CHIEF INFORMATION OFFICER/CHIEF INFORMATION SECURITY OFFICER SUMMIT

October 28, 2016

Cybersecurity as a 'Team Sport': Governance, Organization, Strategy and Tactics

Prepared for the Scottsdale Institute

By Rob Faix, Impact Advisors

Executive Summary: Thirteen Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) of leading health systems gathered in Chicago to share best practices and lessons learned regarding information-security programs. These healthcare executives also explored lessons from other industries on innovative cybersecurity strategies. This report captures their discussion and shared insights.

Impact advisors

SCOTTSDALE INSTITUTE

COLLABORATION • EDUCATION • NETWORKING

SUMMIT PARTICIPANTS

- Mary Alice Annecharico, SVP & CIO – Henry Ford Health System
- David Bensema, MD, CIO – Baptist Health
- Fernando Blanco, VP & CISO – CHRISTUS Health
- Erik Decker, CISO – University of Chicago Medicine
- Michael Erickson, CISO – Baptist Health
- Jim Hanson, Regional Information Officer – Avera
- Meredith Harper, Chief Information Privacy & Security Officer – Henry Ford Health System
- David Jahne, IT Security Senior Director – Banner Health
- Lenny Levy, VP & CISO – Spectrum Health
- Jonathan Manis, SVP & CIO – Sutter Health
- Patrick O'Hare, SVP, Facilities & CIO – Spectrum Health
- Jim Veline, SVP & CIO – Avera
- Larry Yob, National Security Senior Director – Ascension Health

ORGANIZER: SCOTTSDALE INSTITUTE

- Janet Guptill
- Gordon Rohweder
- Shelli Williamson

SPONSOR: IMPACT ADVISORS

- Todd Hollowell
- Andy Smith
- Pete Smith

GUEST SPEAKERS

- Scot Pflug, Chief Information Security Officer – First National Bank of PA
- Ralston Simmons, Information Security Officer – William Blair

MODERATORS: IMPACT ADVISORS

- Rob Faix
- Tim Zoph

Left to right: Robert Faix, Scot Pflug, Ralston Simmons, and Tim Zoph

Introduction

2016 may be considered the Year of Information Security in light of numerous high-profile security events impacting healthcare and non-healthcare organizations alike. In October, leadership representing Information Technology and Information Security functions from Scottsdale Institute member health systems came together to share their perspectives, experiences and strategies for advancing the effectiveness of Information Security Programs. Joining these healthcare leaders were two guest speakers from the financial industry to provide an "outsider's" perspective on the types of challenges and strategies they have encountered for addressing security threats, training and overall management of their security programs.

Moderator Tim Zoph opened the session with his observations on the threats faced by the healthcare industry and the accelerated pace with which new threat vectors are exploited. He balanced these comments with observations that many of the basic activities, such as properly maintaining systems, remain a challenge to the industry. The list below represents a summation of some of the key responses from participants when asked what keeps them up at night:

- Developing effective engagement strategies with Executives and Boards of Directors.
- Rate of emerging threats impacting the healthcare industry and our ability to keep up.
- Maintaining a good balance between process engineering and workflow impact to people when addressing risks.
- Biomed equipment management, updating and segregation.
- Total number of end points that continue to grow throughout the organization.
- Ability to attract and retain talented people and training staff to achieve the organizational goals.
- "Hactivitists"—People motivated by political reasons to cause an intrusion.
- Achieving a reasonable information-security budget.
- Increasingly sophisticated attacks and new markets created as a result of hackers' ability to monetize data thefts.
- Volume of new applications being proposed and an organization's ability to vet applications properly.

Healthcare and the Financial Industry: A Comparative Review of Information Security

Participants were eager to gain insights from information-security practices in the financial industry for application into healthcare and to confirm or dispel myths that healthcare lags other industries for the maturity of such programs. Scot Pflug, Chief Information Security Officer at First National Bank of PA, grouped banking institutions into three broad classifications with each having a different maturity level for their security programs. "Larger banks with assets exceeding $50B," he said, "generally have very mature security programs and are likely much further along than the healthcare industry and even mid-size banks with assets between $15 billion and $50 billion. These are your Chase and Bank of America type organizations that generally have very robust information-security programs and the resources to properly fund these functions."

Lenny Levy, VP & CISO, Spectrum Health

Pflug continued by noting that mid-size banks may or may not have extremely mature information-security programs and, in his 20-plus years in information security as a consultant for a large global consulting firm and as an executive leader, he has seen both ends of the spectrum. Ralston Simmons, Information Security Officer at William Blair, a wealth-management firm, noted he is consistently surprised to see that basic IT-management processes such as the need for a well-developed software-patch-management process can sometimes come as a cultural shock to organizations in the financial industry. He reflected on the rigidity of the traditional mainframe environments of yesterday, which demanded strict coding that inherently added a level of security simply because the code was so well written; Simmons lamented that in today's world of coding, it seems like anything goes—and the security reflects that laxity.

Larry Yob, National Security Senior Director, Ascension Health

Participants of the CIO/CISO Summit were extremely engaged throughout this portion of the event with a continual stream of questions on strategies and tactics they have used to gather threat intelligence, develop effective programs and educate user populations. Pflug acknowledged one of the greatest challenges the financial industry faces today is the volume of merger and acquisition (M&A) activity that is occurring, much as we're seeing in healthcare today. "Organizations are challenged to properly clean up existing security issues in a timely manner before the next M&A opportunity is being explored," he said.

GATHERING THREAT INTELLIGENCE AND COMMUNICATING RISK

No shortage of threat-intelligence sources exist in the market today. Meredith Harper, Chief Information Privacy & Security Officer at Henry Ford Health System, said her organization is a member of the National Health Information Sharing and Analysis Center (NH-ISAC). Most agreed there is value in subscribing to third-party sources and some noted use of NTT Security SERT, InfraGard and similar organizations for gathering threat intelligence. Simmons cautioned those organizations who pay for more than one intelligence service should carefully review and compare the content across vendors to ensure they are not receiving potentially duplicative information. He noted that he participates in monthly meetings in Chicago with about 80 CISOs who share information and respond to specific questions in various email chains. Most attendees confirmed they actively participate in information-security groups in their respective regions.

SPECTRUM HEALTH

Patrick O'Hare, SVP, Facilities & CIO, Spectrum Health

"It's not an issue of 'if' you'll be breached, but 'when' and will you know that you have in fact been breached."

As the topic of information security continues to increase in importance, it is incumbent upon information-security professionals to manage executive expectations and adroitly engage senior leadership. Today, executive engagement ranges widely from "check-the-box discussions" to highly-engaged leaders who crave deeper understanding of security events or the state of the overall information-security programs. Not surprisingly, the visibility of information-security programs increased significantly in the wake of suspected breaches. Patrick O'Hare, SVP, Facilities & Chief Information Officer at Spectrum Health, said, "It's not an issue of 'if' you'll be breached, but 'when' and will you know that you have in fact been breached." Key to success with executive leadership and boards of directors is to maintain the conversation as a business conversation, not a technical one. Successful CISOs need to have the ability to translate IT risk into business risk.

Jonathan Manis, Sutter Health SVP & CIO, added to this thought: "My responsibilities are to identify risks and escalating threats, document-mitigation strategies, develop recommendations and then assist our operational and clinical leaders to make the best possible decisions regarding how we address, resolve and mitigate those risks." Complicating the situation is the reality that generational challenges may exist and hamper clear

Sutter Health

"My responsibilities are to identify risks and escalating threats, document mitigation strategies, develop recommendations and then assist our operational and clinical leaders to make the best possible decisions regarding how we address, resolve and mitigate those risks."

Jonathan Manis, SVP & CIO, Sutter Health

communication of risk to various leaders in an organization. To mitigate this issue, some organizations have elected to add a more technically savvy member to the Board of Directors who can serve as a liaison between IT and executive leadership. Mary Alice Annecharico, SVP & CIO at Henry Ford Health System, noted that the Henry Ford senior leadership and system board have become much more engaged in the information security conversation as well.

PERCEPTION AND REALITY OF INFORMATION SECURITY PROGRAMS

Opinions in the room covered the full spectrum of expectations when discussing the reality that a breach may occur. Some said their leadership clearly understands they will experience a breach event some day and have resolved that cybersecurity insurance is not only necessary, but will likely be called upon to offset the financial impact of such an event. Others noted their senior leadership expects no breaches whatsoever, a position everyone agreed was untenable in today's world. The group agreed that the complexity of cybersecurity threats are evolving rapidly and we, as information-security professionals, must continually advance the maturity of our programs and tactics to address the true nature of each threat. Manis noted that in today's environment, regulators tend to punish the victims of cybercrimes and we need to refocus attention on the prosecution and punishment of the criminals who perpetrate these crimes, not the organizations victimized by them. The room fervently agreed, universally noting that they are fatigued from playing defense from an auditing and compliance perspective and strongly recommend a more proactive position to prevention and early detection of cyber threats to reduce the likelihood and impact of costly data breach events. One of the participants weighed in by saying, "In the end, when we truly measure risk, regardless of a risk rating assigned to a given component of our infrastructure, the feeling is that risk is 'OK' until it isn't. Organizations are often willing to accept a risk until the actual breach occurs and, by then, it's too late."

BAPTIST HEALTH

Michael Erickson, CISO, Baptist Health

Avera

"Look at the percentage of an IT budget that is directed to information security, it's a pretty small number."

Jim Veline, SVP & CIO, Avera

FUNDING OF INFORMATION SECURITY PROGRAMS

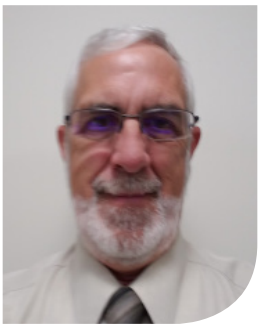
Jim Veline, Avera SVP & CIO, opened a discussion around the percentage of funding directed toward information-security programs, which he asserts is extremely small considering the value to the organization. "Look at the percentage of an IT budget that is directed to information security, it's a pretty small number," he said. "Then consider that the percentage of an IT budget to that of the enterprise is also a relatively small number.

Net this out and you'll see that information-security spend compared to the enterprise is likely a fraction of a single percent when compared to the enterprise. It just doesn't seem right given the task at hand." Annecharico added that there are so many inefficiencies in our industry, as CIOs we need to identify and prioritize those areas that are opportunities to reduce spending, how to work together across the industry on common solutions, and then consider redirecting available funds to support our ongoing information-security programs.

TACTICS FOR EDUCATING THE USER COMMUNITY

David Jahne, IT Security Senior Director at Banner Health, shared his concerns in getting the security message to users: "How do we shore up and get the attention of people who need to hear this message? How do we create an information security culture in the DNA of an organization?" Scot Pflug described the information-security awareness program that he has used, which leverages a variety of communication strategies, training and white papers to get the security message out to his user community. Among other strategies, he publishes a quarterly security newsletter to educate users, with each issue containing five bullet points on how to avoid being a victim of phishing attacks. "My goal with these five bullet points is to continue to put them in the newsletter until people start to ask, 'Why does he keep putting this in there?' That's when I'll know the message has truly been received." Pflug added that his goal is to have an organization filled with what he calls "Human Sensors," the frontline employees who are aware and remain vigilant to potential security threats.

Banner Health.



"How do we shore up and get the attention of people who need to hear this message? How do we create an information security culture in the DNA of an organization?"

David Jahne, IT Security Senior Director, Banner Health

CHRISTUS Health

Fernando Blanco, VP & CISO, CHRISTUS Health

Simmons said one of his main goals is to attend at least one meeting each year for each of the primary business units of his organization to discuss in-person the importance of good security practices and to educate team members on organizational expectations. In response to a question by Fernando Blanco, VP & CISO at CHRISTUS Health, regarding strategies to avoid the "numbing effect" of a recurring information-security awareness message, Simmons said, "We need to talk about an experience, not about numbers. Avoid making the conversation about comparative statistics of progress in the current period compared to the last period. We need to tell effective business stories related to risk if we are going to connect with non-IT leaders."

RANSOMWARE, BIOMEDICAL DEVICES AND OTHER INFORMATION SECURITY THREATS

In 2015 and 2016, the emerging threat of ransomware garnered a tremendous amount of visibility in the healthcare industry with several high-profile attacks impacting organizations that grabbed the attention of many in the C-suite. Most agreed ransomware has elevated the visibility and value of information-security programs within their organizations more so than any other non-breach event in the past. One of the CISOs expressed his dislike for the term "ransomware", as it's only a symptom of a larger problem. "The bigger issue is that we are a digital industry today and many of our systems, notably biomedical devices, were not designed with security in mind. Biomedical devices as a threat vector rank among the greatest targets in the healthcare industry." Jim Hanson, Avera Regional Information Officer, echoed this concern, noting that one of the things that keeps him up at night is "biomed equipment and the number of end points that continue to grow throughout my organization." The participants seemed split when discussing whom biomed currently reports to within their respective organizations, with some having this as an IT function and others as a more traditional facilities function. Harper said, "Bringing biomed into IT was a great idea because it empowered us to manage the devices."

Jim Hanson, Avera Regional Information Officer, noted that one of the things that keeps him up at night is "biomed equipment and the number of end points that continue to grow throughout my organization."

Jim Hanson, Regional Information Officer, Avera

"Bringing biomed into IT was a great idea because it empowered us to manage the devices."

Meredith Harper, Chief Information Privacy & Security Officer, Henry Ford Health System

A lively discussion erupted about the shared concerns with engaging third-party vendors, sharing of data with these vendors and how these concerns are further compounded when using a "cloud-based" solution. Participants voiced their frustration with the level of pushback they frequently receive from third-party vendors when it becomes necessary to conduct a risk assessment of the third-party solution. One of the participants commented, "No other healthcare organization has asked us to complete a risk assessment and we're in 'n' number of organizations throughout the country," is a response often stated by third-party vendors. This statement elicited a slight chuckle from the room as nearly everyone had heard a similar line from one or more of their third-party vendors. Seeking a solution, the group discussed a desire to create a healthcare information-security alliance that would offer a universally accepted risk assessment to be issued to vendors once and accepted by alliance members. This approach would also benefit vendors themselves as they would only need to complete the risk assessment once, thereby saving time and accelerating the overall conversation with various organizations. Veline noted, "There is value in the way we communicate with each other

regarding third-party relationships. If we could all just talk with each other and identify those specific vendors that are problematic, we could all benefit."

When the discussion turned to other areas of concern, the group centered on the Internet of Things (IoT), an especially timely topic as the Distributed Denial of Service (DDoS) attack which impacted significant portions of the Internet and high-profile services had occurred in the prior week. The attack's success has been largely attributed to exploitation of various devices constituting the Internet of Things. Manis suggested, "Of all the important things we've discussed today, the "Internet of Things" concerns me the most. In our increasingly mobile, digital society, virtually everything is addressable and can be connected—wearable health monitors; exercise equipment; kitchen appliances; weight scales; coffee makers; self-service, home diagnostic tests; even over-the-counter pregnancy tests. Healthy individuals and those individuals with chronic, but well-managed medical conditions will want data from these devices in their personal health and wellness records so they can maintain and manage their own health. My concern is that each of these devices may represent a new attack vector for those with criminal intent." Adding to the sheer amount of data which may be generated from various medical devices, Annecharico noted, "As we look toward clinically relevant conversations with CMIOs, it's very difficult to look at what is the sweet spot for valuable data to help make better clinical decisions and what is simply useless data." Key to the successful management of this clinical data is to establish meaningful conversations with IT about sources and methods for collecting, reviewing, accepting and integrating patient-generated health data and to ensure its accuracy. David Bensema, MD, CIO, Baptist Health, suspects that, "Patients may tend to submit the good information and not the bad and we're getting filtered data. We need to be careful to not overwhelm clinicians. Sometimes being 'patient centric' means saying 'no' to patients offering to share their Fitbit steps as part of their legal medical record."

"As we look toward clinically relevant conversations with CMIOs, it's very difficult to look at what is the sweet spot for valuable data to help make better clinical decisions and what is simply useless data."

Mary Alice Annecharico, SVP & CIO, Henry Ford Health System

"Patients may tend to submit the good information and not the bad and we're getting filtered data. We need to be careful to not overwhelm clinicians."

David Bensema, MD, CIO, Baptist Health

Conclusion

Participants of the CISO Summit expressed their sincere appreciation to both Ralston Simmons and Scot Pflug as guests representing the financial industry for their candor and willingness to share a realistic view of the state of information security for their industry and agreed that continued dialogue with one another was crucial to keep current on cybersecurity issues, trends and resources. Specifically, participants acknowledged the value in efforts such as these:

- Share information with one another on an ongoing basis regarding vendor risk-assessment results, product-specific security-controls issues and negotiated rates for National Health Information Sharing and Analysis Center (NH – ISAC) support.
- Join local and statewide cross-industry collaboration networks, as specific security threats may be common across industries.
- Identify organizational culture education techniques that have been successful in reducing internal security threats, including phishing campaigns, incident-response planning and "tabletop" exercises, and department-specific security-risk awareness programs. Avoid mind-numbing statistics; instead become story tellers to help employees understand the significance of risk and their role in preventing breaches.
- Engage the board and C-suite by maintaining cybersecurity as a business conversation, not a technical one. Translate IT risk into business risk and manage expectations adroitly. Lobby for adding a board member who's security savvy and can act as a liaison between the board and IT.
- Lobby for increased cybersecurity funding to better reflect the potential cost of cybersecurity breaches to healthcare organizations. In an increasingly cost-constrained environment, breaches result in less funding for care delivery needs.
- Bring biomed under IT for better security control.
- Aggressively manage vendors—especially cloud-based firms—by insisting upon risk assessments and not allowing them to dictate terms based on previous clients or industries. They'll eventually fall in line.
- Join forces to create a healthcare security alliance that can develop a universal risk assessment. This will be a win-win for health systems and vendors.
- Address the Internet of Things (IoT) by learning to separate clinically valuable information from useless data. FitBits need not apply as patient-generated data.
- Address potential risks associated with mergers, acquisitions and new program launches with specific policies regarding business-associate documentation, contract reviews and physical security considerations.
- Shift the conversation internally to focus on the criminals and not the victims of attacks.

Resources

The New Baldrige Cybersecurity Excellence Framework and Leveraging NIST
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-11-16.Baldridge-Cybersecurity-and-NIST.545trv.pdf
Nov. 17, 2016

Game Changers: Why you can't afford to be wrong about Risk Management
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-11-03.Risk-Management.847pn8b.pdf
Nov. 3, 2016

Building a Cyber Security Team at Partners
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-09-29.Building-a-Security-Team.3jh23q.pdf
Sept. 29, 2016

Taking a Business Approach to Cybersecurity at Henry Ford Health System
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-08-11.Business-Approach-to-Cybersecurity.95136pswxv.pdf
Aug. 11, 2016

Intermountain Healthcare sets up a Cybersecurity War Room
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-07-14.Cypersecurity-Ops-Ctr.39j2sg.pdf
July 14, 2016

Cyber Risk and Network Medical Devices
https://www.scottsdaleinstitute.org/docs/teleconfs/2016/2016-02-02.CyberRiskAndNetworkedMedicalDevices.298djk2.pdf
Feb. 2, 2016

Chief Information Security Officer: Outlook 2016
https://www.scottsdaleinstitute.org/docs/pubs/ie/IE.2016-01.CISO-Outlook-2016.e392nc2.pdf
January 2016

About the sponsors

The ***Scottsdale Institute (SI)*** is a not-for-profit membership organization of prominent healthcare systems whose goal is to support our members as they move forward to achieve clinical integration and transformation through information technology.

SI facilitates knowledge sharing by providing intimate and informal forums that embrace SI's "Three Pillars:"

- Collaboration
- Education
- Networking

For more information visit:
www.scottsdaleinstitute.org

SCOTTSDALE INSTITUTE
COLLABORATION • EDUCATION • NETWORKING

Impact Advisors provides Best in KLAS strategy and implementation services to drive clinical and operational performance excellence in healthcare through the use of information technology.

Impact Advisors is a recognized leader in the healthcare IT industry. We stay attuned to the latest technologies and trends impacting our clients through our involvement with advocacy organizations, including the Scottsdale Institute, HIMSS and CHIME.

Our Mission: Create a positive Impact!

For more information visit:
www.impact-advisors.com

Impact advisors