with them, as did the idea of corporate culture being very important to how security is managed and shared. More specifically, CISOs expressed interest in:

- Leveraging data analytics more formally
- Looking more closely at software such as Triage, RedLock, Fire Eye, Netscope, Proofpoint, Bitsight, TrapEx, Illusive, and Evident.IO
- Blue team/red team pen testing in a sandbox
- Having risk owners update the security steering committee regularly
- Pursuing discussions around better medical device security
- Addressing the threat of data manipulation eclipsing the threat of data theft or destruction
- Making clear the idea that every risk the C-suite decides to not fund is a decision to accept that risk

The workshop was funded by a National Science Foundation grant as part of a project called Trustworthy Health and Wellness (THaW), CNS-1329686.

Participant List

Digital Transformation: A Secure Connected Healthcare System

Hans Brechbühl *(co-moderator)*	Executive Director, Center for Digital Strategies Adjunct Professor of Business Administration Tuck School of Business, Dartmouth College
Scott Breece	VP & CISO Community Health Systems
Paul Connelly	VP & CISO Hospital Corporation of America (HCA)
Ollie Green	CISO Vanderbilt University Medical Center
Andy Heins	Senior Director, Information Security Officer LifePoint Health
Nathan Holman	VP, Information Technology RxBenefits, Inc.
M. Eric Johnson *(co-moderator)*	Dean Owen Graduate School of Management Vanderbilt University
Joey Johnson	CISO Premise Health
Darrell Keeling	VP, Information Technology & Security Parkview Health
Charles Lebo	VP & CSO Kindred Healthcare
Talvis Love	SVP, eCommerce, Enterprise Architecture and CISO Cardinal Health
Rachel Rose	Principal Attorney at Law
Sherry Ryan	VP, CISO Juniper Networks

Brad Sanford	CISO Emory University
Guy Sereff	VP, Enterprise Architecture Change Healthcare
Olivier Witteveen	CISO & Corporate Compliance Officer Avadyne Health
Jenna Romeo T’19 *(observer)*	MBA Associate, Center for Digital Strategies Tuck School of Business, Dartmouth College
Molly Tyler T’19 *(observer)*	MBA Associate, Center for Digital Strategies Tuck School of Business, Dartmouth College