McKinsey Digital

Protecting the business: Views from the CIO's and CISO's offices

At JPMorgan Chase, CISOs and CIOs work together to align cybersecurity with business goals.

March 2020

In an increasingly digital era, protecting information and systems from cyberattack is one of the most important and challenging responsibilities of every IT organization. In some cases, business-unit chief information officers (CIOs) and enterprise chief information security officers (CISOs) can have very different perspectives and agendas, creating friction and reducing organizational effectiveness.

At JPMorgan Chase & Co., which has one of the world's largest private-sector technology environments, two of the four business-unit CIOs have previously served as the bank's enterprise CISO.

McKinsey's James Kaplan spoke with several members of JPMorgan Chase's Global Technology leadership team, led by Lori Beer, Global CIO and member of the company's Operating Committee, about effective collaboration between the security and business-unit technology functions, what makes a good CISO, and how being a CISO can be valuable preparation for being a CIO.

Rohan Amin is CIO of Consumer & Community Banking, Anish Bhimani is CIO of Commercial Banking, George Sherman is CIO of Global Technology Infrastructure, and Jason Witty is JPMorgan Chase's global CISO. All are managing directors. Prior to their current roles, both Amin and Bhimani served as JPMorgan Chase's global CISO.[1]

The attributes of an effective CISO

Jason Witty: Being a successful CISO these days involves wearing many hats, from business to risk to technology to software engineer. You must be aware of the threat landscape and understand human behavior. You also have to know how to work with regulators and gain trust from multiple stakeholders.

Doing those things gives you a firmwide view of what's going on in the business, what's going on in technology, what's going on in risk, and what's going on in the legal and regulatory landscape. This allows you to connect the dots in a way that other roles simply do not provide.

You must constantly be shifting, adapting, and learning. I spend about two hours every morning just digesting what's changed since I went to bed, be it new threats, bad actors, or vulnerabilities. Then you need to translate this into digestible content for a non-technical audience, which requires good soft skills as well.

A CISO drives and controls an agenda, and building trust is critical in implementing that agenda, because trust is a force multiplier. As a CISO, my priorities are to protect the firm, enable the firm to drive growth, and make this growth as seamless as possible from a security standpoint.

George Sherman: I think the best CISOs are the ones who have learned about policy and controls but at their core are very strong technologists. The CISO role must evolve with the threat landscape and technologies. You must understand the technical side of cybersecurity. But information security and protecting against cyberthreats are also about people and process, not just technology, so you have to understand all three dimensions in order to fully appreciate what you have to do to protect the firm.

Sometimes you have to go slow to go fast. It's the old race-car analogy. You can go really fast in a race car because you're wearing a fireproof suit, you're in a protective cage, you have an automatic fire-extinguishing system, and you were trained. This allows you to drive superfast.

[1] For the full interviews with each interviewee, see "The benefits of a CISO background to a business-unit CIO" (Rohan Amin), "Enterprise-wide security is both a technology and business issue" (Anish Bhimani), "Robust cybersecurity requires much more than great technology" (George Sherman), and "The modern CISO: Managing scale, building trust, and enabling the business" (Jason Witty), March 2020, McKinsey.com.

But getting to that point can feel slow. CISOs who "get it" spend a little bit more time up front being thoughtful about their execution.

The changing role of the CISO

Jason Witty: The role of the CISO has already changed. It's about measured risk taking, not risk elimination. This measured risk taking must also evolve with the availability of new technologies. You must constantly adapt, train, and educate so that you can adjust the control environment to enable the things the business is trying to accomplish.

Rohan Amin: If you want to help the builders, you have to know how to build. As a CISO, if you are not close to the modernization agenda—modern architectures, cloud, data, machine learning, and so on—then it's hard to effectively guide an organization in the right direction.

George Sherman: You can go back a decade and see how much has changed. Everything seemed much simpler. The successful CISOs of the future can't be process managers. They must have a deep understanding of technology. Imagine leading thousands of software engineers but never having actually written a line of code. At some point, you have to ask yourself how you can relate to that community. And how will that community relate to you? Those questions are just as relevant to today's and tomorrow's CISOs.

Anish Bhimani: I used to go to the board of directors and the audit committee annually for about 20 minutes. We now meet with the board eight times a year for at least an hour each time.

The value of CISO experience to CIOs

Anish Bhimani: Every CIO should spend time in a security role, since it makes you think differently. Regardless of your role, you're never out of security. With new technologies, including automation, security is a layered process. It's built into the fabric of the organization, from process to people.

Rohan Amin: When we think about what matters most to our customers, running a disciplined environment with stability, resiliency, controls, and data privacy are non-negotiables. Being in the CISO role obviously instilled a lot of that in me.

The other aspect that's helpful in having a CISO background is a deep understanding of non-functional requirements and how to make them easier to adopt. For example, modernizing our applications and striving for platform-centric thinking help to focus our engineers on the most relevant business functions, which are the features and value for customers.

As a CISO, you have a global view of risk and what the issues are and how you think about enterprise management in the application-development context. Some CISOs are policy and governance focused only, while others have a stronger technical and business background. Having a technical background and being able to effectively communicate complex issues to the business have served me well.

George Sherman: We are unique and fortunate in that three of our CIOs are former CISOs. This makes the current CISO's life much easier, specifically as it relates to how you design, deliver, and execute the business-process automation efforts. Thanks to our security background, we tend to think about data protection and security earlier in our processes and require that security and controls be embedded into all the technology we deliver.

I use my technical-security skills on a daily basis. With new technology and connectivity platforms, many of our older security paradigms are being stressed. In the past, you could get away with not having the most robust identity or authorization constructs and authentication and authorization metrics. This is no longer the case, as the dynamic nature of these modern technologies requires dynamic management of the trust chain.

If you add to this the complexity of the multivendor cloud environments connecting into our companies, you must have a strong understanding of the "threatscape" and how you deal with cybersecurity issues. Everyone within the organization must

understand that cybersecurity is non-negotiable. *We* have to get it right all the time. The bad actors only have to get it right once.

How being CISO helped in becoming a CIO

Anish Bhimani: I spent my entire career aspiring to be the CISO of a large bank, and when I got the job, it was a significant accomplishment in my career. When I then became a CIO, it meant shifting to more of an implementation approach, and I was eager to work with the business. But despite my excitement, I was clear that job number one is having a secure operating environment. If you don't do job one, you don't earn the right to do job two, which is to deliver value to the business.

Rohan Amin: In the CIO role, you get a deep appreciation for the importance of the control environment and security. You learn that everyone understands the importance of controls but wants control adoption to be more seamless and part of the engineering process.

Security and controls teams face a continuing challenge to figure out how to make this stuff simple and easy to use. This requires the engineering work to make it easy to adopt, easy to innovate on the platform, and easy for engineers to do the right thing. People can't be forced to read thousands of pages of policy to figure out the right thing to do. The right thing to do should be easy and baked into the platforms and enabled via software, so that something as simple as "you should encrypt your data" isn't something every engineering team has to figure out for itself. Make security the easy answer, not the hard answer.

The impact of the cloud

Anish Bhimani: When moving to the cloud, the first priority is figuring out your technology and business priorities and then striking a balance. Services and architecture templates need to be validated and automated for cloud configuration. Secondly, cloud security can be a business enabler, and we know that businesses need to grow and thus must move fast.

Why do you have brakes on a car? It's not to stop. It's so you can go fast, secure in the knowledge that you can stop whenever you want or need to. Security done right enables businesses to go at the speed they want while being able to manage risk appropriately.

George Sherman: Technology is going to become more segmented but also more hyperconnected. You can see that in the evolution of the private, public, and hybrid cloud and with a combination of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service providers clamoring to support new growth. But with this hyperconnectivity comes hypercomplexity, and with that comes fragility. Fragility leads to reliability and security issues. The enemy of a good security program is complexity. If we're not careful in our execution, CISOs could end up with a "least common denominator" problem where their environments are only as secure as their weakest controls.

Cybersecurity advice for newcomers

Rohan Amin: Spend time with the folks in the business who have to use the stuff you're creating. If your objective is to help the business—which is what it should be—then you need to spend time in the business to understand what it takes to deliver something to a customer. If you spend time only in security land, you really don't understand the complexities the builders go through to deliver. Knowing what I know now, building simplicity into security-control adoption is where I'd recommend they focus.

Anish Bhimani: My first advice is that life never moves in a straight line. You need to be able to adapt to constantly changing circumstances. Well-roundedness is critical, and everything you do should get you a step closer to your goals. Rotations are valuable in gaining experience in security and infrastructure.

Focusing on the future

Jason Witty: "Deepfakes" are a concern, so having the ability to prove that who you are talking to is actually the person you think you are talking to is vital. Artificial-intelligence (AI) and natural-language-processing algorithms are also advancing rapidly, posing new reputational and financial threats in addition to opening new doors for business growth.

Safely enabling AI and maintaining our ability to keep up with the velocity of automated attacks is also something being much discussed. We'll continue to modernize software engineering around the cloud to ensure security and resiliency and to further unlock its business value. Finally, we're looking into crypto-agility and decoupling the encryption process from the software-development process.

Rohan Amin: Authentication is often the first experience a consumer has with an organization, so we're working on the authentication strategy of the future. Previously, authentication was thought about as a channel-specific thing, meaning how do we authenticate you in the branch? How do we authenticate you when you call in? How do we authenticate you online or on mobile?

We're working to bring these experiences together in a secure and more integrated manner. We're thinking about ways of putting the customers at the front of the design and about the multichannel ways people interact with us differently than in the past.

George Sherman: Resiliency, availability, and security are everyone's responsibility, regardless of whether you're involved with infrastructure, applications, or both. Everyone must believe that operational risk and information security are core requirements of their role, so you need to invest in training and move this to the forefront of your team's minds, or you will end up with yet another remediation program.

Secure by design is critical. You can build systems that are reliable and available, but they may not necessarily be secure. But when you build secure systems, you often end up with ones that are both reliable and available. The disciplines around security tend to lend themselves to the same disciplines as resiliency and availability or operational efficiency and effectiveness.

James Kaplan is a partner in McKinsey's New York office.