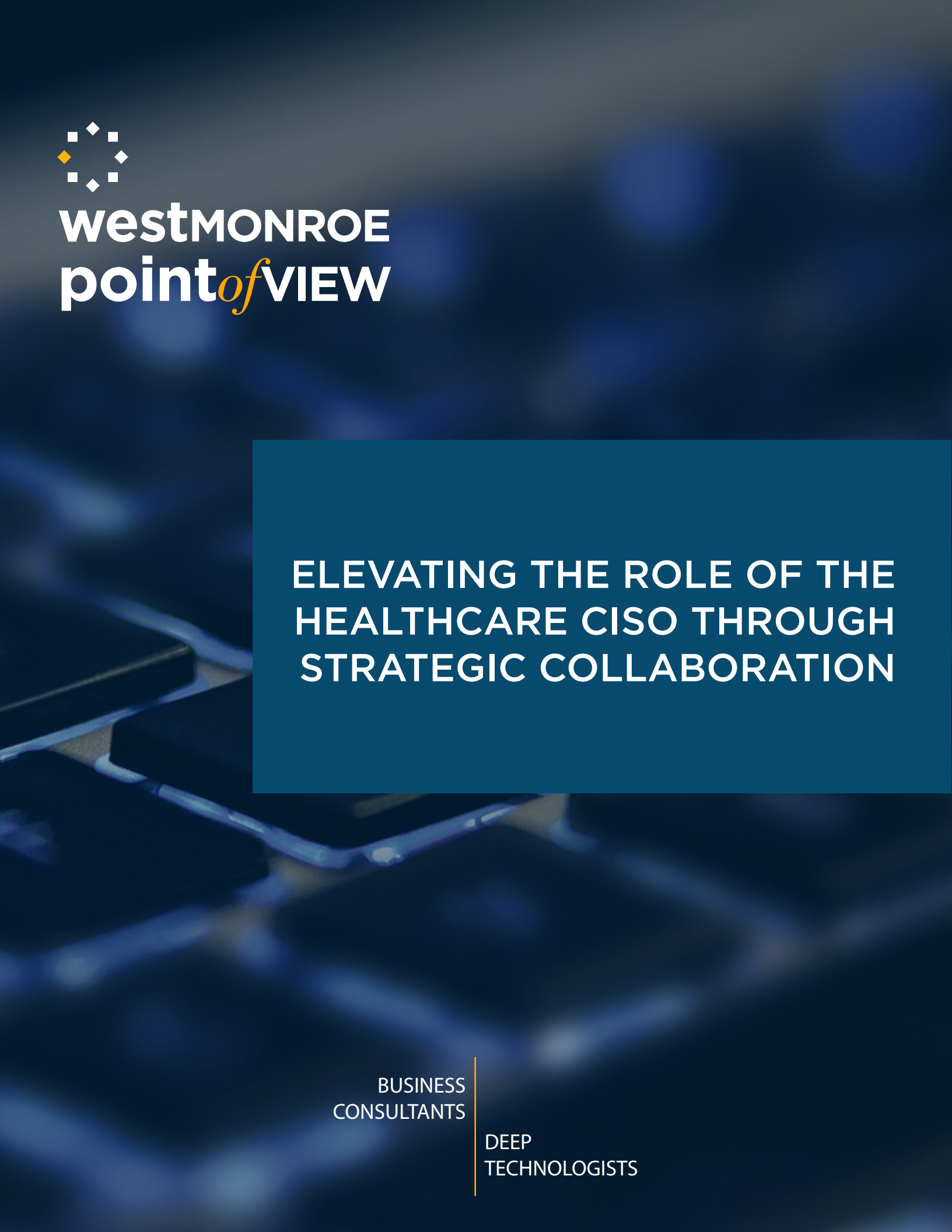

westMONROE

pointofVIEW

ELEVATING THE ROLE OF THE HEALTHCARE CISO THROUGH STRATEGIC COLLABORATION

BUSINESS CONSULTANTS

DEEP TECHNOLOGISTS

Today's healthcare climate presents numerous challenges for chief information security officers (CISOs). According to Forrester's *Global Business Technographics Security Survey*, Healthcare CISOs report they are faced with cost pressures that are constraining their ability to improve security; they will need to be increasingly savvy and efficient in the way they allocate their budgets.

CISOs face an additional challenge in obtaining funding for their security initiatives; they are not always seen as equal partners with other C-level executives. As a result, they often struggle to make their voices heard. CISOs seeking to expand their role into a true executive-level leadership position—one in which they will have more impact and be able to command more support for their programs—will need to initiate, manage, and lead cross-team collaboration.

> *"CISOs seeking to expand their role into a true executive-level leadership position...will need to initiate, manage, and lead cross-team collaboration."*

Historically, the role of the CISO has been primarily a technical one. Despite the "C" in their titles, CISOs are seen as implementers and are often left out of strategic executive discussions. Though the CISO position continues to evolve and edge closer to the C-suite as their responsibilities expand, most are still challenged with bridging the gaps between technology, protection, and business strategy. To bridge those gaps, CISOs need to overcome a few barriers:

BECOMING A PART OF THE **EXECUTIVE-LEVEL** CONVERSATION

TRANSFORMING THE VIEW OF THEIR FUNCTION FROM ONE THAT RESTRICTS INNOVATION TO ONE THAT **ADDS VALUE**

ADDRESSING THE PROBLEM OF APPLYING FUNDING ONLY TO COMPLIANCE INITIATIVES RATHER THAN SPENDING ON **SECURITY ENHANCEMENT** OR **RISK REDUCTION**

GAINING **DIRECT FUNDING** FOR ONGOING SECURITY INITIATIVES

RAISING THEIR ORGANIZATIONAL PROFILE TO ENSURE CISOs ARE **CONSULTED EARLY** ENOUGH IN BUSINESS CHANGE INITIATIVES TO BE ABLE TO PROVIDE VALUABLE AND COMPLEMENTARY TECHNICAL SOLUTIONS

In order to position themselves not just as security experts, but as strategic business partners to the C-suite and the board, CISOs will need to initiate collaboration with all C-level executives and build alliances that will ultimately drive their funding and strategic goals.

Putting a Spotlight on Security

Healthcare CISOs have long faced a dilemma when implementing projects that involve the handling of sensitive customer data such as protected health information (PHI) or personally identifiable information (PII). Their IT security teams have historically had much smaller budgets than those in any other industry, and they only influence IT decisions. How, then, can they command funding for projects that also include protection of customer data throughout the organization and appropriate compliance with the standards that regulate that data?

More often than not, we see three groups heavily involved with sensitive customer information: the customer experience team, which is responsible for the interface between the company and its customers; the data analytics team, which takes customer information and turns it into business insights; and the security team, which is tasked with ensuring that customer information is adequately protected.

Each of these teams within a healthcare organization requires funding to realize its strategic imperatives, and as a result, may find itself competing with the other teams for (often limited) financial resources. This dilemma places everyone at a disadvantage, particularly the security team, which is all too frequently viewed only as a cost center.

A second problem arises once groups do receive funding: they tend to pursue projects in isolation, with the customer experience team or the data analytics team forging ahead, often addressing security as an afterthought. At the same time, security professionals, with their laser-focus on building a moat around PHI and PII, create roadmaps of their own—with functionality and usability as secondary considerations. This siloed approach by each team can invariably lead to cost overruns, drained resources, missed deadlines, and unhappy customers, not to mention increased risk exposure.

> *"A siloed approach [to issues that cross from the business into technology] by each team can invariably lead to cost overruns, drained resources, missed deadlines, and unhappy customers, not to mention increased risk exposure."*

In the last 12 months, West Monroe Partners has assisted a growing number of healthcare clients transform their customer experience to meet changing consumer expectations regarding interactions with their healthcare providers and insurers. Additionally, our team is being increasingly challenged by our clients' data analytics teams to provide them with the tools necessary to extract greater insights from their data - insights that will help them not only reduce costs, but also deliver better services and ultimately enhance the customer experience. Lastly, we are frequently asked by our clients' security teams to help reduce the risks associated with the potential exposure of their data.

We assisted one healthcare client in particular to avoid this siloed approach by fostering collaboration between their teams and combining common goals and shared objectives. The solution not only created an enhanced customer experience, it also generated rich data-driven customer and business insights while reducing the total security risk exposure. This result was achieved by demonstrating to each member of the C-suite that their shared objectives were mutually beneficial. What was unanticipated by our client is that we guided their security team to spearhead this effort. The results spoke for themselves, but the realization within the client's business groups was that early and ongoing engagement of the security team not only reduced friction as the project went live, it also opened up avenues to deliver each team's objectives.

Finding Common Ground: Start with the Data

The following is a closer look at the three groups we identified in the organization involved:

- **Customer Experience (CX):** The group was charged with improving the customer experience through enhanced patient portals and mobile applications, as well as improving customer relationship management (CRM). This team viewed data as a way to get to know the customer better.
- **Data Analytics:** The data analytics team was engaged by the business to aggregate and analyze data in order to provide insights to support more informed decision making. Their biggest concern was having access to as much raw data as possible to allow them to identify patterns and different ways to present those patterns.
- **Security:** The growing proliferation of customer data was a key concern for senior executives, so the security team sought to find ways to keep sensitive customer information safe, ensuring that only authorized individuals had access. The security team was also responsible for complying with all regulations that govern PII and PHI.

The goals of these groups both conflicted and overlapped. For example, building controls around data can reduce the risk of data exposure in the event of a breach. However, it can also make life very difficult for authorized users, including customers. In addition, it can prevent the data analytics team from deriving value from the information the organization has collected.

Despite these conflicts, each team's project overlapped in interesting ways:

- **Locating the data:** Data resides in many different places within an organization. It also takes a variety of forms, such as transactional, financial, or PHI. The customer experience and data analytics teams needed to know where the information pertinent to their particular objectives resided, and the security team also needed to familiarize themselves with data sources to determine how to protect it. Furthermore, they all wanted assurance that the data did not reside in more than one location. Multiple sources for the same information increases the risk that one of those sources is inaccurate as well as unnecessarily exposed. Therefore, having a "single source of truth" is critical. Likewise, having a single place to house data is important to the security team, because it reduces the extent of the assets they need to protect.
- **Determining who owns the data:** All three teams needed to understand who was accountable for ensuring the accuracy, completeness, consistency, and accessibility of data. When it is unclear who is accountable, it is impossible to know where the single source of truth is at any given moment.
- **Understanding the value of the data:** Each team defined data value in a different way, depending on how they used it. For example, the customer experience team placed the greatest value on information that allowed them to better understand how customers

used the website or mobile app—for instance, number of visits per year scheduled through the site or number of calls for online help. The data analytics team valued data that provided them insights into business decisions such as margins for certain services. Finally, the security team sought to understand what data might be governed by regulatory or industry security requirements and the minimum access required. When each team failed to recognize the value the other teams placed on various data elements, it became difficult for each to achieve their objective cost effectively. By working together, data can be better protected, richer to support reporting, and more accurate to provide better customer connections.

For each of these three teams, their project roadmaps began with data discovery. To support our recommendation that the teams combine efforts to avoid duplication of activities, we identified significant budget savings for each project that could be used to enact additional functionality.

Getting Funding: Mastering the Art of Packaging

If the CISO of the healthcare organization can persuade the customer experience and data analytics leaders to acknowledge that getting their projects approved and resourced is not a zero sum game, they will realize they have a better value proposition if they approach budget decision makers together. Not surprisingly, this is also an effective "pitch" to whoever is holding the purse strings.

In the aforementioned client example, the CISO was in a position to both initiate and own collaboration across the three different teams. The CISO had visibility into each of the business initiatives through the project approval process, allowing the security team to identify the synergies between each project's plans. If the CISO can bundle all of these projects together as one and approach the executive team with the promise to deliver a solution faster, more securely, and with fewer tools and resources, that project has a higher probability of being funded than each project individually. Furthermore, the success of one joint effort creates a virtuous cycle: when leadership sees the risk reduction that can result from collaboration, the next effort will be a much easier sell.

Every organization has its hot buttons, depending on the competitive environment, recent events, or even leadership priorities. When budget time rolls around, these teams can improve their odds of receiving funding when they demonstrate that they will address those issues first. In this way, the hot-button issue can serve as a "wrapper" for other asks. For example, if driving an improved customer experience is what resonates with management and the board, then the team needs to lead with that. At the same time, by including "while reducing the risk of customer data exposure," as part of the project's objectives, they can underscore the dual purpose and win support for both efforts.

Alternatively, if the organization has recently suffered a breach or has been slapped with a fine for non-compliance, the team should stress the

security plans while pitching the business benefits. This helps keep the business on board as the organization focuses on risk reduction.

Delivering Value by Joining Forces

When the customer experience, data analytics, and security teams work together to create business-applicable solutions that are also secure, invariably they will find that such solutions are worth more than the sum of their parts. In order for this to happen, teams need to understand each other's perspectives and priorities, and where the actions of one team will impact the other—in other words, not treating security as a bolt-on and not treating business needs as an inconvenience.

Ultimately, if the CISO masterminds this collaborative partnership, they can establish themself as a trusted C-suite player and savvy business operator. Collaboration across customer experience, data analytics, and security teams leads to project roadmaps and initiatives that are not only cheaper and faster to implement, they are also of higher value to all those involved.

For more information about this Point of View, please contact:

Sean Curran
Senior Director, Security & Infrastructure

Sean is a director in West Monroe Partners' Security and Infrastructure practice, based in Chicago. He has more than 20 years of business consulting large-scale infrastructure experience across a range of industries and IT domains, including extensive work in the areas of data and information security. He has experience designing secure environments, helping clients adhere to industry and government compliance frameworks including PCI DSS, HIPAA, and ISO 27000.

scurran@westmonroepartners.com

Will Hinde
Managing Director, Healthcare

Will is a senior director with West Monroe Partners and leader of the firm's Healthcare practice. He has more than 20 years of experience partnering with a wide variety of healthcare organizations to create business value via strategic business and technology solutions. He has experience across multiple disciplines including healthcare policy and reform, mergers and acquisitions, customer experience, business and IT strategy and execution, operational assessment and improvement, and systems integration and consolidation.

whinde@westmonroepartners.com

westMONROE

BUSINESS CONSULTANTS | DEEP TECHNOLOGISTS