McKinsey
Digital

The modern CISO: Managing scale, building trust, and enabling the business

The modern CISO is uniquely positioned to bridge gaps across technology, processes, automation, and cybersecurity.

March 2020

Securing the information of a multibillion-dollar enterprise with more than a quarter of a million employees is a daily Herculean labor. Enterprise chief information security officers (CISOs) must manage myriad cybersecurity threats, automation, regulatory compliance, and ever-evolving technologies. Jason Witty, global CISO, JPMorgan Chase, discusses his role and these challenges with McKinsey's James Kaplan.

This interview is part of a series of interviews on the evolving relationship between the CISO and CIO. (See "Protecting the business: Views from the CIO's and CISO's offices," on McKinsey.com.)

James Kaplan: How do you define the role of a CISO?

Jason Witty: 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.

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 nontechnical audience, which requires good soft skills as well.

James Kaplan: How do you manage the complexity of an institution the size of JPMorgan Chase?

Jason Witty: You manage scale. You build trust. You have command of the details without getting bogged down. You also have to have very strong leaders under you that you can trust. I am fortunate to have a fantastic team.

James Kaplan: How are you addressing security concerns amid increasing automation and continuous controls monitoring?

Jason Witty: We put a lot of effort around controls as code, or policies as code, ensuring the ubiquity of modern software engineering practices across the firm. All of our applications are in the process of being rearchitected to support a modern software environment, with automated, self-evidencing controls built in.

We have hundreds of engineers on the security side dedicated to automation, such as by making controls seamless and integrating security tools within the product, platform, and service pipeline.

It's all about data and code now. This ensures strong integration and collaboration with the businesses as well. Security is thought of as a part of each technology capability or product rollout, which is a tremendous advance compared to a decade ago, when security was viewed as a hindrance.

James Kaplan: In years past, security was fragmented. How have the organizational structure and lines of responsibility evolved?

Jason Witty: DevOps has significantly changed the way that IT in general thinks about product management, application development, and production support. Site reliability engineering (SRE) is a big focus, along with our product journey. It's a change in traditional telemetry management from years ago, when it was very fragmented and siloed. Our software environment provides transparency, which enables people to respond quickly to issues.

We're simultaneously integrating core functions with SRE, as well as modernizing the environment. This means more colocation and cocreation, which spur both product and security innovation. We're completely aligned on the customer and client experience.

James Kaplan: How are new technologies like cloud impacting the institution?

Jason Witty: Today's modern software environment is faster from a business-capability standpoint. You have more incremental change and faster release cycles; you can also know earlier when something goes wrong, which means you can respond faster.

James Kaplan: There's often an overlap between infrastructure and security engineering. How have you addressed this collaboration?

Jason Witty: The product model supersedes departmental silos. When you have multiple teams working on the same set of issues, it completely transcends organizational boundaries. If everyone involved understands the end objectives and how they are measured, then they're all pointing the needle in the same direction. It's a combination of site reliability engineering and product that makes the process more seamless.

James Kaplan: As the product model becomes more pervasive, how does the role of the CISO change over time?

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.

James Kaplan: Talk about the collaboration around regulatory compliance.

Jason Witty: We take compliance very seriously. We are constantly mapping and cross-mapping international regulations to our control environment and legal obligations. We're always looking for better ways of automating that process. We're adopting the Bank Policy Institute's Financial Services Sector Cybersecurity Profile as our framework of frameworks in 2020 and encouraging regulators to start auditing against the profile, which has the potential to be an industry-wide game changer.

James Kaplan: Are you experiencing the talent or skills gap that we hear about in the cybersecurity space?

Jason Witty: Yes. We have myriad ways we try to address that. We have programs specifically focused on bringing in non-computer-science talent, who we put through coding boot camps and upskill. We also have a Cyber Kids school program that goes into schools and provides basic skills training on internet safety and security. We hope to help spur interest in STEM-related activities and careers. We also recruit talent from the military and affinity groups to attract the best talent available. We were a founding sponsor of the Financial Services Information Sharing and Analysis Center's (FS-ISAC's) scholarship program for female university students looking to pursue a career in cybersecurity. Recruiting the right people is critical, but retaining them is also important, hence our emphasis on upskilling, training, and continuing education.

James Kaplan: If you look down the road for the next three or four years, what keeps you up at night?

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.

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