GOOD GOVERNANCE CASE STUDY

AN ONLINE SERIES BY **THE GOVERNANCE INSTITUTE**

Governing Cyber Risk in Healthcare: Case Studies

SUMMER 2021

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

The Governance Institute®

The essential resource for governance knowledge and solutions®

1245 Q Street, Lincoln, NE 68508
(877) 712-8778

GovernanceInstitute.com
/The Governance Institute
/thegovinstitute

Jona Raasch	Chief Executive Officer
Cynthia Ballow	Vice President, Operations
Kathryn C. Peisert	Managing Editor
Glenn Kramer	Creative Director
Kayla Wagner	Senior Editor
Aliya Flores	Editor

The Governance Institute is a service of NRC Health. Leading in the field of healthcare governance since 1986, The Governance Institute provides education and information services to hospital and health system boards of directors across the country. For more information about our services, please call toll free at (877) 712-8778, or visit our Web site at GovernanceInstitute.com.

The Governance Institute endeavors to ensure the accuracy of the information it provides to its members. This publication contains data obtained from multiple sources, and The Governance Institute cannot guarantee the accuracy of the information or its analysis in all cases. The Governance Institute is not involved in representation of clinical, legal, accounting, or other professional services. Its publications should not be construed as professional advice based on any specific set of facts or circumstances. Ideas or opinions expressed remain the responsibility of the named author(s). In regards to matters that involve clinical practice and direct patient treatment, members are advised to consult with their medical staffs and senior management, or other appropriate professionals, prior to implementing any changes based on this publication. The Governance Institute is not responsible for any claims or losses that may arise from any errors or omissions in our publications whether caused by The Governance Institute or its sources.

Governing Cyber Risk in Healthcare: Case Studies

Healthcare cyber risk has risen exponentially in the past decade as hackers have increasingly targeted healthcare organizations due to the rise in black-market value of patient health information. Unfortunately, the COVID-19 pandemic served as the perfect storm, enabling cyber criminals to take advantage of an industry in crisis when all focus was diverted to saving lives and rapidly moving non-COVID patient care to the virtual space.

As no organization is immune in today's environment, healthcare boards need to better understand actual cyber threats facing their organizations and what the security team is doing in order to effectively mitigate cyber risk. It is an undertaking that should be integrated and aligned with the organization's programs and processes for identifying, prioritizing, and mitigating enterprise risk.

Understanding the board's role involves receiving the right level of information from the security team, presented in a way that the board can understand, along with arming itself with tough questions to hold the team accountable—and get past the jargon—to have robust discussions and decision making to support a strong enterprise cyber risk management (ECRM) program. It does not require deep technology or cybersecurity-related expertise, although we recommend that you bring such expertise to your board if possible.

To accompany a Governance Institute Strategy Toolbook by Bob Chaput, *Enterprise Cyber Risk Management*, we provide case studies below of three large health systems with significant experience in managing cyber risk, demonstrating how their boards support their ECRM programs:

- Providence, Renton, WA
- Spectrum Health, Grand Rapids, MI
- IU Health, Indianapolis, IN

Providence

Providence has significantly increased its investment in ECRM over the past several years. Adam Zoller, Chief Information Security Officer (CISO), leads the cybersecurity team of 250 people and reports to the system CIO. The board is regularly engaged and informed about Providence's cybersecurity risk and the programs in place to effectively mitigate that risk.

The cybersecurity team structure is set up as follows (each pillar is executive-led):

- **Threat and Vulnerability Management:** 24/7 security operations center, penetration testing (e.g., "ethical hacking"), and "red teaming" (multi-layered attack simulation).
- **Identity and Access Management:** includes identity engineering and authentication.
- **Governance Risk Compliance (GRC):** responsible for how IT risk is governed, such as how compliance is implemented, including regulatory compliance frameworks such as HIPAA and PCI-DSS (payment card industry data security

standard)[1]; how the system identifies and manages risk, and maintaining the risk register. This pillar integrates with Providence's enterprise risk organization under a separate team let by the CRO.

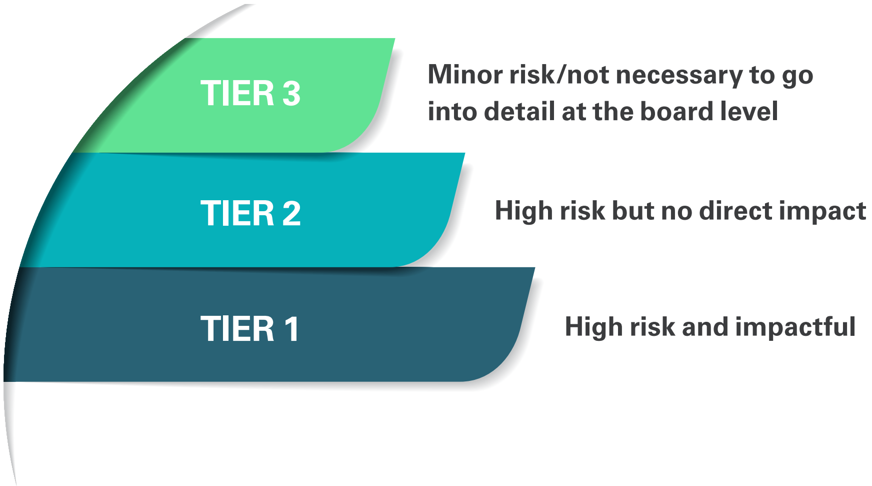
- **Office of the CISO:** this encompasses the cross-system functions that touch on every other pillar listed here. It includes communications training awareness, security strategy and maturity modeling, budget and finance/personnel, and security related to M&A and divestitures.
- **Providence Global Center:** the system's global security apparatus. A pillar leader at a site in India leads the night time/swing shift for Providence's security and operations center, as well as some extensions of the GRC and Identity and Access Management teams.

Providence is a large, regional system of 120,000 full-time caregivers serving 51 hospitals, 1,085 clinics, and a comprehensive range of health and social services across Alaska, California, Montana, New Mexico, Oregon, Texas, and Washington.

Arming the Board with the Right Information

Zoller presents to the system board quarterly, starting with an update on the projects and programs his team is advancing to directly reduce risk. For example, the system rolled out a new remote access solution, which is cloud-enabled and travels with the caregiver, to address risks around remote work (this roll-out began months prior to the pandemic; it accelerated and was completed during the pandemic). Zoller feels it is important to directly connect a given program to a specific risk. He then provides an overview of incidents the system faced over the last quarter: the volume, whether volume is increasing/decreasing and why, contributing factors, and so forth.

Providence stratifies its incidents into the following tiers:

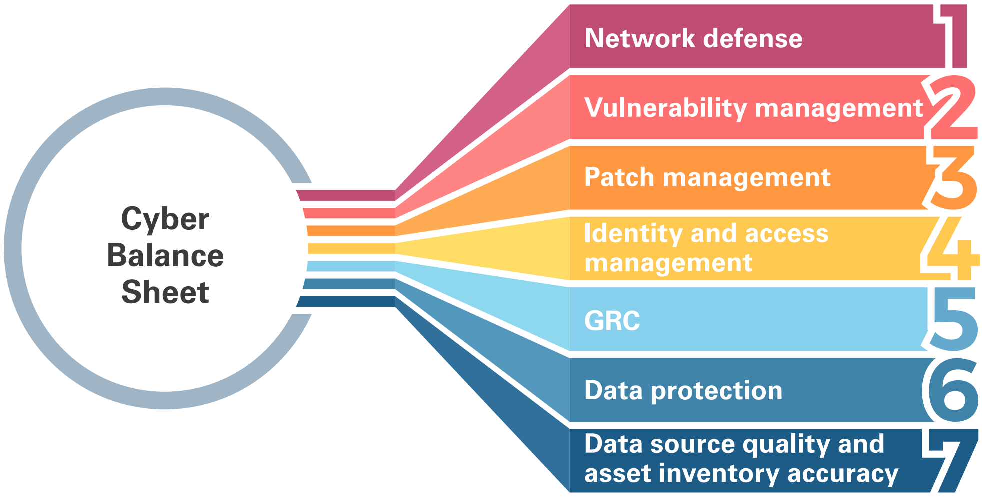

TIER 3
Minor risk/not necessary to go into detail at the board level
TIER 2
High risk but no direct impact
TIER 1
High risk and impactful

[1] The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. More information can be found at www.pcicomplianceguide.org/faq/.

Zoller gives the board a deep dive into the Tier 1 incidents, and his team keeps a running tally throughout the year. (The board receives a written report showing all incidents; however, Tier 2 incidents are rarely discussed at the board level, and Tier 3 incidents are not discussed.)

The final section of Zoller's report is a "threat spotlight" to both further board education and demonstrate actual threats that have targeted Providence recently. "For example, we have been targeted with phishing emails designed to steal Office 365 credentials over the last quarter, so I show the board screen shots of actual phishing emails our caregivers are receiving," said Zoller. "These demonstrate what the board should be watching out for, the types of information attempting to be stolen, and how threat actors are targeting Providence."

Zoller then runs down a quantitative risk reporting solution the system employs called the "Cyber Balance Sheet." Several domains are shown:

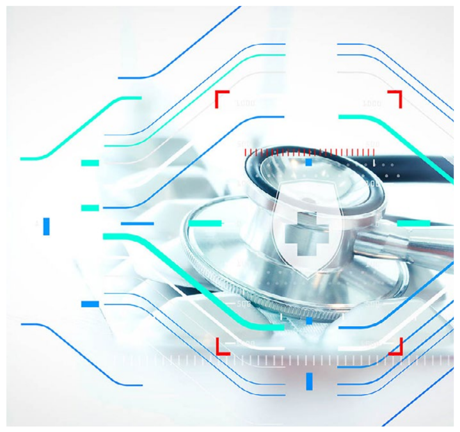

Cyber Balance Sheet
Network defense 1
Vulnerability management 2
Patch management 3
Identity and access management 4
GRC 5
Data protection 6
Data source quality and asset inventory accuracy 7

This dashboard gathers telemetry from the system's network defense and IT management tools across the enterprise, pipes it into a security data lake, then applies AI/visualization and analytics on top of the data to show a meaningful picture of Providence's network defense posture. "This allows me to have conversations with the board about the actual risks we face," explained Zoller. "I think it is easy to get caught up in the threat of the week or the day, such as SolarWinds, and then you spend two hours talking about what we are doing to mitigate the impacts of SolarWinds. I would much rather spend time talking about, strategically, the risks we face, and how we are measuring our progress to address those risks. Because at the end of the day, I am a cost center and a risk-reduction function. I am here to enable the system and our caregivers; I can't directly help patients get better with security."

Board Support of Cybersecurity

Zoller has found that the board can best support his efforts when he is successful in tying together the board's concerns related to what they hear in the news media with the risks faced by Providence: "[Publicly reported incidents and Providence's risks] often overlap like a Venn diagram."

Zoller credits significant support for his efforts from the board and CEO and all the way down. "We had to make some unpopular changes during the pandemic," he explained. Changing the way non-employee caregivers authenticate remotely to Providence applications was one example. "The providers were very upset that they had to do this right in the middle of the pandemic. I raised this issue to the CEO and board and asked for their support, showing them the risk, the data that supports what I am saying, and explained why it is so important and why I needed their backing. They aligned with me 100 percent and I can tell you that, as a CISO, it made my job so much easier because ultimately people were upset for a couple of weeks, and then it died off because they got familiarized with the new process. I couldn't have made the change without the board's support."



Lessons about Third-Party Risk

Ensuring security protections when contracting with third-party vendors is a primary risk focus for all three organizations we profiled. Zoller cautions smaller organizations that might have fewer resources and less internal expertise when contracting with third-party vendors. "In my experience working with vendors, a lot of people who sell security products will tell you anything you want to hear just to get through the door, and it's really unfortunate. A lot of security products are sold through fear, uncertainty, and doubt."

Providence relies on a program that assesses vendors on the level of risk posed by that vendor to the organization, including from a cybersecurity capability perspective as well as general security processes and data protections on the vendor's side. They use a third-party security risk questionnaire and commercial tools to determine if a vendor is fit to engage with (see sidebar: Tough Questions for Vendors, for a sample list of questions).

"We ask them questions aligned to industry standard frameworks like NIST [National Institute of Standards and Technology] and ISO [information security management], and when we get those answers we have a general understanding of how they address information security," Zoller said. A vendor's answers guide his response back to them as well as the contract negotiation process. If the vendor doesn't invest in cybersecurity, Providence may make the decision to choose a different vendor for that capability, or go back to the vendor and require that they put in place remediation steps in order for the system to do business with them. For a smaller organization contracting with a larger vendor, it can be a challenge because the larger vendor may simply choose to move on. However, assessing vendors risk and having contractual language enforcing security protections is critical from Zoller's perspective. "In the Target breach, which was very public facing, they weren't only breached because of their own data practices or lack of security execution; they were breached because their HVAC vendor wasn't performing acceptable security on their side. We all could fall victim to the exact same thing."

Zoller says you don't have to start from scratch. "Talk to peers in the industry. Join an organization like Health-ISAC. Talk to people who have done a bunch of business with vendors. Which vendors have a good reputation? Talk to those vendors. Take an unbiased, fact-based approach."

> "If you're on the Internet, you're a target. If you rely on information systems, you will be targeted. No one is immune to this. If you don't know that you are being targeted, you probably have been already. It's what you don't know that can hurt you the most."
>
> *—Adam Zoller, CISO, Providence St. Joseph Health*

A Centralized Effort

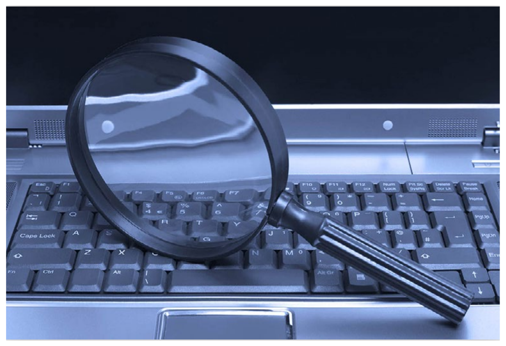
Zoller's team controls cybersecurity for the whole system. By operating on one tool set, it enables the system more standardization, control, and economies of scale:

- Paying for one set of licenses (which are very expensive), along with volume license discounts
- Less time spent on vendor negotiations and signing contracts
- Better infrastructure management and standardization

"There is no real reason to have multiple cybersecurity teams, either regulatory or operationally or otherwise," Zoller said. Providence's IT spectrum is huge, covering analytics, software engineering, genomics research, "and everything in between." They may report up to the broader IT organization, but they are under different executive-level leaders and different missions, with their own sets of infrastructure and goals and objectives. Zoller runs the cybersecurity infrastructure centrally, while empowering those different teams with a standard set of goals, tools, policies, and procedures. "I empower them to use those security tools appropriately in their own environments and give them some level of autonomy to manage their own environments, while checking in and verifying and validating that they are following the rules and policy," explained Zoller. This way, Zoller's team doesn't have to configure software and network devices in every segment, which would be impossible from a time and resource standpoint. But the expectation is that teams are using those standard tools and configuring them to the security standards according to system policies, with Zoller's team verifying that using a series of checks and balances.

Zoller cautions that if security is not centralized, it would be difficult to know how the different functions are managing risks. There may be disparate levels of capabilities and software running with different capabilities to address different risks, which can lead to infinite problems.

Looking Forward



"From a cybersecurity perspective, before the pandemic the threat landscape was pretty scary," Zoller admitted. "Going into the pandemic, threat actors were trying to exploit the fact that a lot of people were working from home with a healthcare security premise built around an on-site model." Providence was already moving towards a cloud-driven, flexible, and scalable model well before the pandemic, and Zoller was already working to build security into the caregiver experience so that it can travel with them no matter where they are in the world. "Whether we have someone in Renton, Seattle, California, India, or Guatemala on one of our mission trips, that security experience should be the same. The level of coverage should be the same," said Zoller. "We need to provide a latency-free, friction-free experience where people can log in remotely and do their work no matter where they are."

The pandemic was hugely disruptive for Providence as it was for so many health systems, but because many of Providence's security initiatives had already taken off—with board, CEO, and CIO support—"we were well-positioned," said Zoller. "We were already using cloud-enabled security technologies and our next-generation remote access solution was well on its way to being pushed out and adopted."

Post-pandemic, Providence is still driving towards cloud-native, cloud-enabled technologies, and security technologies and processes that travel with the caregiver, which aligns with the overall organizational strategic plan, "Health 2.0." The past strategy was acute-care centric and data-center driven. The new strategy, being driven on the IT side by widespread adoption of the Azure cloud platform, is in lockstep with the expectation of continuing expansion of telehealth and in-home services. Going forward, Providence anticipates more threats directly targeted to individual employees.

"At Providence, there will come a point where we decide we can safely bring knowledge workers back. We are already starting to pilot some measures to do that. In practice, how that looks and how that interacts with security will be seamless," said Zoller.

Key Board Takeaways

- Cybersecurity should have its own staff and budget separate from the IT team and budget. (Bob Chaput, author of the accompanying toolbook, recommends that the CISO be a senior executive-level leader who reports to the CRO or better yet, the CEO.)
- Make sure the board has the right amount of information to understand the cybersecurity risk mitigation efforts; where, how, and why resources are being allocated; with supporting data that tell the story in a meaningful way, so that the board can ask probing questions about how the CIO or CISO knows that the necessary steps are being taken to effectively mitigate the risk on behalf of the organization. Push the management team to make it understandable to the board. Don't accept "it's complicated" as an answer.
- It is not feasible to work towards zero risk of a cybersecurity event. It has to be looked at from a standpoint of what level of risk is acceptable and what actions will be taken to mitigate the risk.
- Board and CEO support of CISO and ECRM efforts is critical, especially for unpopular changes that might seem inconvenient or difficult to implement.
- ECRM programs should rely on national standards such as the NIST framework to determine the organization's current and desired level of cybersecurity maturity, and determine what needs to be done to fill the gap between the two to create a roadmap.
- Assess third-party vendors on the level of risk posed by that vendor relationship on your organization, including cybersecurity, general security processes, and data protections on the side of the vendor. Use a third-party security risk questionnaire to determine how seriously the vendor takes information security in general. Talk to peers in the industry who have done business with technology vendors to find out which ones have a good reputation.
- For systems, it is important to centralize the cybersecurity infrastructure and leadership. Benefits include economies of scale, paying for only one set of licenses, fewer vendor relationships to manage, and standardization of security across the enterprise. The centralized cybersecurity infrastructure then enables empowerment of the IT teams to operate autonomously but using a standard set of goals, tools, policies, and procedures, with appropriate checks and balances to verify that those are being followed properly.

Spectrum Health

Spectrum Health has maintained a board-approved investment in cybersecurity for over five years. When the initial program was created, it was focused primarily on standing up the technical infrastructure, processes, and people to manage cybersecurity more aggressively. The CIO and management team provided updates and reports on progress, as well as key industry trends and threats. This really helped get the program off the ground and moving in the right direction.

A few years ago, Jason Joseph, Senior Vice President & Chief Digital & Information Officer, made some adjustments in the structure of the program. "The pace of change in cybersecurity is very high, and we recognized we needed to shift from our primary focus from executing on a program to managing risk. We still execute on a program, but the focus starts with identifying and quantifying risk, and putting things in place that will effectively mitigate those risks." Joseph typically reports to the full board annually on the status of the cybersecurity program. "I have tried to make the conversation understandable and engaging by sharing stories, using an objective way of quantifying cyber risk and maturity, and engaging the board in a dialogue. The board has so much wisdom to share; that really informs our risk tolerance and shapes our investments."

Determining an Appropriate Level of Risk

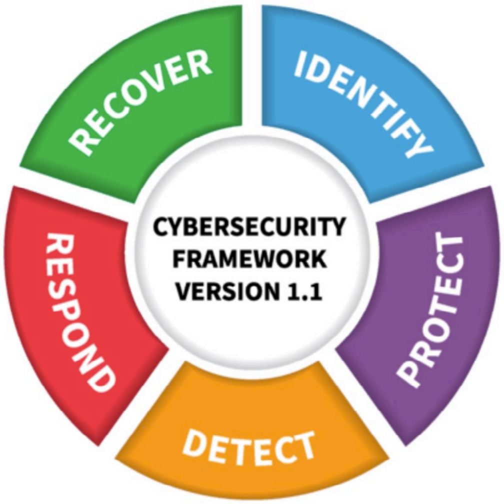
The cyber risk level can never get to zero. "It's really not about if, but when you will have an issue. The question is how big, how bad, and how exposed you will be," said Joseph. The key is creating a common understanding of risk so that this dialogue can occur. "We use the NIST cybersecurity framework (CSF) to guide our program. The NIST CSF model enables us to evaluate our risks, develop strategies to implement mitigations of those risks, and communicate our risk posture to the board. We also use the NIST model to measure the maturity of our cybersecurity program. By using a common model for both our risk assessment and program maturity, we can communicate our risks to the board using more approachable language. This simplifies the discussion about what our risks are, how we are mitigating them, and if our cybersecurity program has an appropriate level of maturity to manage to those risks." Joseph makes a direct connection with this approach to how the system's financial risk scenarios are put together using S&P and Moody's medians.

Spectrum Health is an integrated system of 4,700 physicians and advanced practice providers serving 14 hospitals and 150 ambulatory sites across the State of Michigan, as well as a health plan.

Spectrum Health

Joseph created a roadmap based on their maturity score against the NIST framework, which reflects actions his team is taking to close the gaps and reach their future goals. "For example, as part of our work to mature our capabilities, we needed to improve our ability to detect potentially malicious activity in our environment. In response to that need, we implemented solutions that leverage AI and machine learning to enhance our ability to sift through billions of data points. This helps us to identify indicators of compromise that our teams can focus in on to evaluate and remediate potential threats. This greatly improved our ability to separate the signal from the noise and ultimately reduced our risk," said Joseph.

NIST Cybersecurity Framework at a Glance



Developing Board Understanding

"The hard part is determining risk tolerance in a way that makes sense," Joseph explained. "There is a level of risk that no system of scale should tolerate—and that is achieved with a reasonable level of investment. There are some risks that will likely always be present because the cost of mitigating them is so high relative to their overall potential impact and likelihood of impacting the system. The discussion is really relevant around the 'sweet spot'—the area where additional investment starts to have diminished returns."

Joseph uses a graphic to illustrate this principle and to help guide dialogue around these investments. Joseph strives to give board members objective evidence. "We highlight the most significant risks to the organization and the potential impact of those risks. We show program roadmaps that align the work necessary to mitigate those risks and inform as to progress towards those objectives. We seek third-party objective assessments of our program maturity so the board can have confidence that we are doing the things we need to be doing to protect the organization. The point is not to review each line item on the roadmap, but rather to ensure the management team is in alignment with the board on the overall tolerance for risk and level of investment."

Tough Questions from the Board:

- What level of risk is acceptable to our organization?
- How do we know our risk mitigation activity is targeted at the right areas?

Another early lesson for Joseph was to talk with the board about cybersecurity using a story, not just in terms of metrics. "The first time I presented to the board, I told them the story of a cyber event that happened through the lens of our framework. I walked them through the story, and I showed them how each part of the NIST model applied to how we handled the event, and if we did not have certain things in place, what would have happened. It helped make some of the concepts more real for the board, beyond the specific language of the framework, beyond compliance, beyond descriptors of risk."

Again, Joseph compares board reporting on ECRM to how the CFO might report to the board on financial metrics. "It's a similar approach—how do you know that we are performing at a level that is good enough? Because the CFO showed us the metrics and explained why we are setting our targets the way we are, and why we chose the metrics, and then the board has confidence that we can meet those targets and that they are the right ones. If you take the same approach with cybersecurity, it drives a more robust discussion." Joseph continued, "Establish metrics that define both key performance indicators of the cybersecurity program and key risk indicators to highlight emerging risk concerns. Framing the board discussion in the context of risk reduction leads to the right discussion about how well these risks are being managed."

M&A: A Lesser-Known Area of Risk

Joseph also highlighted the importance of having cybersecurity mitigation strategies in place early as part of any M&A. "It cannot take you three, six, or 12 months anymore. In today's environment, we should expect that on day one of any M&A activity, some basic set of cybersecurity mitigation tactics need to be in place." Joseph recommends having a specific cybersecurity risk assessment conducted to understand what risks exist within the new organization that require remediation. It is often not possible or practical to get everything in place that you would like day one, but you should be able to address some of the most impactful items that reduce risk. For example, if the new organization is not PCI compliant, it may be necessary to address PCI compliance gaps before you connect them to your network to reduce the potential impact to your own PCI compliance program, "…because there is so much at stake," Joseph added.

> "Cybersecurity cannot be an afterthought. It's core to our business—something we have to manage. We need to manage risk more aggressively, conduct more 'what if' scenarios than we used to, and plan for impacts to our organization continuously, including strategy."
>
> *—Jason Joseph, Senior Vice President & Chief Digital & Information Officer, Spectrum Health*

Third-Party Risk at Spectrum

Third-party risk is one of the most challenging risks for an organization to manage. "We rely heavily on third parties for many services, and each one presents a different set of risks to our organization," said Joseph. Mitigating these risks contractually is becoming increasingly challenging, and boards should understand the level of risk exposure present and how organizations are dealing with this exposure.

Like Providence and IU Health, Spectrum Health conducts a risk and security review on each vendor relationship, prior to contracting with the vendor, and then updates it on an annual basis. With the increasing frequency of third-party breaches since the start of the pandemic, it is incumbent upon customers of these vendors to evaluate their contracting processes to ensure appropriate terms are included to address the threats third-party breaches pose to organizations.

Technology and cloud-based vendors are increasingly risk averse and attempt to transfer their risk to customers using contract terms that limit their exposure; for instance, most vendors won't insure customers beyond fees paid without a fight. This exemplifies the need for a strong upfront assessment, specific security provisions outlined in the contract, and regular follow up to make sure the vendor is following its agreed-upon security protocols. "Given how prevalent third-party data breaches have become, cybersecurity programs need to put even more effort into quantifying and mitigating third-party risk," said Joseph. Cybersecurity programs should apply the same principles to this category of risk as they do to other cyber risks, and boards should ensure these risks are part of the discussion.

Spectrum Health's Security Team Structure

At Spectrum Health, the CISO is also Chief Technology Officer (CTO) and reports to Joseph. This role leads the infrastructure and cloud teams as well as security. "We put these teams under one leader because of all of the synergies. Although security and infrastructure are two distinctly different disciplines, there is so much overlap in terms of what needs to be accomplished." The CISO works closely with the ERM and compliance programs. "Our cybersecurity program is closely integrated with our ERM program. It's easy to consider anything related to cyber or data risk to be a cybersecurity issue. But in reality, these are risk issues, and there are actions we take to mitigate those risks via cybersecurity controls and processes."

With that perspective, the ERM and compliance teams can better identify and quantify the risks, making informed decisions about how much of that risk the organization accepts based on risk appetite and tolerance thresholds established by the board. That allows the cybersecurity team to focus on mitigating risks, operating cybersecurity 24/7, and executing so that when a third-party data breach occurs, the cybersecurity team can get engaged immediately.

Spectrum Health Board's Supporting Role

The CISO reports to the compliance committees once per year, or more frequently if requested. The compliance committee is the most engaged with the risk roadmap at the board level. Joseph said the open dialogue, both with the compliance committee and with the full board, is a key to success. "The key is making sure the board understands the current risks, level of maturity, and roadmap. Once that is clear, it paves the way for dialogue that helps ensure the board and management team are aligned," said Joseph.

Joseph feels that the Spectrum Health system board really has a strong grasp of what is important regarding ECRM. They ask hard questions about whether the organization is being efficient and effective in using resources. But, if the CISO identifies a real risk that can be mitigated with an incremental investment, the board is generally very supportive. "It only takes one event to do a lot of damage. Our board is really good at being pragmatic around the spending and wanting to know it's being applied well, while also giving us the resources we need to make sure we are hitting our goals," said Joseph.

Looking Forward

Joseph concurs with Zoller about the state of cyber risk in healthcare post-pandemic. "I do think it is getting worse, unfortunately. A lot of the targeting in healthcare has been to extract money via ransomware. Each organization is doing things to protect itself, but it is never 100 percent or enough. It's more important than ever to have a proactive and diligent approach."

Joseph anticipates the difficulty increasing in the years ahead. As organizations grow and adopt more cloud and digital services, there needs to be even more diligence and focus placed on cybersecurity. "We are really entering a new era, where information is ubiquitous, and cybersecurity needs to be considered in every part of our business," said Joseph. "Even so, it's tempting to move past the fundamentals and get distracted by new technologies. We are always looking for ways to innovate and take advantage of new technologies in our program. A disciplined approach, centered around risk identification and mitigation, helps ensure we are making progress in the most meaningful and impactful ways."

Questions for Boards to Ask the CISO:

- What measures are in place to ensure there is a reasonable and appropriate level of security across the system?
- Are our biggest risks being mitigated appropriately today? If not, what is our plan to mitigate these?
- What should I as a board member be thinking about when it comes to the types of cyber threats our organization faces?
- What are the implications of our Tier 1 incidents?

Boards should focus on developing an understanding of significant risks and where and how to allocate resources for risk mitigation, and less on specific attacks and how those were dealt with.

IU Health

Mitch Parker, CISO at IU Health, reports to the system CIO and also has a dotted line to the legal team and Chief Privacy Officer. The IU Health system board focuses on its long-range strategic plan and how cyber risk fits into that plan. "We have three pillars [for the Informatics and Information Services Team]—digital transformation, high-reliability, and advanced analytics. I'm the co-lead on high-reliability, which encompasses cybersecurity," said Parker.

Parker does not report to the board directly on cybersecurity programs and cyber risk, but he is the author of the written reports the board receives. The CRO presents to the board on the risk management program overall, which includes cyber risk, and the CIO reports to the board on other technology-related issues. Parker uses the NIST framework as a guideline for how he organizes his written board reports, because the board is familiar with the framework and understands how Parker and his team use the framework to guide their programs.

"The number one area my team focuses on is third-party risk," said Parker. "We have a significant third-party risk team aligned with supply chain and system operations." The second area of focus is PCI compliance and change management; number three is the "red team," which conducts threat intelligence, threat research, and offensive security.

IU Health is a regional, 17-hospital system that includes an academic health center and works in partnership with the IU School of Medicine to train physicians, blending breakthrough research and high-quality patient care. It also has the largest network of physicians in the State of Indiana.

Like many others, Parker has seen a significant increase in the need to emphasize cybersecurity industry-wide. For example, IU Health's PCI compliance/HIPAA risk management team also conducts tabletop exercises as a requirement for cyber liability insurance.[2] "The 21st Century CURES Act final rule has made it difficult for us because it requires us to programmatically expose our infrastructure so that patients can download their medical records," added Parker. "Our industry never had to do API security before,[3] but now everyone has to do it. With the SolarWinds example, looking at how your vendors actually function, whether they do security well, and asking them tough questions, is more important than ever. A lot of healthcare organizations don't do this," Parker concurred.

[2] Cybersecurity tabletop exercises examine stakeholders' readiness to respond to and recover from a cybersecurity incident, and include scenario examples of major incidents and their implications.

[3] API security refers to the transfer of data from APIs (application programming interfaces) to your network.

Tough Questions for Vendors:

- If the vendor is handling PHI, do you have a Business Associate Agreement with them?
- Have your vendors certified against a third-party for their security? Do they have a current HITRUST or ISO 27001/27017/27018 certification?
- Do they complete an annual risk assessment and plan?
- Does their hosting have SOC2 certification?
- Do they have a good vulnerability management program?
- Do they have a bug-bounty program?[4]
- Do they conduct source code analysis and testing? (According to Parker, this is a common area where vendors fall short.)
- Do they integrate their authentication with your own enterprise portal or active directory as opposed to standing up their own?
- Do they use good encryption?
- Do they provide written assurance that they keep their software up to date?
- More importantly, do they keep their third-party components that they leverage up to date as well?
- Are you able to secure and lock down the applications?
- If they process credit cards, do they have a current PCI-DSS Attestation of Compliance (AOC)?
- How will you be notified if there is an issue?
- Do they have cyber liability insurance?

Integration with the ERM Team

Parker and his team use the same scoring system to assess and prioritize risks as the ERM team. Further, Parker serves as one of the co-authors of the annual ERM analysis. The teams conduct a one-month exercise every September to analyze all of the organization's risks, including surveying all top executives, scoring the risks, and presenting the top risks to the CRO who then makes the presentation to the board.

"When you see risk scores for your cyber risk that are 10 times what the economic impact is, based on the board-approved risk management methodology, that sends a very strong message to the board," said Parker. "We rank ransomware 10 times higher than a hospital closing, tax impact, and government affairs impact. The board is used to seeing risk scores in the hundreds, but I come in with scores starting at 4,000 and they realize the importance."

[4] A deal in which individuals can receive recognition and compensation for reporting bugs, especially those related to security exploits and vulnerabilities.

COVID Challenges for IU Health

The pandemic forced IU Health to rapidly move 10,000 people out of their offices into working from home. Some employees didn't have broadband. During this time, breached identities were used to file for unemployment, so the system, like numerous other businesses, had to deal with unemployment fraud. Due to the number and severity of threats that have occurred over the past year, "threat intelligence went from something that we did to something that is now front and center with what my team does, and this will continue permanently," said Parker.

> "We had to get very good at this very quickly—and the board needs to know the whole story."
>
> *—Mitch Parker, CISO, IU Health*

Lessons Learned and Looking Forward

Parker recommends that, for any new initiative being put in place, the board must look at how it is being monitored and maintained and to ensure there is a security component. He emphasizes that this should be a focus beyond the typical issues boards focus on such as lowering costs and increasing ROI.

For smaller organizations without the infrastructure or manpower to effectively conduct ECRM, Parker points to third-party managed security services providers. Parker also believes it essential to have strong technology advisory expertise on your board, and in his view, it is appropriate for these board members to be very active in how they ask questions and participate (perhaps more involved than board members might be for other topics). Parker serves on the board of the Children's Museum of Indianapolis and is on its technology advisory committee. He works with the museum's CIO and directly with their cyber team. "I think a lot of boards need to have people like me to help with work like this. The Children's Museum is leading the way compared to other similar organizations because there are three or four of us that sit on this committee and actively work to make sure its cybersecurity products, services, and budget are used to maximize security," explained Parker. "I can't say enough about [the impact of] a good technology advisory committee that knows what it is doing. It's an angle that not a lot of organizations have considered. It's a great way to expand community partnerships as well."

Like Zoller and Joseph, Parker agrees the trend from inpatient to outpatient will continue at IU Health as well, and along with that telework and virtual care. This is making an impact on the organization's future facility plans. For example, the system is planning to build a 625-bed downtown facility to replace two hospitals with a combined bed count of over 1,000 because the capacity for inpatient beds is expected to continue to drop significantly. The system will retain 150–160 beds in relief so that it can pivot quickly for the next surge or pandemic.

Parker's Recommendations to Boards[5]

If the plans presented to your board contain any of the following, they are flags for potential serious security implementation issues:

- Eliminating risk instead of risk mitigation
- Purchasing products instead of developing programs to mitigate risks
- Extensive use of outside consultants as opposed to developing internal resources
- Implementing without resource allocation plans, policy changes, training plans, or communication plans
- Not addressing legacy systems
  Not addressing continual upkeep and maintenance to stay current and certified

Also, beware if the organization is implementing new technology and not considering the following:

- How will it be monitored for performance and effective service levels?
- How will it be monitored for security and exceptions?
- Who will be providing day to day maintenance?
- Who will be conducting the initial security reviews and risk assessments?
- What is the plan for addressing security on a continual basis both at implementation and during operation?

Parker's recommended documents to show the board progress:

- Risk assessment status and completion dates
- Risk management plan, key management items, accountable and assigned team members, completion status, and completion dates
- Risk register open items, progress, and estimated completion dates

Nice to have items for the board report:

- PCI-DSS compliance status and metrics
- Major cybersecurity events
- System compliance status for supported operating systems, applications, and supporting systems
- Vulnerabilities discovered/vulnerabilities addressed
- Third-party vendor security status, including review dates, submitted artifacts, status, and review completion dates
- New and updated systems reviewed, discovered items, and remediation plans
- Security training/communication plan status

[5] From Mitch Parker, "What do Board Members of Smaller Healthcare Organizations Need to Know about Healthcare Information Security?," *Healthcare IT Today,* December 21, 2020.