Cyber Insurance Roundtable Readout Report

Health Care and Cyber Risk Management: Cost/Benefit Approaches

National Protection and Programs Directorate
Department of Homeland Security

February 2014

TABLE OF CONTENTS

BACKGROUND

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) helps both private and public sector partners secure their cyber networks, assisting them collectively and individually and improving the nation's overall cybersecurity posture in the process. Through these interactions, DHS has become aware of a growing interest in cybersecurity insurance as well as limitations in the current market – especially when it comes to first-party market coverage for cyber-related critical infrastructure loss.[1] To better understand those limitations and how a more robust market could help encourage better cyber risk management, NPPD hosted its first-ever Cybersecurity Insurance Workshop during the fall of 2012. NPPD had two main goals for the event: (1) determine what obstacles prevent carriers from offering more attractive first-party policies to more customers at lower cost; and (2) promote stakeholder discussion about how to move the market forward.

At that event, NPPD hosted a diverse group of participants, registered on a first-come, first-served basis, from five stakeholder groups that included insurance carriers, risk managers, information technology/cyber experts, academics/social scientists, and critical infrastructure owners and operators. Several federal agencies also sent representatives. As part of its planning, NPPD asked participants to nominate breakout group topics in order to develop the workshop agenda and ensure that it addressed matters of critical interest. Participants nominated the following topics, which focused specifically on the first-party market: (1) Defining Insurable and Uninsurable Cyber Risks; (2) Cyber Insurance and the Human Element; (3) Cyber Liability: Who is Responsible for What Harm; (4) Current Cyber Risk Management Strategies and Approaches; (5) Cyber Insurance: What Harms Should It Cover and What Should It Cost; (6) Improving the Cyber Insurance Market: Stakeholder Roles and Responsibilities; and (7) Sequencing Solutions: How Should the Market Move Forward?

On May 13, 2013, NPPD held a roundtable based on what it had learned during the fall workshop. The roundtable focused on how organizations should go about building more effective cyber risk cultures as a prerequisite to a stronger and more responsive first-party market. With representatives from each of the same stakeholder groups in attendance, NPPD led a discussion about four "pillars" of such cultures: (1) Engaged Executive Leadership; (2) Targeted Cyber Risk Management and Awareness; (3) Cost-Effective Technology Investments Tailored to Organizational Needs; and (4) Relevant Information Sharing. Participants described the importance of and challenges with implementing the pillars in three distinct but related contexts: within companies; between partnering companies; and nationally. They likewise offered their opinions about how large, mid-size, and small companies should go about meeting those challenges given their traditionally disparate levels of expertise and risk management resources.

[1] First-party cybersecurity insurance policies cover direct losses to companies arising from events such as business interruption, destruction of data and property, and reputational harm. Third party policies, by contrast, cover losses that a company causes to its customers and others, such as harms arising from the exposure of personally identifiable information (PII) through a data breach. *See* U.S. Department of Homeland Security. *Cybersecurity Insurance Workshop Readout Report*. ONLINE. 2012. National Protection and Programs Directorate. Available: http://www.dhs.gov/publication/cybersecurity-insurance [29 January 2014].

During both events, participants shared a wide range of perspectives on these various topics, which were included in workshop and roundtable readout reports. The reports are available on the DHS Cybersecurity Insurance webpage at http://www.dhs.gov/publication/cybersecurity-insurance.

Building on the ideas surfaced at the workshop and roundtable, and after conducting its own additional research, NPPD publicly announced its intent to convene a second roundtable in the fall of 2013. That event, the subject of this readout report, addressed a fundamental yet unanswered question that had arisen over the course of the prior discussions: how do cost and benefit considerations inform the identification of not only an organization's top cyber risks but also appropriate risk management investments to address them? On November 20, 2013, NPPD accordingly hosted a small number of participants, registered on a first-come, first-served basis, at the National Intellectual Property Rights (IPR) Coordination Center in Arlington, Virginia, to find answers.

NPPD adopted a new format for the roundtable that included three cyber risk management use case presentations by health care organization (HCO) representatives. The representatives described an actual cyber incident that their organizations had experienced; how they managed the incident; and how lessons learned from the incident have influenced their actions and investments to improve patient safety. The presentations likewise addressed how the organizations are incorporating cost/benefit considerations as part of cyber risk management strategies; how their individual risk cultures are evolving as a result; and what role cybersecurity insurance is playing as part of their processes. An extended group discussion period followed each use case presentation in order to examine all of these themes in detail and to identify potential opportunities to enhance cyber risk management best practices.

Prior to the roundtable, NPPD advised the presenters and participants alike that their input during the event would be included in this final readout report on a non-attribution basis. NPPD explained that the purpose of this report would be to: (1) capture diverse ideas about how cost/benefit considerations motivate cyber risk management investments, including insurance investments; and (2) record a wide range of perspectives that might inform cyber risk management efforts nationally. NPPD further advised that it wasn't looking for, wouldn't accept, and wouldn't solicit group or consensus recommendations during the roundtable. NPPD likewise clarified that neither DHS nor NPPD would make any decisions about agency policy or positions during the event. In addition to 8 roundtable leaders, organizers, and support personnel, NPPD hosted 30 participants from the following stakeholder groups:

- Insurance Carriers: 7
- Risk Managers: 6
- Information Technology/Cyber Experts: 6
- Academics/Social Scientists: 3
- Critical Infrastructure Owners/Operators: 5
- Government: 3

EXECUTIVE SUMMARY

The HCO representatives, all of them Chief Information Security Officers (CISOs) or risk manager equivalents, hailed from a variety of organizations including an academic medical center and research university, a university hospital system, and a medical vendor that provides health care consumer products, pharmaceuticals, and medical devices/technology. Although each presented very different cyber risk management use cases, they shared many of the same challenges while addressing them. They consequently directed their remarks to three principal topics during the roundtable discussions: (1) making the case for cybersecurity investments to senior leadership; (2) incorporating cost/benefit considerations into their arguments; and (3) negotiating the boundary between risk mitigation efforts and risk transfer/insurance options to promote more effective cyber risk management strategies.

ENGAGING LEADERSHIP

The HCO representatives described two approaches to driving cybersecurity investments within their respective organizations. Several emphasized the value of enterprise risk management (ERM) to their efforts, noting that involving senior leadership in both the identification and prioritization of cyber risks has been critical to building trust in and promoting the effectiveness of their teams. They explained how they create master lists of priority cyber risks and corresponding risk controls for leadership review, drawing heavily on their team members' subject matter expertise as informed by real world cyber incidents. After presenting and discussing his team's list, one representative reported that his board of directors literally "draws a line" between those controls that will be funded given available resources and those controls that will not. This practice, he noted, generates a sense of ownership by the board that invests it in the success of its chosen approaches. By contrast, another representative explained that more primal factors motivate his leadership to spend against cyber risk: namely, fear of substantial regulatory fines and "public shaming" under the Health Insurance Portability and Accountability Act (HIPAA).[2] The representative advised that even though HIPAA does not focus on malicious hacking or other activity that doesn't directly impact the delivery of patient care, he nevertheless tries to market all his recommended risk controls on HIPAA grounds. Given its role as "primary driver of IT security funding," he observed, HIPAA currently serves as a necessary – albeit imperfect – vehicle for obtaining the cybersecurity funds he needs. Despite these disparate approaches, the HCO representatives concurred that ERM strategies that include cyber risk become easier to develop, fund, and implement once senior leaders mature their understanding of the full range of online dangers their organizations face.

COSTS AND BENEFITS

The HCO representatives likewise advised that when it comes to cost/benefit considerations, they use an exclusively qualitative approach when prioritizing cyber risks on the one hand and making the case for cyber risk management resources on the other. They asserted that cyber risk management today – at least in the health care sector – is more of an art than a science. One representative explained that his senior leadership usually defers to him regarding "top cyber risks" so long as he

[2] The Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191; 110 Stat. 1936).

maintains a keen sense of what's happening on his organization's networks, what's likely to happen on them in the future, and where the greatest potential for financial and other loss exists. This trust in his expertise likewise carries over directly to his proposed solution sets. Spreadsheets with quantitative details about the merits of one risk control over another, he continued, consequently have little to do with convincing corporate leaders to act. Several representatives agreed and reported that their leadership instead encourages them to "ballpark" their cybersecurity investment recommendations "in relation to the pack." As one noted, the rule of thumb is to spend not so much more than their peers that shareholders get angry and not so much less that regulators come knocking.

The representatives agreed that getting their organizations to actually *fund* their cybersecurity investment recommendations is the hard part. One stated that the best way for him to "sell" a particular investment's benefit is to assign ownership for potential cyber incident losses to specific individuals. He explained that once department heads understand that they're institutionally on the hook for such losses, resource conversations about purchasing and pre-positioning various risk controls suddenly become much easier. Another advised that avoiding the costs of a HIPAA audit typically is the only "benefit" he needs to demonstrate regarding a proposed mitigation. In short, casting a cyber risk control's benefits in terms of avoiding direct financial pain appears to be a highly successful technique.

The Role of Insurance

The HCO representatives were somewhat ambivalent about the role of cybersecurity insurance within their organizations' cyber risk management strategies. Several reported that they meet annually with underwriters to provide updates about their organization's cyber incidents and believe that data breach coverage in particular is "good to have." While one appreciated that his employer's insurer paid for an incident response firm to help out during a major cyber incident, he stated that he saw cybersecurity insurance as a way to address "catastrophic" situations only. He emphasized that he would *not* welcome insurers dictating how he or his team should mitigate cyber risks in his day-to-day environment. While another representative concurred that cybersecurity insurance has value because it purports to cover costs arising from unavoidable data breaches, he was dubious about the level of reimbursement his organization could truly expect in the event of a breach. It's never made a claim to test its policy. The third representative advised, in turn, that his organization has not yet invested in cybersecurity insurance. In view of his limited cybersecurity resources, he added, it makes more sense to spend on risk mitigation rather than risk transfer options.

Under these circumstances, the roundtable participants agreed that both cybersecurity professionals and insurers would benefit from a sustained dialogue about what each community brings to the cyber risk management table. Several remarked that a good first topic of conversation would be how they could work together to advance the cybersecurity insurance market's ability to cover cyber-related critical infrastructure loss.

HEALTH CARE ORGANIZATION 1

ORGANIZATION OVERVIEW: The Chief Information Security Officer (CISO) for Health Care Organization 1 (HCO 1) described HCO 1 as a nationally top-ranked research university and academic medical center. HCO 1 comprises several hospitals and hosts influential and sometimes controversial faculty and alumni – the profiles of whom, he noted, sometimes make it a cyber target. He stated that HCO 1 is home to almost 15,000 students; 28,000 faculty and staff; and 500 central information technology (IT) staff. The CISO advised that HCO 1 employs eight full-time information security staff. Four of those professionals work on operational and tactical information security issues such as establishing firewalls and providing hardware and software tokens. The remaining four focus on more strategic issues. Two of those four, he added, work strictly on IT compliance matters. The CISO described his team's budget as "small." Apart from employee salaries, he receives less than a million dollars annually to fund cyber risk management initiatives.

USE CASE PRESENTATION AND DISCUSSION:

CYBER RISK LANDSCAPE

- The CISO described HCO 1 as having a "high" threat environment in which his team, on a monthly basis, quarantines and/or blocks approximately 450 new bad actors; 30 million communications attempts to and from bad actors; seven million malicious websites; and 60 million emails. By contrast, his team supports the secure delivery of approximately six million emails. The CISO added that threat actors that target HCO 1 typically include identity thieves, phishers and spammers, and nation states.

- The CISO next described the number of cyber incidents that he and his team must respond to on an annual basis. They include anywhere from 400 to 500 minor incidents, including unauthorized beaconing out of the HCO 1 network (indicating malware or spyware); 10 to 15 "significant" incidents such as identity theft schemes that directly engage his team; and one to five breach notifications. One to three of those breach notifications, he added, include reportable events under HIPAA. The CISO advised that his team routinely cooperates with local and federal law enforcement on such incidents.

HCO 1 RISK MANAGEMENT CULTURE

GOVERNANCE

- The CISO stated that he believes that HCO 1 has a "healthy risk culture" when it comes to managing its cyber risk environment. He explained that HCO 1 has six governance bodies that support his team's cybersecurity work. They include:

    - A Board of Trustees Audit Committee. The CISO reported that he meets with the Board of Trustees Audit Committee once a year to provide an overview of the HCO 1 cyber risk landscape;

- The HCO 1 President's Cabinet and the HCO 1 Healthcare CEO. The CISO stated that he meets with these individuals multiple times per year, as necessary;

- An Enterprise Risk Management Committee. The CISO advised that the Enterprise Risk Management Committee includes both an Executive Committee and Risk Management Process Owners; and

- A Breach Notification Team. The CISO explained that the Breach Notification Team includes the HCO 1 Chief Information Officer (CIO), the CISO (himself), the General Counsel, and the Chief Risk Officer – all of whom have responsibility for both the HCO 1 healthcare system and the university – as well as the University Privacy Officer, the Healthcare Privacy Officer, the HIPAA Steering Committee (which monitors HCO 1's HIPAA compliance), and an IT Steering Committee (which centralizes IT efforts across HCO 1).

- The CISO advised that these governance bodies are comfortable making hard cyber risk management decisions and accordingly will take inconvenient mitigation steps; notify parties affected by a cyber incident; and accept institutional risk, when appropriate. He explained that HCO 1 leadership is guided by a desire to make the "right" cyber risk management decisions for impacted individuals within the HCO 1 community and for HCO 1 as an institution, in that order.

    - The CISO reported that the governance bodies involved in HCO 1 cyber incident response include the Breach Notification Team, the Enterprise Risk Management Executive Committee, and business unit leaders from business units impacted by cyber incidents.

    - The CISO noted that the Enterprise Risk Management Committee worked collaboratively to reduce an original list of 1,600 priority risks to 60 risks – three of which involve data breach and/or exposure risks. He advised that his team meets with the Committee several times a year to provide updates on the state of HCO 1's cybersecurity risk. He explained that his primary responsibility, as the cyber risk management process owner, is to get the right information to the Committee in order to enable effective management of the most pressing cyber risks.

    - The CISO further explained that after a cyber incident, the Breach Notification Team gathers the relevant facts and generates a one-to-two page, high-level risk document with recommendations on how it thinks HCO 1 should respond to the incident. The Team then provides its recommendations to the Enterprise Risk Management Committee which, in turn, determines what actions to take.

Governance Questions

- An IT professional asked about the mechanics of the Breach Notification Team process. The CISO replied that it usually takes a short but significant amount of time to conduct a fact-finding effort in support of the one-to-two page Breach Notification Team report. He added that the process – from initial notification of a breach to final decision by the Enterprise Risk Management Committee – can address both cyber and physical threats. For example, HCO 1 maintains its own police department to which the Breach Notification Team can provide "trackable" leads such as phone calls. The CISO stated that the police department in turn can issue subpoenas, an authority which it has exercised on his team's behalf in the past. In return, he noted, his team can provide technical expertise for law enforcement tasks such as forensic analysis of infected workstations.

- A risk manager asked the CISO about his communications strategy following a cyber incident. He responded that his team puts together the first draft of any message in order to ensure that all the technical and other facts about an event are correct. The team then sends the draft to the HCO 1 press office for final preparation. The CISO added that he and his staff are very cognizant of all the downstream impacts that might result from an incident and that that knowledge informs everything they do. An IT professional then asked whether the CISO has a "holding" press statement "at the ready" whenever cyber incidents occur. The CISO responded in the negative.

- A critical infrastructure representative asked what participation the CISO has in "higher-level discussions for business decisions." The CISO responded that although neither he nor his team directly participate in discussions about large and strategic IT purchases, the Chief Information Officer (CIO) does so participate and is "very security minded." The CISO added that if HCO 1 considered such a purchase, the CIO would come to him and ask for advice and guidance.

Strategies for Success

- The CISO described a two-pronged strategy for his team's cyber risk management success that includes obtaining leadership approval for HCO 1's Strategic Plan for Information Security and involving leadership in the incident response process itself.

Strategic Plan

- Regarding the first prong, the CISO advised that his team works to align HCO 1's Strategic Plan for Information Security, which addresses where large information security initiatives should be focused for HCO 1 in the coming 18-36 months, with HCO 1's overall institutional vision and strategy. As part of that effort, his team generates a prioritized list of information security risks every 12-18 months. That list includes a corresponding series of information security initiatives designed to address those prioritized risks. Each such initiative includes a description of its estimated one-time and recurring costs; staffing requirements; and the specific risks – e.g.,

those arising out of Bring Your Own Device (BYOD) and other business trends – that they're designed to address.[3] The CISO advised that he seeks funding for the highest priority initiatives recommended by his team but has HCO 1 leadership literally "draw a line" between the information security initiatives that it will fund and those which it will not.

- The CISO reported that this decision process highlights to HCO 1 leadership that, in a resource-constrained environment, some threats will not be addressed. In this way, leadership is forced to explicitly prioritize between different types of threats and risks and accordingly "own" its final decisions in a much more complete manner. He stated that HCO 1 executives have accordingly become more and more invested over time in the success of the HCO 1 Strategic Plan for Information Security.

- A critical infrastructure representative asked if the CISO sometimes argues in the "opposite" direction, attempting to convince his leadership not to fund specific initiatives that may not offer a comparative value. He responded that his team does not make such arguments but that the CIO is much more likely to do so.

Leadership Involvement In Incident Response

- Regarding the second prong, the CISO reported that his team provides regular cybersecurity briefings to HCO 1's six governance bodies – a service that has gone a long way toward building a "great relationship" with key leaders and establishing his team's credibility. As a result, he has obtained leadership approval for not only a unified cyber incident/breach response process but also incident/breach response teams to actually implement that process. To fortify this progress, the CISO ensures that HCO 1 leadership has final decision making responsibility for all strategic cyber risk management decisions that impact the incident/breach response process.

- The CISO emphasized that his team's efforts have resulted in strong leadership support for a predetermined funding model that imposes the direct costs of cyber incidents on the HCO 1 business units responsible for them. The CISO mentioned that he wants those units to "share the pain" that their sometimes poor cybersecurity causes to the enterprise. Using an internal billing code, he accordingly charges them for breach notification, investigation, and mitigation expenses as they arise and accrue over time. The CISO noted that this cost ownership policy is meant to reduce reliance on institutional risk across HCO 1. He stated that this approach is very effective and that he rarely, if ever, feels that he's being asked to internalize too much risk.

[3] Bring Your Own Device (BYOD) refers to the practice of allowing an organization's employees to use their own computers, smartphones, or other devices for work purposes. Oxford Dictionaries. BYOD. ONLINE. N.D. Available: http://www.oxforddictionaries.com/us/definition/american_english/ [7 January 2014].

HCO 1 USE CASE

THE INCIDENT

- In the summer of 2013, HCO 1's network monitoring tools alerted security administrators that an unexpected system management tool had executed on several systems. The security team investigated the activity and determined that administrative accounts were accessing systems in a manner that suggested that they had been compromised by malicious hackers. HCO 1's initial investigative efforts revealed that at least a partial list of domain accounts and password hashes had been compromised by the malicious hackers and that they had obtained the credentials of at least two domain administrators.

- To assist with forensic analysis and other security efforts involved with the incident, HCO 1 engaged the assistance of one of the nation's leading incident response firms. Doing so took several days because HCO 1 first had to verify that its insurer would pay for the services – the costs for which exceeded insurance policy limits – before entering into negotiations with the firm. HCO 1 actively cooperated with federal law enforcement agents during this time. Through its combined investigative efforts, HCO 1 was able to determine that approximately 44 systems within the HCO 1 environment were either compromised or accessed by the malicious hackers. Other than the aforementioned list of user accounts and hashed passwords, the investigation did not find evidence that the malicious hackers had accessed additional personally identifiable information (PII).

- HCO 1 took immediate steps to investigate and contain the intrusion, including the disabling of privileged accounts to which the malicious hackers had access and replacing potentially compromised Active Directory servers. In conjunction with HCO 1's Enterprise Security team, the incident response firm performed investigative activities both onsite and remotely for just over five weeks.

- The incident response firm asked HCO 1 not to remove the malicious hackers immediately in order to provide it with sufficient time to figure out what they were up to on the HCO 1 network. The CISO and his team accordingly recommended to HCO 1's Enterprise Risk Management Committee that they initially make a very limited mitigation response so the firm could conduct its requested assessment. The Enterprise Risk Management Committee agreed. After determining the full scope of systems impacted by the incident, a second round of remediation activities were identified and planned. In addition to finally removing the malicious hackers from the environment, those planned activities were designed to improve HCO 1's defenses and enhance its monitoring capabilities over the long-term.

- HCO 1 initiated the second round of remediation activities two weeks after the incident response firm began its onsite activities. At that time, HCO 1 launched an enterprise-wide

password change;[4] removed any remaining compromised systems that had been identified through the ongoing investigation; blocked communication with known malicious hacker network addresses and domains; and implemented hardening countermeasures to make it more difficult for malicious hackers to regain access to HCO 1's internal network and to move about within it. Additionally, HCO 1 implemented enhanced monitoring and alerting capabilities to help detect future attacks.

- HCO 1 currently is working on several additional long-term efforts to improve its ability to prevent, detect, and respond to similar events in the future.

Lessons Learned and Rules of Thumb

- The CISO and his team identified seven "lessons learned and rules of thumb" following the use case incident that continue to inform their strategic cyber risk management planning across the HCO 1 enterprise:

    - Carpe Incident! Be prepared to take advantage of funding opportunities that may arise from a cyber incident.

      The CISO stated that very often during or immediately after a significant cyber incident, leadership will ask questions like, "Is there anything we can do to keep this kind of thing from happening again?" "Do you need any additional resources to help resolve this?" "Is there any assistance we can provide?" He advised that if cybersecurity professionals have security initiatives "waiting in the wings" solely because of funding or staffing limitations, they should seize this moment to ask for the additional resources they need. In short, having a small portfolio of pre-prepared, ready-to-go project proposals might just be the thing that will turn a bad situation into an opportunity for improvement.

    - During extended incident response efforts, having all the members of an incident response team share the same physical space while doing their work is extremely beneficial.

      The CISO explained that he co-located malware analysts and network engineers throughout the duration of the incident response cycle, an arrangement that led to many efficiencies and synergies in terms of communications, coordination, and situational awareness. These efficiencies and synergies were important, he observed, because approximately 500 individuals across HCO 1 and associated organizations, including the incident response firm, were involved in the response effort.

[4] The CISO stated that many individuals within the HCO 1 community were likely using their HCO 1 passwords for their personal accounts. HCO 1 didn't want anyone's personal accounts to be affected by the incident, so it chose to notify everyone of the need to change the passwords for those accounts.

The CISO added that he'd tell insurance companies that paying for an outside incident response firm to conduct an on-site, real-time assessment of a cyber incident is money well spent. He advised that the costs involved with the use case firm totaled $300,000. By comparison, he commented, traditional off-site forensic analysis "would have cost an order of magnitude more and would have been slower."

- Things are seldom as definitive as they may seem during the early stages of an incident, so CISOs should not overstate or understate the "facts."

  The CISO suggested that cybersecurity professionals should manage the expectations of their organization's leadership by phrasing their messaging carefully – saying, for example, "the incident is fluid, and this is what we believe at this time" – and then providing more detailed and precise updates as more (and better) information becomes available.

- A decision not to fund a security initiative is a de facto risk acceptance decision and needs to be made by someone with the authority to accept such risks.

  The CISO noted that most security incidents don't result from completely novel attack vectors. On the contrary, he continued, most of the potential avenues of compromise likely have been anticipated and potential solutions identified in advance. The CISO added that the real issue is that cybersecurity professionals typically can't do everything at once, so tradeoffs must be made based on priority. "When you're choosing which initiatives to implement you should be doing so because those solutions are believed to provide the highest value in terms of risk reduction versus cost/impact to your organization," he stated. "In contrast, the initiatives you choose not to pursue (for good reason) will mean that there are known/anticipated risks that will not be addressed (at all in some cases) because the initiative is not undertaken."

  The CISO added that choosing not to fund these initiatives means that, intentionally or not, an organization also chooses to accept certain cyber risks as the cost of doing business. He added that such a decision may be entirely rational, but that the people making it should have not only sufficient budgetary authority to do so but also sufficient management authority to accept the level of anticipated risk that will result. These are joint decisions, he emphasized, that should be decided together by the same people at an enterprise-wide level.

- A system compromise is not the same thing as a data breach.

  Knowing early that malicious hacker(s) have not accessed data, the CISO explained, can save incident responders a lot of time, effort, and expense.

- Proactively instrumenting an IT environment is critical to effectively managing a cyber incident.

  The CISO explained that he and his team had pre-positioned most of its instrumentation prior to the use case incident but only because they hadn't had it in place before other previous incidents. Even so, he continued, HCO 1 had not pre-positioned the solutions that the incident response firm ultimately provided – solutions that made a huge impact during and after the use case incident. As a result, HCO 1 is now deploying those solutions on a permanent basis to assist with future incidents.

- Vulnerabilities in "non-critical" systems can lead to the compromise of critical systems.

  The CISO advised that HCO 1 had multi-factor authentication in place for its critical systems prior to the use case incident. He noted that the vulnerability that the malicious hacker(s) exploited, however, existed on a non-critical system that did not require two-factor identification. Once the malicious hacker(s) gained access to that system, he added, they worked laterally across the entire HCO 1 network.

COST/BENEFIT CONSIDERATIONS

- The CISO explained that HCO 1's approach to identifying top cyber risks and appropriate controls to address them is qualitative and not quantitative. He explained that a qualitative approach focuses his team on the relative priority and ordinal ranking of cybersecurity initiatives – as outlined in the HCO 1 Strategic Plan for Information Security – that in turn inform which specific cyber risk management investments to make. To generate that ranking, the CISO added, his team relies heavily on its own cybersecurity knowledge and expertise. "Cybersecurity is an art," he observed, "not a science." When asked whether he felt pressure to justify his recommendations using return on investment (ROI) analyses, the CISO responded, "It would dilute our message to just put numbers on a spreadsheet. Our relationship with management is based on trust."

- The CISO explained that when it comes to cost/benefit considerations, information security "generally carries a big stick" across the HCO 1 environment. That big stick, he continued, derives in part from the organization's ongoing defense of a class action lawsuit involving the lost PII of several thousand people. The CISO noted that the lawsuit powerfully drives home to HCO 1 leadership every day the cost/benefit reality of information security investment.

- The CISO advised that he and his team do not prioritize their risk mitigation efforts in isolation but in direct reference to the leadership-approved HCO 1 Strategic Plan for Information Security. "Everything sounds like a good idea in a vacuum," he observed, and therefore must be considered in relation to the strategic plan. Doing so, he continued, helps ensure that the team does not overreact to the "threat of the week." The CISO added, "We do not want to try to do everything and fail in everything due to lack of resources."

- The CISO noted, however, that he and team sometimes "rank order" their strategic mitigation efforts alongside non-mitigation initiatives of potential benefit to the organization. For example, they might treat inexpensive "quick wins" as operational initiatives worthy of action and will fund them accordingly.

- Finally, the CISO advised that his team has been able to reduce costs by leveraging pre-negotiated contracts such as the one with the incident response firm retained during the use case incident last summer. When asked by an insurer whether HCO 1 sustained additional costs beyond retention costs for that firm, the CISO reported that the enterprise had also suffered a "loss in productivity."

USE CASE QUESTIONS

- A critical infrastructure representative asked if HCO 1 had taken forensic images of the described attacks; whether it had been able to determine the identity of the malicious hacker(s); and the extent to which law enforcement provided value. The CISO responded that most of HCO 1's systems were running on virtual machines, so his team easily created necessary forensic images, captured memory, and produced disk images. He added that HCO 1 had "flow data for days" on its network as well as network packet capture solutions that retain 28-30 hours of network traffic into and out of the organization at a time. "Every time we identified a suspect system," the CISO added, "we added it to our list [for network packet capture]." He advised, however, that neither the incident response firm nor law enforcement had been able to confirm the identity of the malicious hacker(s). While work continues in this area, he explained, the malicious hacker(s) did not appear to match other known actors. The CISO observed, moreover, that information sharing with federal law enforcement during the incident had proven to be a largely one-way affair, although his federal partners during their investigation had been able to identify four or five additional "bad guy" systems that had been communicating with HCO 1 servers.

- A risk manager asked whether the CISO believed that HCO 1 has a trusted network with other universities. The CISO responded affirmatively and advised that HCO 1 is involved with the Research and Education Networking Information Sharing Analysis Center (REN-ISAC). He added that during the use case incident, HCO 1 reached out to similarly-situated health care organizations through the REN-ISAC who were also experiencing attacks. The CISO asserted that the nation needs an "ISAC of ISACs" so organizations from multiple sectors can share cyber risk and cyber incident information in real time.

- An insurer asked what kinds of interactions HCO 1 had or is having with regulators in the wake of the use case incident. The CISO responded that the Department of Education asked specific, high-level questions of HCO 1 and that he and his team had provided background about the incident. He advised that although user IDs and passwords appeared to have been exposed during the event, there have been no indications that other PII was compromised.

- An IT professional asked how long it took to get the incident response firm on site. The CISO responded that a contract was signed within several days; gear was shipped and installed a few days after that; and that the firm – once it arrived – took 17 days to "figure out what was going on." The CISO and his team were very pleased with the firm's performance and, as previously noted, plan to maintain their business relationship.

- A second IT professional asked if HCO 1 was happy with its insurer's support during the incident. The CISO responded affirmatively, noting that HCO 1 had paid the required deductible and that the carrier covered all the costs beyond that amount. He added that the carrier had helped HCO 1 get better prices for services in some cases – typically from approved vendors – and that requiring the use of approved vendors was a reasonable demand from his perspective.

CYBERSECURITY INSURANCE

- The CISO advised that HCO 1 has maintained cybersecurity insurance since 2008 and that he considers it to be the cyber equivalent to a catastrophic health plan – in short, it provides limited coverage with a large deductible. In response to a question from a risk manager, he advised that he's fairly isolated from the financial side of insurance and that his only interaction with the insurer in that respect is to "answer their annual [information security] questionnaire." While the CISO stated that HCO 1's risk transfer needs are being met by its existing policies – especially when it came to getting the incident response firm on-site quickly – he identified several gaps that he'd like to see the broader cybersecurity insurance market fill:

    - Identity theft insurance for breach notification recipients, so individuals who experience fraud and related losses as a result of a breach can be made whole;

    - Elimination of exceptions for widespread incidents such as Internet worms and viruses; and

    - Coverage that applies to HCO 1 data regardless of where it "lives" – for example, beyond HCO 1's network to BYOD devices and Cloud/SaaS Services.

- The CISO added that he would not welcome additional cybersecurity "regulations" being imposed by HCO 1's insurer through the insurance contract.

HEALTH CARE ORGANIZATION 2

ORGANIZATION OVERVIEW: The Chief Information Security Officer (CISO) for Health Care Organization 2 (HCO 2) described HCO 2 as an enterprise that includes six major hospitals, over 100 clinics, and a university system that includes a medical community of almost 60,000 members. It serves millions of patients. Given HCO 2's size, he explained, he doesn't have to look hard for examples of cyber incidents that occur within it. The CISO stated that HCO 2's network security team employs approximately 30 full time equivalent (FTE) employees. He advised that approximately 15 of those FTEs are application security specialists, meaning that they set up rules dictating user access to systems. He added that approximately seven other FTEs work directly on network security issues while another seven focus on acquisitions or "buying security."

The CISO commented that his team currently lacks risk management experts and "data cops." Finding and hiring specialists in these areas is difficult, he explained, because they have inherently tough and thankless jobs. The CISO advised that he's made the case to HCO 2 leadership that the same person should not be responsible for all network security needs. He commented that the cybersecurity field is very specialized and that the person handling laptop encryption, for example, should not also be working on network security. As the cyber threat continues to escalate, he added, the need for specialized cybersecurity professionals will increase accordingly.

USE CASE PRESENTATION AND DISCUSSION:

CYBER RISK LANDSCAPE

- The CISO described the HCO 2 cyber risk landscape, and the cyber risk landscape for health care organizations generally, through the prism of electronic health records (EHRs) and the increasing number of security issues involving them.

LONGSTANDING CHALLENGES

- The CISO observed that most doctors still use paper medical records despite the fact that health care providers have been talking about implementing EHRs since the 1960s. He noted that the transition to EHRs has been slow for two main reasons.
    - First, system designers often don't put the needs of end users – i.e., the doctors – first. Instead, they develop underlying infrastructure to support the creation, transfer, and storage of EHRs before they build out end user applications. The CISO commented that strict usability requirements of the medical profession create a high performance bar for the technology that must be satisfied before doctors will adopt it. For example, he explained, doctors examining patients can't wait minutes at a time for EHRs to load onto handheld devices. In addition to cutting into the doctor's efficiency – and, consequently, his or her profit margin – inadequate technology (i.e., the end user application) and/or the perception thereof erodes patient confidence.

- Second, EHR statutory and/or regulatory requirements themselves impose significant technical challenges that must be successfully addressed. The CISO described the two primary components of medical record exchange in most practices:

  - Documentation, the so-called "easy" part, such as when a doctor prescribes a medicine for a patient; and

  - Order entry, the so-called "harder" part, when an order for medicine or a test is actually placed based on a doctor's diagnosis and recommendation.

  The CISO emphasized that the Health Information Technology for Economic and Clinical Health (HITECH) Act,[5] by requiring doctors to use electronic order entry by 2015,[6] has inserted "medical IT" into the center or medical practice itself. The importance of this new requirement, he commented, can't be overstated.

- The CISO added that getting electronic order entry wrong could cause a doctor's life to go from "bad" to "intolerably bad." Specifically, he stated that some technologies already slow down trust delegation data processes used by doctors today. In view of the fast approaching 2015 deadline, he added, some doctors fear that faulty or underperforming order entry technology could compromise their already "brittle" medical record exchange systems. The CISO observed that doctors further worry that the new mandate will require them to do more work, slow them down, and ultimately reduce their productivity by cutting the total number of patients they can see on a daily basis. Given the already low reimbursement rates of Medicare and other programs, he concluded, this could result in severe risk to a health care organization's already low profit margins.

---

[5] The HITECH Act, enacted in Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), set as a critical national goal the "meaningful use" of interoperable EHR. Wikipedia. Health Information Technology for Economic and Clinical Health Act. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act [23 January 2014]. The term "meaningful use" means that health care providers use certified EHR technology in ways that can be measured significantly in quality and quantity. U.S. Department of Health and Human Services. ONLINE. N.D. Available: http://www.hrsa.gov/healthit/meaningfuluse/ [24 January 2014]. Under the HITECH Act, health care providers that achieved meaningful use by 2011 became eligible for incentive payments. Meaningful Use. ONLINE. N.D. Available: http://www.healthcareitnews.com/directory/meaningful-use [8 January 2014]. Those who fail to do so by 2015 may be penalized. *Id.* Stage 1 meaningful use criteria set the baseline for electronic data capture and information sharing, while Stage 2 and Stage 3 – expected to be implemented in 2015 – will continue to expand on that baseline. *Id*.

[6] Electronic order entry, also known as Computerized Physician Order Entry (CPOE), refers to a process of electronic entry of medical practitioner instructions for the treatment of patients (particularly hospitalized patients) under a physician's care. Wikipedia. Computerized Physician Order Entry. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/Computerized_physician_order_entry [8 January 2014]. These orders are communicated over a computer network to the medical staff or to the departments (pharmacy, laboratory, or radiology) responsible for fulfilling the order. *Id*. CPOE is intended to decrease delay in order completion, reduce errors related to handwriting or transcription, allow order entry at the point of care or off-site, provide error-checking for duplicate or incorrect doses or tests, and simplify inventory and posting of charges. *Id*.

- When another IT professional responded that some of the challenges with adopting electronic order entry may arise from the preferences of individual doctors rather than from underlying sector dynamics, i.e., "people" problems versus "process" problems, the CISO disagreed. He stated that medical IT applications have always slowed doctors down, but that they typically complete only the documentation portion of the medical record exchange process – leaving order entry to other staff such as nurses, pharmacists, and other licensed professionals. Regardless of the technical preference of doctors, he added, the requirement that they now play a bigger role in the order entry process itself imposes a significant burden. The CISO concluded that doctors typically aren't technophobes but literally can't afford to be slowed down by anything at the patient point of care.

- The CISO remarked that the EHR solutions industry is comparatively immature, likening it to the maturity of enterprise resource planning (ERP) solutions in the 1980s and 1990s.[7] While massive changes in the EHR solutions industry are underway, he continued, obtaining the right solutions still can be very hard. He noted that integrating and obtaining required levels of interoperability among systems, based on existing Health Level Seven International (HL7) and other standards, present even more complex challenges that will require patience and tolerance by all relevant stakeholders as the health care sector evolves in the years ahead.

- The CISO then cited the overwhelming need for health care organizations to communicate both internally among their various business units and externally with other organizations in order to serve their patients. In view of the complex coordination this requires, he observed, it's not surprising that their medical record exchange systems are "brittle." "Securing brittle systems is very difficult," he added, and imposing new layers of security on them only contributes to their "brittleness." The CISO concluded that for these reasons, health care organizations generally are not predisposed to supporting major cybersecurity investments.

REGULATORY REGIMES AND AUDITS

HIPAA

- Despite these challenges, the CISO explained that cyber incidents nevertheless are very much on the radar of most health care organizations given the main regulatory structure against which they must perform: HIPAA. Although he described HIPAA as a law that's "difficult to decipher," he stated that health care organizations pay very close attention to the results of HIPAA audits in order to understand how the Department of Health and Human Services (HHS) assesses and evaluates cybersecurity best practices. The CISO disclosed that HHS recently subjected HCO 2 to

[7] Enterprise resource planning (ERP) software refers to business process management software that allows an organization to use a system of integrated applications to manage its business and automate back office functions. Webopedia. ERP – Enterprise Resource Planning. ONLINE. N.D. Available: http://www.webopedia.com/TERM/E/ERP.html [14 January 2014]. ERP software integrates all facets of an organization's operation, including product planning, development, manufacturing processes, sales and marketing. *Id.*

a random HIPAA audit that provided it with a series of performance scores against a full range of HIPAA regulations.

- The CISO advised that pursuant to HIPAA, HHS publishes the results of investigations into security breach events that impact over 500 people. He added that there have been over 800 such incidents for which investigation results have been made publicly available – a list known in the trade as the "wall of shame." He stated that the most common source of reported HIPAA violations stems from the theft and/or loss of laptops and desktop computers, and that lost paper records run a close second. He noted that the number of health care organizations reporting hacking incidents also has ticked up, rising from very low percentages several years ago to the 10-12% range today. The CISO said that although only about 80 breaches in the last three to four years have involved over 500 people, many more are "almost certainly" occurring but go undetected. He concluded that these statistics nevertheless show that HIPAA is driving a more complete accounting of what were, until recently, undisclosed security lapses.

- The CISO added that even as health care organizations are seeing a rise in the number of reported laptop security breaches, they're also seeing a rise in the number of reported paper-based security breaches – e.g., hospitals failing to shred patient records and other documents properly, opening them to compromise by dumpster diving criminals. He asserted that this trend indicates that security breach reporting generally – driven by HIPAA and other authorities laws – is improving in terms of its pervasiveness and thoroughness.

HIPAA's Limits

- The CISO reported that his fundamental concern with HIPAA as a cybersecurity "regulation" is that it doesn't effectively address his biggest security problem: the malicious hacking of EHRs and the medical IT infrastructure that supports their creation, sharing, and storage. He observed that HIPAA instead focuses on securing the medical IT infrastructure that supports the business processes that enable doctors to see and treat their patients. While ensuring that those processes are "up and working" is important, he continued, that emphasis creates a perverse incentive to *not* focus on the cybersecurity of everything else. The CISO attributed this shortcoming to the sector's "mental model" of what constitutes a medical IT failure. "The community does not see IT as a vector for attack," he explained, "but rather as an enabler of organizational processes that themselves are often difficult to effectively perform." In short, health care organizations face stiff fines if they fail to comply with HIPAA's regulations concerning medical IT availability, so their leadership unsurprisingly directs the bulk of available security funding to that area.

- The CISO observed that cybersecurity professionals instinctively realize that conversion to an EHR system opens new opportunities for unauthorized access to, or corruption of, patient health records. This new vector of attack, he added, compounds the already significant challenges that exist with securing medical IT infrastructure – much of which health care organizations outsource to third parties in order to save money. "If a health care provider

doesn't even hire its own networking experts," he stated, "it's even less realistic to expect that it will hire its own security experts." The CISO added that HIPAA further complicates this situation. The law's emphasis on business process security, he added provides health care organizations with a further rationale to bypass the larger issue of ensuring network security altogether and focus instead on regulatory compliance. "In other words," he concluded, "those who can't and/or won't do security do compliance."

- The CISO advised that this HIPAA prism consequently makes his cyber risk management messaging to HCO 2 leadership very challenging. He explained that when HCO 2 leadership asks him how things are going with network security, he responds, "Everything is going great; the situation is dire." From a HIPAA perspective, he stated, the very few notification events (involving impacted business operations) that HCO 2 has experienced *is* great. By contrast, threats to the HCO 2 community's intellectual property (IP) and PII from malicious hackers, nation-states, and others pose very serious and growing problems.

- The CISO noted that efforts to gather data about malicious hacking incidents across the HCO 2 enterprise are relatively new and that discerning trends in this area is accordingly difficult. Consistent with HIPAA's business process-oriented regulations and related statistics, however, he confirmed that HCO 2's main "operational" security breaches stem from the theft and/or loss of laptops and desktops. Publication of sensitive data on the Internet, he added, represents an additional challenge area.

Regulatory Regimes and Audits Questions

- The CISO's discussion about HIPAA – and the theft and/or loss of laptops and desktops in particular – spurred a series of questions from other roundtable participants about academic freedom, how HCO 2 conducts its asset management activities, and what software solutions it uses for those activities.

Academic Freedom

- An insurer asked why laptops aren't encrypted as a matter of course if they represent the leading cause of security breaches. The CISO responded that the number of unencrypted HCO 2 laptops has decreased significantly in recent years but that the BYOD trend has driven up the number of personal laptops in use on HCO 2's network. He advised that the reason for this development is straightforward: medical researchers expect to be able to use their personal laptops and open-source software to conduct their work in collaboration with others. Taking away their permission to do so, he stated, would not only severely restrict their ability to conduct research but also run counter to the very concept of academic freedom. "The freedom to compute," he concluded, "is fundamental to conducting science." Unfortunately, he added, some researchers forget to enable the encryption installed on their personal laptops when exercising that freedom.

- The CISO advised, moreover, that significant problems arise when conducting network device interrogations to remotely verify whether the encryption software on personal laptops connected to the HCO 2 network is operating. He explained that those myriad personal laptops used by both medical researchers and doctors – often for very different purposes – include many different kinds of encryption software. This variation could well lead to incomplete or inconsistent interrogation results that, in turn, would require significant follow up with and inconvenience for end users.

- The CISO observed that while HCO 2 can attempt to reduce unnecessary data, monitor the data that leaves its major warehouses, and institute reasonable security practices for people to follow, it remains severely limited in its ability to address many cyber risks given its academic culture. For this reason, he advised, rules-based security efforts such as whitelisting are wholly unviable within the HCO 2 environment. He added that the biggest related issue on the horizon is with network permissions – specifically, balancing end user freedom to access whatever networks they deem necessary for research with the very real security threats that attach to some of those networks. The CISO stated that HCO 2 will likely continue to err on the side of academic freedom when faced with a tradeoff between openness and security.

- The CISO concluded that while the profile of malicious hacking incidents that target PII continues to rise, significant changes to the academic mindset about cybersecurity won't happen until end users experience first-hand the consequences of a cyber incident. He advised that those changes might come about as a result of browser exploits such as ransomware and keyboard loggers that negatively affect the ability of end users to perform online banking and other personal tasks on their organizations' networks. In his view, once end users become more suspicious about the cybersecurity of their workplaces, they'll become more open to network owners implementing the kinds of security improvements that they currently resist.

Asset Management and Software Security Solutions

- An IT professional noted that many organizations don't have a complete understanding of where their electronic assets are located and, as a result, must resort to managing assets in an indirect fashion by issuing device calls to identify asset matches. The CISO agreed, noting that the BYOD trend, for instance, makes visibility into devices connecting into the network more difficult. He added, however, that he isn't surprised by the current lack of clear asset management procedures – especially because the networks to which assets connect often comprise multiple smaller, federated networks. The CISO explained that HCO 2 occasionally acquires medical facilities that have existing networks of their own and then absorbs those legacy networks into its community network. As an example, he described a hospital that once maintained a wireless network with very strict access permission rules. Those rules had worked because the hospital had hosted only five or six devices as compared to the 50,000 devices on the HCO 2 network. With its addition to the HCO 2 community, however, it was required to

adopt HCO 2's wireless rules. While the hospital now enjoys the benefits of easier provisioning through HCO 2's community network, its accordant cyber risks have substantially increased.

- An insurer then advised that he worked with a client that once employed an IT professional who downloaded a health care IT database onto a jump drive, took it home to work on his personal laptop, and then uploaded it back on his work computer – all without any malicious intention. Years later, the individual sold his personal laptop at a second-hand store. The person who bought it found the sensitive information and offered to return it to the client for $10,000. The insurer asked how HCO 2 protects itself against this type of risk. The CISO replied that to chase down incidents like this one, health care organizations would need an impossibly huge staff. Accordingly, they must accept some level of data breach vulnerability as residual risk because health care data is the lifeblood of their businesses operations. He explained that if rules make it too difficult to move data around, even in the name of security, the efficiency of an entire organization will be compromised and service standards will degrade accordingly.

- A second insurer asked if HCO 2 is using data loss prevention (DLP) software to monitor information downloaded onto removable media.[8] The CISO responded that HCO 2 is beginning to successfully use DLP software for e-mail and device-based checking. He advised, however, that implementing DLP software for network-based checks and monitoring traffic exiting the HCO 2 network remains difficult given the sheer amount of data that it must examine. The CISO explained that that DLP software allows health care organizations to see patient data on almost all of its many machines – to such an extent that they're "swimming in data." Under those circumstances, he stated, it can be very challenging to determine what type of indicator should even trigger a DLP event. The CISO advised that he's consequently pushing HCO 2 to adopt an enterprise desktop encryption policy to better address network-level data loss.

- An IT professional next asked about the utility of Database Activity Monitoring (DAM),[9] which monitors, captures, and records database events in near real-time and provides alerts about information policy violations. The CISO replied that DAM can be useful for mitigating data breach risks but that even DAM processes many not provide sufficient clarity into the activities that are happening "at their source." He stated that thoroughly exploring all questionable

[8] Data loss prevention (DLP) refers to systems that detect potential data breach and/or exfiltration transmissions and prevent them by monitoring, detecting, and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). Wikipedia. Data Loss Prevention Software. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/Data_loss_prevention_software [15 January 2014].

[9] Database Activity Monitoring (DAM) refers to the observation of actions in a database. SearchITChannel. Database Activity Monitoring (DAM). ONLINE. N.D. Available: http://searchitchannel.techtarget.com/definition/database-activity-monitoring-DAM [11 January 2014]. DAM can be accomplished through a combination of several methods, including network sniffing, reading of database audit logs and/or system tables and memory scraping. *Id*. Regardless of the methodology chosen, the data must be correlated in order to detect and get a more accurate picture of what's going on within the database. *Id*.

database events requires a significant amount of analytical manpower – a dedicated use of resources that most health care organizations, including HCO 2, cannot afford.

HCO 2 Risk Management Culture

Governance

- The CISO stated that HCO 2 is not organized like a conventional business but rather as a federation of approximately 8,000 small businesses. That construct, he continued, contains a multitude of individual research protocols and features leaders in each of those small businesses who exercise significant levels of autonomy. Simply protecting sensitive information across those many entities, he stated, is a sufficiently challenging problem. His job as a security specialist therefore is to try to convince everyone to "row in the same [security] direction."

- The CISO advised that given this environment, the HCO 2 board does not exercise as much centralized control in practice as do the boards of for-profit companies. Even if HCO 2 board members had such control, however, his ability to communicate cyber risks to them is further complicated by the highly technical nature of most cybersecurity problems. It can be very difficult to clearly define the boundaries of what constitutes information security in the health care sector, he observed, and justifying priorities to leadership accordingly becomes very challenging.

- The CISO then referenced HCO 2's IT strategy to describe how and where cybersecurity is prioritized within the HCO 2 community. That strategy, he said, focuses on five core concepts: (1) functionality; (2) usability; (3) portability/extensibility/interoperability (highlighting interoperability among systems); (4) resilience; and (5) security. HCO 2 essentially divides 100% of its IT budget five ways, he explained, with each division receiving a 20% share. The CISO added (happily) that "because resilience and security work together," he ends up with 40% of the resources. He concluded that while the IT strategy is not a security strategy, it nevertheless helps explain HCO 2's overall priorities and allocation of resources.

Strategies for Success

- The CISO reported that HCO 2 does not have a single cybersecurity strategy but instead "different strategies for different components of [HCO 2's] security efforts." He emphasized that the gap between strategy and tactics is consequently narrower for HCO 2 than in other entities given its construct as "a federation of multiple quasi-independent organizations." To illustrate his point, the CISO explained that he used to work individually with each HCO 2 business unit on its particular cybersecurity needs. That became overwhelming. Now, he stated, it's more effective and efficient to simply "watch the data." If he sees data leaving a major warehouse, he continued, he looks to where it's sent and then pushes more responsible security practices out to the entire HCO 2 community in order to collectively address the underlying issue.

- The CISO stressed his ongoing need to clearly communicate the pervasiveness of cyber risks to HCO 2 leadership in order to refine and mature the organization's existing risk management structures and to manage them more effectively. "When you have a culture that is structured to provide maximum benefit for science," he observed, "there's going to be an information security downside." The CISO advised that he hasn't gotten very far by focusing just on security risks and their potential impact on HCO 2's reputation. Instead, he stated, he focuses primarily on *compliance* risks and their potential impact on HCO 2's reputation. He explained that this framing through HIPAA enables him to focus on contrasts between risk management efforts. For example, he can draw distinctions between comprehensive ERM programs that other health care organizations have developed with the more modest DLP software and other solutions that HCO 2 has implemented. The CISO asserted that when he's able to demonstrate that other major competitors and peers take advantage of advanced risk management steps, he's more likely to receive funding to perform similar work.

- The CISO mentioned that this approach to securing funding is more effective in his environment than explicitly linking his cybersecurity resources requests to HCO 2's overall risk management strategy, which tends to develop through a very slow-moving and bureaucratic process. He stated that he instead "improvises" to fix problems. Focusing tactically on compliance risks that arise in the day-to-day environment, he added, has proven a highly successful way to obtain the cybersecurity funding he needs. "If we need to develop software and defeat hackers," he explained, "we do it and there's no need for the fanfare of a strategy to do it." He added that he nevertheless tries to link to "whatever strategy is in the works at the time" as a starting point before using tactics to actually fix the problems at hand. The CISO noted, however, that this approach makes it harder for him to translate HCO 2's current cybersecurity needs into strategic terms.

- The CISO advised that to support this approach, he and his team maintain "scorecards" that reflect cyber incident counts across the HCO 2 community. In the eyes of his leadership, he explained, the decreasing numbers of HIPAA notification events over recent years show that his efforts have been fairly effective. He acknowledged, however, that his tactics address only the tip of the iceberg – i.e., for compliance-based risk management purposes only – and that malicious hacker risks to EHRs and their supporting IT technology continue to escalate. The CISO asserted that, going forward, HCO 2 leadership must look beyond regulations-based cyber investments in order to better address growing risks from these and other threat sources.

- The CISO reported that one area where he has had some strategic success is with the HCO 2 workforce. He stated that he's told human resource personnel that under the surface, cyber risk is the greatest risk HCO 2 faces. He accordingly collaborates with the HCO 2 human resources department to try to modify the risk culture itself – through training opportunities and other initiatives – rather than address cyber risks by technical means alone (e.g., making the compliance risk case for encrypting more laptops). He reported that he's seen progress among

cyber risk professionals across the HCO 2 community as a result of this engagement but that communication of cyber risk to top-level leadership remains difficult.

- When asked by a risk manager what "carrots" he uses to encourage more cybersecurity investment across HCO 2, the CISO quipped that his approach is to "stab leadership and security officers with the carrot" – that is, he highlights the negative ramifications (e.g., fines, public shaming) for non-compliance with HIPAA and ties as much of his security agenda as possible to existing compliance requirements. He did cite one incentive, however, that he routinely discusses with cybersecurity professionals who work on the medical research side of the HCO 2 enterprise: the Federal Information Security Management Act (FISMA).[10] The CISO explained that he tells his colleagues that investing in IT infrastructure to satisfy FISMA requirements makes it marginally easier to apply for future grants from the Federal Government. This marginal value, he asserted, may increase over time and further justify the investment.

Compliance Versus Enterprise Risk Management

Costs, Benefits, and the Power of Compliance

- An IT professional challenged the CISO's described approach to risk management, claiming that absent an enterprise risk-based approach to cybersecurity investment, HCO 2 will continually fall behind rapidly evolving cyber threats. A critical infrastructure representative concurred, noting that, "Strategy is not grand planning but the ability to step into board meetings, present a refined elevator pitch, and apply actions to the basic principles outlined in that pitch." The representative advised that he uses three words as the foundation of that elevator pitch – aggregate, automate, and accelerate – that lie at the root of his organization's operations. He then observed that risk management strategy is not so much about deploying tools as it is about helping people understand risk issues.

- The CISO responded that he runs a risk-based security program, albeit with compliance risk as its starting point, and that he too uses three words in his own pitches to HCO 2 leadership for funding – "see, segment, and spend." While he attempts to reduce investments involved in each category, he added, he's not overly focused on reducing costs because he's not yet come to the point where he's not getting the money he requests. The CISO acknowledged HCO 2's longer-term need to move beyond HIPAA-based cybersecurity investments but added that those investments will come over time once his leadership comes to understand the full range of cyber risks that HCO 2 faces.

- A risk manager then asked how the CISO uses cost/benefit considerations to inform his cybersecurity investment portfolio. He replied that he and his team have developed a series of metrics based on what it will cost the organization in terms of HIPAA fines if specific cyber incidents occur without appropriate controls being in place. Put simply, he advised, he's

[10] The Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.) was enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899).

developed a cost avoidance structure that helps him highlight specific actions that HCO 2 should take now to completely avoid or otherwise mitigate losses. "My approach," he continued, "is to tell my leadership the following: when the HIPAA cops come in and turn over all the tables and find other things as a result of this breach, this is what we're likely to pay in fines; if we do these five things, we'll likely reduce the fines by X amount." This approach works, he added, because it's often too difficult to predict other losses associated with a breach (e.g., the value of lost IP).

- The CISO concluded that while HIPAA accordingly might not help him address "freak breaches" – that is, the kinds of breaches that a more strategic approach might anticipate – the fines that arise from HIPAA compliance failures are something his leadership immediately understands. In short, HIPAA serves as a powerful tool to justify at least a subset of very worthy cybersecurity investments. The CISO nevertheless lamented that HIPAA does not better address cyber risks more generally given its role as HCO 2's primary driver of IT security funding.

Costs, Benefits, and Enterprise Approaches

- An IT professional asked whether HCO 2 hosts a cross-domain committee to examine and address cyber risks on an enterprise level. The CISO replied that although such a committee once existed, it ultimately failed because "it didn't sign the checks."

- An insurer responded that, in a highly federated system such as the HCO 2 community, establishing a cross-functional risk management group comprised of senior representatives from HCO 2's many business units would be helpful. He stated that such a group could help those representatives explain what cyber risk "costs" – not to the entire HCO 2 enterprise but to the individual HCO 2 business units themselves. Using such a structure, he advised, would empower the HCO 2 business units to self-identify and address the cyber risks of greatest importance to them. The CISO agreed in theory but emphasized that cyber risk mitigation comes with an institutional cost in the health care context. He explained that HIPAA regulations do not apply to HCO 2's individual business units but to the organization as a whole. He added that HCO 2 consequently has been working to bring all its cyber risk management activities within a single, organization-wide cost/benefit analysis. He described that analysis as one that is significantly more mature today than ten years ago. The CISO then explained (again) that what drives that analysis are the follow-on costs of a cyber incident – that is, the total fines that will be imposed upon HCO 2 *organizationally* as a result of a HIPAA violation.

- A second insurer asked if a cross-functional group would work better if it was allowed to "sign checks" – that is, integrate cyber into the overall incentives structure of the organization in order to motivate change. The CISO responded that he doubted this approach would succeed – not only for the reasons previously stated but also given the likely difficulties involved with incentivizing the vast number of end users within the HCO 2 environment. He explained that given their sheer number of doctors, students, and others within that environment, taking cybersecurity all the way down to the individual level would be tough. "We should do a better

job of changing end user behavior," he acknowledged, "but we're not at a mature enough level to do this yet."

- The insurer then asked if the CISO's calculus would change if a cross-functional group was empowered to sign checks to cover things beyond technology expenditures, including insurance and public relations efforts. The CISO replied that he could justify such expenditures already through his team's HIPAA compliance efforts.

REGULATION

- A risk manager commented that HCO 2's risk culture appears to be "slowing its progress toward meaningfully addressing cyber risks," and asked if cybersecurity regulation beyond HIPAA could help drive improvements. He specifically referenced regulatory actions in the financial sector that have helped companies to internalize cyber risks posed by malicious hackers and others by providing them with a binary choice: compliance or non-compliance. The risk manager observed that catastrophic risk models of cyber and other incidents often do not resonate with organizational leadership in the financial sector because of their inherent ambiguity – in other words, even mature catastrophic risk models cannot effectively demonstrate that a company will be driven out of business by a given catastrophic event. On the other hand, he continued, leadership knows that regulatory non-compliance can very quickly put a bank out of business. This realization, he concluded, often motivates immediate action on the cybersecurity front.

- The CISO replied that cybersecurity-focused regulatory authorities have indeed driven high levels of compliance within the IT security community generally but not as heavily within the health care community. He reiterated, however, that all research performed by HCO 2 on behalf of the Federal Government is subject to FISMA and NIST 800-53 security regulations and requirements. As a result, he noted, those authorities have been a "huge" driver for enhanced cybersecurity on the medical research side of the HCO 2 enterprise. The CISO advised that herding the FISMA and NIST 800-53 compliance efforts of multiple business units within even this more discrete area, however, presents ongoing and significant challenges.

- An insurer asked the CISO if the concept of meaningful use, as defined in the HITECH Act is also driving his efforts.[11] The CISO responded affirmatively, explaining that the meaningful use paradigm now requires him to consider the security of data at-rest in addition to data in-motion. He asserted that this will invariably lead to a strategic requirement to encrypt entire databases, adding that he'd "love" to be able to reference a current law or regulation to justify such action. In the meantime, the CISO concluded, real-time security issues that impact the delivery of medical services continue to dominate his responsibility set and accordingly require the bulk of his funding resources.

[11] *See* HITECH Act "meaningful use" definition, *supra* note 5.

Reputational Risks

- A critical infrastructure representative from another health care organization noted that his institution faces many of the same cultural challenges and issues as HCO 2 when it comes to motivating senior leadership to take action against cyber risks. He reported that his board members also struggle to meaningfully manage end-user behavior in addition to the architecture-related cyber risks that the CISO described. The representative added that his board members have only a limited understanding about where their organization "stacks up" against existing security models. Unlike the HCO 2 board, he asserted, reputational and safety risks nevertheless are huge issues for his board and have motivated several deep dives into his organization's broader cyber risk management practices. These deep dives, he observed, have resulted in the creation of several cybersecurity investment strategies. The representative concluded that his organization therefore appears to be less motivated by news of individual HIPAA breaches than is apparently the case at HCO 2.

- A social scientist then asked if any risk management processes broadly address cyber-related reputational risks. He suggested that such processes must be more complex than simply addressing compliance issues and instead might include such areas as investment relations, crisis management, and the like. An insurer replied that a primary consideration for health care and other organizations should be mitigating exposure to reputational risk and that they should not limit the scope of their incident response activity to just regulatory compliance. The social scientist agreed, noting that crisis management communications were particularly essential. "There's a significant difference between proactively disclosing that an organization had one major cyber incident during a given year," he stated, "and responding to a negative article about a cyber incident in the New York Times." The social scientist added that reputational losses can easily trump business fines.

- The CISO responded that although HCO 2 does face reputational risks for security breaches – and has suffered related losses in the past – the potential costs for failing to comply with HIPAA are, in many respects, worse. He then presented a hypothetical about a patient with a strange, life-threatening disease whose doctor says he's going to put the patient's EHRs on a CD and hand it out to everyone in Times Square. Despite this threatened breach of privacy, he continued, the patient still will say to the doctor, "Treat me." The CISO observed that this sums up where the health care sector is focused when it comes to cybersecurity: on securing medical IT to ensure effective patient treatment rather than the security of patient data.

HCO 2 Use Case

The Incident

- The CISO described a cyber incident at HCO 2 that involved malicious hackers who inserted malware via Structured Query Language (SQL) injection through a web interface that was used

to control an electron microscope in a student lab.[12] The malware caused several HCO 2 network servers to beacon out to various bad overseas Internet Protocol (IP) addresses. The incursions affected an administrator account, and the CISO accordingly contacted the server administrator – a non-central IT participant – to alert him to the problem. That individual subsequently checked his systems' diagnostics and blocked the bad IP addresses. After taking over the server that controlled the web interface, the malicious hackers had apparently waited to see what other servers communicated with it. In so doing, they compromised a total of 30 servers with the same administrator account.

- The malicious hackers had kept a low profile in order to access as much information from employee credentials as possible. The CISO stated that it wasn't clear how much agency was involved in the attack but speculated that it could have been highly automated. As a result, the incursion may not have been as aggressively exploratory as it might otherwise have been. The CISO explained that his concern was less about the disruption of applications and more about the addition of unauthorized and undesired functionality on the HCO 2 network. On the contrary, none of the organization's applications had been disrupted to the point of causing financial loss. Cleaning up the infected machines, however, posed a major challenge because the malicious hackers had been able to move around quickly among multiple machines.

USE CASE IMPLICATIONS

- The CISO described this and incidents like it as typical within the health care sector and stated that most go unnoticed because any associated loss of functionality is rare. He explained that the bad IP addresses involved in this use case, however, had fortuitously been published in a threat alert bulletin from the REN-ISAC. An analyst on his team who happened upon the bulletin while reviewing his email plugged in the addresses and found the problem. The CISO added that while HCO 2 eventually would have discovered the beaconing activity when it performed its routine network scans, the information sharing by the REN-ISAC combined with the diligence of the analyst brought about a much quicker fix.

- The CISO explained that the use case incident underscores the fact that health care organizations are just as much targets of malicious cyber actors as are defense contractors and other more "in the news" organizations. This kind of event, he added, demonstrates in stark terms HIPAA's shortcomings when it comes to motivating effective cyber risk management investment against malicious hackers.

[12] Structured Query Language (SQL) injection refers to an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code. United States Computer Emergency Readiness Team (US-CERT). SQL Injection. ONLINE. June 22, 2012. Available: http://www.us-cert.gov/security-publications/sql-injection [29 January 2014]. SQL injection usually involves a combination of "overelevated" permissions, unsanitized/untyped user input, and/or true software (database) vulnerabilities. *Id*. Since SQL injection is possible even when no traditional software vulnerabilities exist, mitigation is often much more complicated than simply applying a security patch. *Id*.

- The CISO reiterated his concern that organizations such as HCO 2 focus primarily – and almost exclusively – on the fines they face for failing to comply with HIPAA rather than the larger cybersecurity picture. Malicious hackers may be actively trolling their networks in an effort to exfiltrate IP data, he continued, but they'll never know it because they're not incentivized to proactively find and remove them. He concluded that without evolving beyond their currently excessive focus on compliance, health care organizations may be in for rough days ahead.

CYBERSECURITY INSURANCE

- The CISO explained that HCO 2 maintains cybersecurity insurance with very high deductibles for some data breach risks. He noted, however, that HCO 2 has never been compensated for a cyber incident, so the "real limits" of what its policies cover have not undergone a real-world test. The CISO advised that he engages with insurance underwriters as part of his job duties and doesn't "pull punches" by withholding detailed information about the kinds of incidents that HCO 2 has experienced and the additional risks it faces. He added, however, that he doesn't have a high degree of confidence that HCO 2's cyber insurance will fully cover the costs of an actual cyber incident. He nevertheless believes that cybersecurity insurance is worth having given its *potential* for coverage.

HEALTH CARE ORGANIZATION 3

ORGANIZATION OVERVIEW: The Risk Management Director (RMD) and Global Operations Center Director (GOCD) for Health Care Organization 3 (HCO 3) described HCO 3 as a medical vendor comprised of three major divisions: health care consumer products, pharmaceuticals, and medical devices/technology. Each division, they advised, is responsible for its own research and development, corporate sales, and supply chain management activities, including risk management activities. The RMD further characterized HCO 3 as a "highly federated and distributed international enterprise" that includes 260 operating companies located in some 60 countries. "We have a decentralized management approach," he noted, "with eggs in 260 baskets." To illustrate his point, the RMD referenced the fact that approximately 150 of HCO 3's operating companies host their own ERP software platforms.[13] He remarked that this is a bit more than even HCO 3 can bear, and that it recently initiated a standardization program to bring the platforms under a "single management set" in order to promote greater efficiencies.

The RMD asserted that cyber attacks are less likely to affect the entire HCO 3 organization given its highly federated and distributed nature. The company accordingly doesn't maintain fully centralized security operations – employing just 350 people in that category, of whom only 50-60 focus on information security. The RMD explained that only a small number of those professionals work on "true" cybersecurity. "We only do [cyber risk] analysis when we're tipped off," he observed. "While we're moving from a reactionary to a 'pro-actionary' approach, from a corporate perspective we need to fight day-to-day fires to keep [HCO 3] operations up and running."

The GOCD added that to support this tactical battle rhythm, he manages a strategic operations center staffed with a "total incident response team" that responds to all business critical outages that impact HCO 3's worldwide operations. "If a server is down and we're not making hip replacements," he stated, "we're losing $100,000 an hour." The GOCD advised that he's deployed a number of staff internationally to support his team's efforts.

USE CASE PRESENTATION AND DISCUSSION:

CYBER RISK LANDSCAPE

- The RMD reported that HCO 3 rarely sells products and services directly to consumers, a business model that effectively transfers a significant amount of cyber risk to its outsourced providers and intermediaries. He observed that this arrangement makes HCO 3 a somewhat "different kind of animal" than some of its competitors. The RMD nevertheless described the company's priority risk as "product safety." While the majority of HCO 3's customers are medical professionals or medical enterprises, he added, the company must ensure that its risk management efforts remain focused on the ultimate consumer: individuals who directly use or are otherwise treated with HCO 3's products.

[13] *See* ERP definition, *supra* note 7.

- The RMD explained that companies like HCO 3 face complex challenges in implementing security policies across their multiple divisions, numerous operating companies, and myriad business units. For example, he continued, different consumers within the same industry sector might use a HCO 3 technology for very different purposes. That same technology, in turn, could be marketed for all those and additional purposes in still other industry sectors. That's where things get complicated from a cyber risk management standpoint. The RMD advised that each HCO 3 technology carries with it varying IT security requirements depending upon its intended use. The widely varying and sheer number of those intended uses – within and across industry sectors – makes standardization of security policies for vended technologies very difficult.

- The RMD noted that another source of HCO 3 cyber risk stems from the fact that its major growth drivers are emerging medical markets in developing nations. Many of those nations, he commented, do not have the underlying infrastructure necessary to implement the full scope of IT requirements that would be expected of medical vendors in developed countries. He specifically mentioned in this regard the infeasibility of bringing an ERP software platform into medical markets in China, Malaysia, and Vietnam.[14] He then stated that ROI considerations present still another obstacle. "We can't justify taking [an ERP software platform] that costs $100 million to operate annually into a developing market," he observed, "when we generate only $2 million in revenue there annually."

- The RMD explained that yet another obstacle to HCO 3's cyber risk management efforts arises from the highly varied legal, security (i.e., employee safety), and other compliance requirements that exist within the multiple international, state, and local jurisdictions in which the company operates. He advised that HCO 3 works hard to harmonize its security and other compliance requirements through a unified Governance, Risk Management, and Compliance (GRC) platform,[15] but that disparities among its host jurisdictions significantly complicate its efforts. He explained that HCO 3 nevertheless requires all of its operating companies to address four overarching risk categories, regardless of their geographic location:

    - Strategic Risk. HCO 3's strategic risk assessments focus on the loss of IP, especially in so-called "grey markets."[16]

---

[14] *Id*.

[15] The term "GRC platform" or "GRC software" refers to software that allows publicly-held companies to integrate and manage IT operations that are subject to regulation. TechTarget.com. GRC (Governance, Risk Management, Compliance) Software. ONLINE. 3 May 2010. Available: http://searchcio.techtarget.com/definition/GRC-governance-risk-management-and-compliance-software [21 January 2014]. Such software typically combines applications that manage the core functions of GRC into a single integrated package. *Id*. GRC software enables an organization to pursue a systematic, organized approach to managing GRC-related strategy and implementation. *Id.* Instead of keeping data in separate "silos," administrators can use a single framework to monitor and enforce rules and procedures. *Id*. Successful installations enable organizations to manage risk, reduce costs incurred by multiple installations and minimize complexity for managers. *Id.*

[16] The term "grey market" refers to a market where a product is bought and sold outside the manufacturer's authorized trading channels. Investopedia. Grey Market. ONLINE. N.D. Available: http://www.investopedia.com/terms/g/greymarket.asp [14 January 2014]. For example, if a store owner is an

- Operational Risk. HCO 3's operational risk assessments focus on disruption to product supply; physical damage and disruption; and the confidentiality, integrity, and availability of IT resources. HCO 3's primary concern among these categories is the availability of IT resources because the company can't make money if its systems aren't operating.

- Compliance Risk. HCO 3's compliance risk management efforts focus on global regulation, including but not limited to regulations that pertain to cybersecurity, employee health, patient safety, clinical trials, and tax policy.

- Financial and Reporting Risk. HCO 3's financial and reporting risk management efforts focus on ensuring compliance with relevant reporting requirements. In the wake of the Sarbanes-Oxley Act, the company places an increasingly high priority on enhancing its reporting processes.[17]

- The RMD explained that for all four of these overarching risk categories, each HCO 3 operating company tailors its related policies, processes, and programs to address the specific circumstances and unique requirements of its host jurisdiction.

- Regarding the "Financial and Reporting Risk" category, the RMD warned that the greater emphasis on reporting requirements occasioned by the Sarbanes-Oxley Act has the potential to complicate the actual security posture of public companies by "unintentionally turning security programs into compliance programs." The RMD asserted that HCO 3 accordingly works actively to counteract this potential drift.

HCO 3 Risk Management Culture

Governance

- The RMD stated that despite the highly varied environments in which HCO 3 does business, he nevertheless establishes uniform corporate policies that apply to all of its operating companies in several key areas such as digital asset risk management and internal IT control adoption. With the blessing of the HCO 3 board of directors, he then "pushes out" those policies for implementation. The RMD added that HCO 3 hosts a number of audit and compliance

---

unauthorized dealer of a certain high-end electronics brand, the product is considered to be sold on the grey market. *Id*.

[17] The Sarbanes–Oxley Act of 2002 (Pub.L. 107–204, 116 Stat. 745, enacted July 30, 2002) , also known as Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Wikipedia. Sarbanes-Oxley Act. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act [15 January 2014]. Under the law, top management must now individually certify the accuracy of financial information. *Id*. In addition, penalties for fraudulent financial activity are much more severe. *Id*. The law likewise increases the independence of outside auditors who review the accuracy of corporate financial statements and increases the oversight role of boards of directors. *Id*.

committees that have direct access to the board to assist in this regard, superseding the CEO in certain circumstances. For example, he continued, all business risk matters and "damage to public trust" issues – no matter where they arise globally – go directly to the board for review and action.

- The RMD advised that to bring cohesion to its overall risk management process, HCO 3 hosts an enterprise risk management council (ERM Council) to better understand and address risks that arise across the company. He explained that HCO 3 established the ERM Council only after agreeing to do so as part of a lawsuit settlement agreement. While pursuing an ERM strategy was the right thing to do anyway, he observed, the lawsuit underscored for everyone the importance of pursuing proactive approaches to risk management.

Strategies for Success

ERM Frameworks

- The RMD reported that HCO 3's health care consumer products, pharmaceuticals, and medical devices/technology divisions have all adopted and use their own ERM Frameworks to identify and assess their external and internal risks. While those frameworks reflect the specific business lines in question, and are informed by each division's available funding, business plan, and ERP solution, all share the following five process steps:

    - Identify and address external and internal risk. This step includes assessing the impacts of an event, system vulnerabilities, and environmental threats to the division.

    - Determine an appropriate risk response. This step represents the strategy "piece" of the ERM process, where decisions are made on how best to allocate technological solutions, programmatic controls, and human resources for the division's benefit.

    - Establish policies and procedures to support the risk response. This step includes the division's development of accountability structures, internal testing, programmatic controls, and response systems – and/or the adoption of well-established response guidance in the form of handbooks, policies, and other documents – to support risk response. Those documents may include scripts for explaining why an operating company within a division presents a particular risk and/or requires a certain risk control.

    - Communicate risks and establish mitigation plans. This step involves ensuring board visibility into a division's risks and related risk management efforts; establishing a business case for those efforts; and obtaining funding and other support for them.

    - Monitor risk program efficacy continuously.

- The RMD commented that for each of these steps, technology investment represents only one part of the risk management equation, which also includes people and process. HCO 3 consequently sponsors employee awareness programs, for example, to highlight processes that can address incidents effectively. The goal, he stated, is to instill knowledge about cyber risks and personal accountability for addressing them across the entire enterprise.

- A critical infrastructure representative asked the RMD if anyone working at HCO 3 has, in their performance review, a requirement for creating a controlled environment for HCO 3's multiple ERM Frameworks. The RMD responded affirmatively, noting that his own performance review includes the stipulation that he "maintain a controlled environment."

Catastrophe Planning

- The GOCD explained what would happen if HCO 3 were to experience a catastrophic event that required a major risk management decision such as shutting down operations at a key manufacturing plant. He advised that HCO 3 has developed a "run book" that designates a corporate emergency response team known as a "C-CERT" to convene and begin managing the incident response immediately. Depending upon the kind and duration of the event, he added, C-CERT members might include human resources, legal, operations, public relations, and other personnel. The GOCD reported that HCO 3 has not yet run a cyber exercise to test the run book but has scheduled one in the near future.

- The RMD added that the run book includes HCO 3's formal escalation policy for engaging the right company leadership at the right time. He explained that even without being exercised, the "relevant people [already] know their roles" during a variety of event scenarios and have received related training for them through HCO 3's extensive learning management system. The RMD noted that although he and the GOCD have a direct line to the CEO, they would follow the run book protocol regarding when and under what circumstances to contact him during an emergency situation.

HCO 3 Use Case

The Incident

- The GOCD described a cyber incident at HCO 3 that involved the CryptoLocker virus.[18] During the incident, malicious hackers obtained illicit access to two company laptops and mapped their drives. The malicious hackers then encrypted files stored on the drives. When HCO 3 employees logged onto the laptops, a pop-up box appeared stating, "You have to pay $400 if you want to access your files." While the mapping didn't extend to business critical files, the

[18] CryptoLocker is a new variant of ransomware that restricts access to infected computers and demands the victim provide a payment to the attackers in order to decrypt and recover their files. United States Computer Emergency Readiness Team (US-CERT). CryptoLocker Ransomware Infections. ONLINE. Nov. 18, 2013. Available: https://www.us-cert.gov/ncas/alerts/TA13-309A [14 January 2014]. The primary means of infection appears to be phishing emails containing malicious attachments. *Id.*

GOCD explained that the situation would have been "mission critical" had it done so. Even with the contained impact of this particular event, he noted, his team still had to restore approximately 5,000 files from backup tapes.

Incident Observations

- The GOCD emphasized the importance of bringing response teams into strategic discussions when addressing real-time, unfolding events like the CryptoLocker incident. The perspectives of those teams, he advised, are essential for determining what an event actually means to a business and how it should be addressed over the long term.

- The RMD added that cyber risk management cultures vary from company to company depending upon the nature of their business. Given HCO 3's emphasis on maintaining the availability of operations across its three business divisions, he continued, HCO 3 has prioritized a risk management process that's highly reactive to incidents like the one described in the use case.

Use Case Questions

Cost/Benefit Communications to Leadership

Risk Management Roadmaps

- A critical infrastructure representative observed that the CryptoLocker incident was not a catastrophic or otherwise corporate-wide event. He then asked how HCO 3 nevertheless could "use it" to both inform and justify risk-based investments to the board. The GOCD responded that his team meets monthly with HCO 3's Chief Technology Officer (CTO) to review significant security incidents and to determine what mitigation and controls to apply in response. He advised that HCO 3 has a well-established cyber risk management cycle that includes a lengthy list of cyber incidents that might impact the company and corresponding mitigations and controls that are specifically "road-mapped" to address them. When reviewing a significant cyber incident, he continued, the CTO will determine the urgency of executing an applicable road-mapped solution or a new one if necessary. The GOCD added that if an unforeseen cyber incident is sufficiently serious, the CTO can amend the incident list to include it and its corresponding mitigations and controls for future reference.

- The GOCD advised that this cyber risk management cycle directly informs how new cyber incidents are communicated to the board for action. "Depending on the need," he stated, "we can escalate a request for funds to the next year's business plan in order to respond to an unforeseen incident and then implement the appropriate mitigating control."

Assessing Costs

- When asked if HCO 3 uses a quantitative approach for assessing the costs of cyber incidents, the GOCD responded in the negative. While we're "firefighting" during an incident response, he stated, it's very difficult to determine the operational cost of a specific server being down or, for that matter, the value of exfiltrated IP. "When I crash my car, it's immediately obvious what the damage is," he added, "but how do we estimate the damage from a cyber incident?"

- The RMD agreed, noting that he uses both quantitative and qualitative approaches for his more strategic risk management work, especially when it comes to assessing the potential impacts of various cyber risks to HCO 3 supply chains. He advised that his quantitative assessment in this regard begins with a fundamental measure of time – for example, how long a server is down – and ends with a standardized back-solving approach to determine the cost of an associated outage of a given duration. This calculation, the RMD explained, enables him to use an ordinal scale, normalized between 1 and 5, that assigns different parameters to estimate the overall costs of an attack on production; the state of HCO 3's preparedness; and the likelihood of a risk occurring. For qualitative purposes, he concluded, he assigns different colors to the risks assessed through this approach – red, yellow, or green – so the board can compare them visually.

- A second critical infrastructure representative responded that determining cyber incident cost impacts are not as difficult as they might initially appear. She stated that that the Department of Defense (DoD), for example, as a matter of course estimates the dollar costs of downed servers and other IT equipment attacked by APTs and other intruders.[19]

Assessing Benefits

- A risk manager asked the RMD how he goes about demonstrating that one security control is more effective than another for purposes of addressing a particular cyber risk. The RMD explained that he has good relationships with the investment professionals in his security portfolio who not only conduct those assessments but also make the appropriate business case to the board. "We map out three to five years for where we want to be," he stated, "and incorporate as part of our reviews an analysis of the incidents we've experienced, losses we've suffered, and the likely effectiveness of existing and new technologies to mitigate them in the future."

[19] Advanced Persistent Threat (APT) refers to a group, such as a government, with both the capability and intent to persistently and effectively target a specific entity. Wikipedia. Advanced Persistent Threat. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/Advanced_persistent_threat [21 January 2014]. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. *Id*.

- The RMD emphasized that a key part of analyzing a security control's effectiveness involves evaluating the technical maturity of the environments in which it will be deployed. A control that might work in a developed country, he explained, might be impossible to deploy in a developing one – especially if it involves new technology that needs access to modern telecommunications networks in order to function properly. While HCO 3 prioritizes deployment of security controls to locales wherever its data centers are located, the RMD concluded, it accordingly can't deploy them in all such locales.

MONITORING TRAFFIC FOR INDICATORS AND EVENTS

- In view of the CryptoLocker incident, a risk manager asked whether HCO 3 has considered decrypting all the packets leaving its network – i.e., full packet capture – as a means of preventing IP theft. The RMD responded that malicious hackers typically encrypt the "most interesting" content before it goes out, and that the capability to intercept and read it before it exits the network is therefore essential. "The members of the board are very visual," he continued, "so if you can show them that spreadsheets [rather than anonymous data packets] are on their way out the door, they immediately understand that we have a compromised machine."

- A critical infrastructure representative noted that full packet inspection of data leaving a network should itself be subject to risk analysis – not only to prioritize that traffic but also to identify, hold, and assess suspect packets that trigger alerts. He asserted that information security analysts need network optics technology to make appropriate risk management decisions about both unencrypted and encrypted data in real time. The representative noted that when it comes to encrypted packets, deep packet inspection associated with DLP solutions can help.[20] Specifically, he advised that properly configured DLP can provide sufficient context about the packets – e.g., they were obtained by abnormal access to a particular database – to justify automatically pulling them for decryption and review by analysts at a later date.

- The GOCD replied that while proactivity is a desirable goal for cyber risk management, the cost for monitoring all network traffic across the HCO 3 enterprise would be very high. He added that employees likely would not welcome the news that their personal use of network resources (e.g., online banking) is being inspected as part of a new corporate security initiative. Finally, he concluded, the Safe Harbor Privacy Principles are a significant consideration for companies like HCO 3 with an international presence and would raise significant hurdles to adopting a full packet inspection approach.[21]

---

[20] *See* DLP definition, *supra* note 8. One DLP category – advanced security measures – employs machine learning and temporal reasoning algorithms for detecting abnormal access to data and abnormal email exchange, honeypots for detecting authorized personnel with malicious intentions, and activity-based verification (e.g., recognition of keystrokes dynamics) for detecting abnormal access to data. *Id*.

[21] The Safe Harbor Privacy Principles, also known as the International Safe Harbor Privacy Principles or U.S. – EU Safe Harbor, provide a streamlined process for U.S. companies to comply with EU Directive 95/46/EC on

ADVANCED PERSISTENT THREAT RESPONSE

- An IT professional observed that HCO 3 is heavily involved in developing markets – including Brazil, Russia, India, and China, the so-called "BRIC" countries – where APTs are "imminently present." She then asked why, under the circumstances, HCO 3 is so focused on reactive security rather than proactive security measures. The GOCD responded that HCO 3 has taken the position that it has an Internet presence, it must assume that it's already been compromised by APTs (among others). Accordingly, while HCO 3 has made considerable investments in prevention technologies, especially perimeter defense technologies, it also must invest significantly in response – i.e., "reactive" activities. The RMD agreed, noting that a recent study had found that some 70% of companies have experienced a material cyber breach that they've chosen not to report. Given the fact that APTs are likely inside the networks of all those companies, he asserted, the primary question for them and HCO 3 is necessarily a reactive one: how fast can we find them and kick them out?

CYBERSECURITY INSURANCE

- A critical infrastructure representative asked how cost and benefit considerations inform HCO 3's cyber risk management decisions, including the purchase of cybersecurity insurance. The GOCD replied that HCO 3 does not currently carry cybersecurity insurance, relying instead on its aforementioned cyber risk management cycle and cyber incident run book to direct actions based on perceived costs and benefits to the company. He added that while HCO 3 is concerned about cyber risks that pose financial and/or reputational harm, both the cyber risk management cycle and cyber incident run book focus on cyber risks that could cause significant operational disruption. "The operational impact of an anticipated cyber incident determines its priority," he explained, "and directly informs the communication of an actual incident to the board."

- An IT professional then asked, given HCO 3's decision not to purchase cybersecurity insurance, whether or not HCO 3 self-insures or alternatively assumes the cost of a cyber incident when it occurs. The RMD responded that HCO 3 is actively considering whether to purchase a policy but

---

the protection of personal data. Wikipedia. International Safe Harbor Privacy Principles. ONLINE. N.D. Available: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles [22 January 2014]. Intended for organizations within the U.S. or EU that store customer data, the Safe Harbor Privacy Principles are designed to prevent accidental information disclosure or loss. *Id*. U.S. companies can opt into the program as long as they adhere to the seven principles outlined in the directive. *Id*. They include: (1) notice – individuals must be informed that their data is being collected and about how it will be used; (2) choice – individuals must have the ability to opt out of the collection and forward transfer of the data to third parties; (3) onward transfer – transfers of data to third parties may only occur to other organizations that follow adequate data protection principles; (4) security – reasonable efforts must be made to prevent loss of collected information; (5) data integrity – data must be relevant and reliable for the purpose it was collected for; (6) access – individuals must be able to access information held about them, and correct or delete it if it is inaccurate; and (7) enforcement – there must be effective means of enforcing these rules. *Id*. The process was developed by the U.S. Department of Commerce in consultation with the EU. *Id*.

is “not yet sold” on obtaining one given the overall effectiveness of its cyber risk management cycle and its “road-mapped” cyber risk mitigations and controls. HCO 3 has only finite resources, he explained, and the debate really is whether it gets more cybersecurity bang for the buck from purchasing a policy or installing intrusion detection and other solutions that HCO 3 has pre-selected to address anticipated cyber incidents. He added that HCO 3’s CISO and the company’s finance office will collectively make this call.

- The RMD emphasized that HCO 3 does not question the importance of managing cyber risk – including through risk transfer to insurers – but currently believes it has a reasonably effective range of alternate mitigation approaches to do so. He added that because HCO 3 does not maintain customer PII, it may not be a company that really needs cybersecurity insurance. When asked how HCO 3 nevertheless would manage a privacy breach if one occurred, the RMD responded that the company has a privacy plan in place. “We’re ultra-conservative in terms of recalling deficient products,” he commented, “and in the event of a privacy data breach our privacy office will adopt a similar posture.”

CONCLUSION

Roundtable participants commented that the cyber risk management use cases highlighted the need for a sustained dialogue between cybersecurity professionals and insurers about how they could better partner for the benefit of the organizations they serve. Several noted that both communities are only now getting to know one another. A joint effort to bring about complementary cyber risk mitigation and cyber risk transfer strategies, they observed, would advance the cybersecurity cause considerably – not just for health care organizations but for entities in other sectors as well.

A critical infrastructure representative described the presenting organizations as large enterprises with "low-level cybersecurity budget and staffing." That common characteristic, he continued, suggests that their respective leaders, despite some openness to ERM, care more about governance and regulatory compliance than true cybersecurity. Another critical infrastructure representative responded that, unlike the presenting organizations, approximately 80 percent of hospitals don't have even basic awareness about their cyber risks let alone strategies to address them. He called this state of affairs, "a big problem for [the] industry." The representative added that no matter what their approach to cyber risk management, the presenting organizations accordingly should be considered advanced cybersecurity managers within the health care market.

A risk manager commented that whether an organization adopts an ERM or a "regulatory compliance" approach to cyber risk management, cybersecurity insurance can serve as a "risk reducer" by incentivizing it to adopt better security controls in return for more coverage at lower cost. He added that car manufacturers introduced anti-lock brakes because *insurers* demanded them – not regulators. An IT professional concurred, noting, "The goal of getting lower premiums will drive [cyber] risk management investments higher . . . to that end, cybersecurity insurance can be used as a market incentive." A second risk manager agreed and asserted that regulatory compliance should be abandoned as a rationale for cyber risk management investments altogether in favor of ERM approaches. He emphasized that insurance is itself an ERM issue and that teams of experts – including CISOs and other cyber risk managers – should provide their input to the "check cutters" about what kinds of coverage to purchase, for what risk transfer purposes, and in what amounts.

An insurer acknowledged the benefits of ERM but noted that insurance also could be marketed as a way to prove regulatory compliance. If an organization has cybersecurity insurance, he noted, it must adhere to certain cybersecurity requirements, some of which may be required by law. Continued adherence to those requirements as evidenced by policy renewals therefore could signal that an organization is doing what it's supposed to be doing under the contract and – by extension – the law. An organization's chief risk officer accordingly could tell its chief financial officer that, "If we have this insurance, then we don't have to separately prove that we're complying with cybersecurity regulations." The insurer concluded that this could spare organizations considerable expense. An IT professional noted that insurance likewise could be used as an attestation method to obtain incentives such as priority in government procurement.

A second insurer cautioned, however, that cybersecurity insurance should not be considered an incentive that will somehow encourage critical infrastructure owners to use the Cybersecurity Framework called for in Executive Order 13636. Instead, she asserted, carriers will assess over the next several years what positive impact that framework has on the cyber loss experiences of the organizations that use it. She observed that, based on those experiences, carriers might incorporate into their policies those framework elements that demonstrably result in better cybersecurity outcomes. The framework accordingly might have an incentivizing *effect* through insurance contracts that require an insured to incorporate proven aspects of it into their cyber risk management programs in return for new and/or more extensive coverage – i.e., for cyber-related critical infrastructure loss. Several participants responded that insurers should identify what policy, programmatic, and other initiatives should be undertaken to encourage their entry into the first-party market for this purpose.

Roundtable leaders and organizers agreed to share this feedback with DHS and NPPD senior leadership and to communicate with participants about next steps.

APPENDIX: FULL AGENDA

Cybersecurity Insurance Roundtable

Health Care and Cyber Risk Management: Cost/Benefit Approaches

Wednesday, November 20, 2013

National Intellectual Property Rights Coordination Center

2451 Crystal Drive – Suite 200

Arlington, VA 20598-5105

AGENDA

8:00 – 8:30	Arrival/Registration
8:30 – 8:45	Opening Remarks from DHS/NPPD ○ *Tom Finan, Senior Cybersecurity Strategist and Counsel*
8:45 – 9:30	Health Care Use Case I Presentation
9:30 – 10:15	Group Discussion
10:15 – 10:30	Break
10:30 – 11:15	Health Care Use Case II Presentation
11:15 – 12:00	Group Discussion
12:00 – 1:00	Lunch (On Your Own)
1:00 – 1:45	Health Care Use Case III Presentation
1:45 – 2:30	Group Discussion
2:30 – 2:45	Break
2:45 – 3:30	Health Care Use Case IV Presentation
3:30 – 4:15	Group Discussion
4:15 – 4:30	Summary Discussion/Q&A/Close