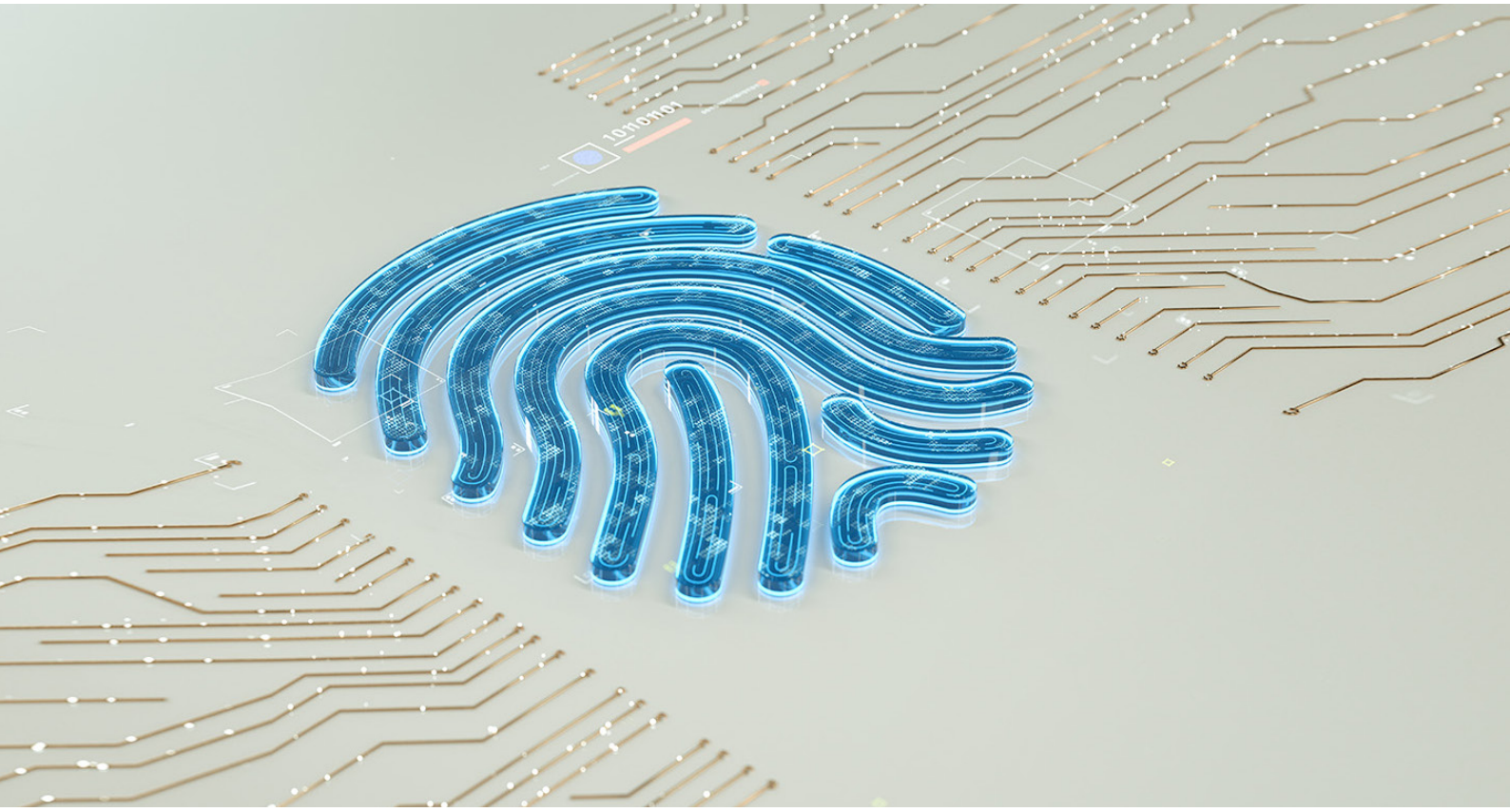
McKinsey & Company

Cybersecurity Practice

Building a cybersecurity culture from within: An interview with MongoDB

MongoDB's security champions program leadership team discusses how cybersecurity training can create a company-wide culture that prioritizes security and encourages employees to get involved.



October 2022

Transforming the cybersecurity culture underpins successful security program implementation. Building and integrating security throughout an organization is accelerated when all employees understand why security matters and how it adds value to the business. Further, equipping high-risk teams with security expertise, training, and development allows companies to place talent in areas where the business needs value protection the most.

In line with recent McKinsey research, understanding best-practice programs provides insight for other organizations on what levers to implement and how to shift their culture to viewing cyber as an enabler rather than a control. This interview provides one example of how a company implemented a broader cyber-awareness program that has led to a rapid expansion of frontline cyber knowledge and addressed critical internal security gaps.

During this time of ever-evolving cybersecurity threats, the developer data platform company MongoDB developed a security champions program to help ensure its employees are making security a top priority.

McKinsey recently hosted cybersecurity leaders from MongoDB for a virtual conversation about taking an everyday, every-employee approach to securing their organization. McKinsey's James Kaplan and Charlie Lewis interviewed MongoDB's Lena Smart, chief information security officer; Amy Berman, director of security engineering; and Felix Chen, cybersecurity education and advocacy senior analyst. The following is an edited version of their conversation.

McKinsey: What is MongoDB's security champions program?

Lena Smart: This is a program we rebooted in February 2021 during the pandemic. We saw the desire and need from various parts of our organization to raise security awareness. We wanted to create a positive security culture. There are now more than 100 security champions within the program from 45 different global locations.

We have hosted more than 20 events, bringing these people together to work on different things, such as capture the flag and scenario planning, as well as team-building activities, including watching movies and TV shows about hackers, technology, and cybersecurity. Our security champions program has been very successful, and it continues to grow. We believe it encompasses all our cultural values as well.

Felix Chen: To add to Lena's comments, we also have a diverse group within our program, from the most experienced cybersecurity professionals to novices. Participants come to our events prepared and ready to learn and participate. For example, we may have password-cracking sessions on rainbow tables for more advanced members, while a security playbook discussion might be more suited to intermediate levels.

Amy Berman: Our program's diversity in background, beyond experience, ensures a broad range of ideas, innovation, and engagement.

McKinsey: To what extent is your security champions program focused on engineers and other technical personnel versus non-engineers?

Lena Smart: We have tried to make it as open as possible to anyone in the company, from executive assistants to programming and development engineers. We have employees with no cybersecurity experience at all, which makes up about 10 percent, as well as people who would describe themselves as experts, which makes up about 20 percent. And the rest is in between. We've found that there is a

lot of collaboration among all different levels of expertise. This is creating a culture with security at the forefront. The champions are basically the voices of their team for security.

We continue to develop activities to grow the program, including competitions, for example, to win tickets to cybersecurity conferences and events such as DEF CON [hacking conference].

Our goal is to have 10 percent of our employees be part of the security champions program, but ultimately, everyone is a security champion, responsible for security at the company. But our program participants have just taken it one step further and vowed to give us a certain amount of their time each week. They are valuing what they get from the program, and they help us grow the program at the same time.

We are also using the program from a feeder or training approach—we have seven participants who have now moved into the security and compliance teams. This is great during a time when it is quite difficult to find skilled talent.

McKinsey: As it relates to employee retention, what is the selection process for the program, and how do you train participants to be first responders?

Lena Smart: This is a voluntary program, but occasionally I will approach someone and say, "Hey, you've come to me with a great idea for security; are you part of our security champions program?"

Amy Berman: When we redesigned the program, we looked at motivation theory and adult-learning theory and asked, "How do we really make this a long-term, sustainable program and continue the interest across multiple different angles?" Each quarter we have a formal meeting for insights and feedback for continuous program improvements. We make changes to keep the program fresh and relevant in an effort to address ever-evolving cyberthreats.

McKinsey: What is the time commitment for program participants?

Felix Chen: It varies by interest level, but generally it is a couple of hours per week. Participants are basically the initial data testers for certain security-related tools. In addition to our feedback loop, we maintain dedicated channels of communication where program participants can disclose potential vulnerabilities within their teams.

There is no one-size-fits-all approach to onboarding or training. We do these in various locations and on various topics; it is designed to encourage behaviors of pointing out security flaws or vulnerabilities and also providing feedback to the security team.

McKinsey: How did you get leadership buy-in for your security champions program?

Lena Smart: We had weekly e-staff meetings with our executive management team. We outlined the program mission and how it aligns with our company's mission and values. We discussed adding this to people performance and growth. The following week, our CEO introduced the program during an all-hands meeting, and shortly after, we were accepting program volunteers. We also developed a playbook we share with external stakeholders for program development and implementation.

McKinsey: Are there people you think are especially effective security champions?

Amy Berman: Each participant has unique insights, and each sees a potential vulnerability in a different light. You hear a lot from the technical side, but I think some of the nontechnical side has been extremely helpful in contributing to messaging, positioning on new policies, and so on.

Lena Smart: I think people sometimes forget that an executive assistant [EA] has access to everything his or her boss has access to. So if I'm a hacker, I'm going after an executive assistant. We make sure that we give them specialized training as EAs, but we also encourage them to be part of the security champions program, so we're covering them through individual training, group training as

EAs, or overall training as security champions. And they enjoy that; it's something different from their everyday work. Just being part of the security champions program gives them visibility into a world that they're not part of, generally, and it's really helping.

McKinsey: How does MongoDB manage people risk as it relates to cybersecurity?

Felix Chen: Human risk is a very big vulnerability for companies—and usually the starting point for cyber vulnerability. It's a matter of figuring out the most effective way of influencing behavioral change.

Amy Berman: Team members can apply their experiences and test out and reimagine what cybersecurity looks like and how it fits with our culture. It's a matter of looking at different perspectives and then coming together and thinking about culture changes and organization changes.

McKinsey: How do you measure success?

Felix Chen: We test the success of different measures and determine where to make adjustments. We look at trends over time—for example, in our phishing simulation campaigns, we look at how many people clicked on a phishing link. We look at event attendance and reported vulnerabilities. And, importantly, we communicate our progress with leadership.

McKinsey: What are some lessons learned with your security champions program?

Lena Smart: Buy-in is critical. People need to be able to manage their teams, and if they're acting as security professionals when they're not security professionals, that's not good. Making this voluntary, fun, and collaborative is important.

McKinsey: What advice would you give to other companies contemplating this type of program?

Lena Smart: My top four things would be to get buy-in from the top, ensure ongoing communication and progress reporting—we do so with regular "tailgate" meetings—develop a playbook to set procedures and processes, and demonstrate the value of the program company-wide.

McKinsey: Where would you like to see the program a year from now?

Lena Smart: We would like to double membership and give more employees the opportunity to learn about cybersecurity. Again, we've had instances in which a non-security-centric employee has joined our program and it sparked further interest and professional development in cybersecurity, opening up new job opportunities within MongoDB.

Amy Berman: One other thing that's important is the respect we have with the champions. You have to create an environment where they feel comfortable to come to us and that we are open to the feedback they provide. It's important that there's a level of respect, not just from us running the program but also from the entire information security team to the champions.

Felix Chen: What is also important is the correlation between involvement and adoption. If program and participant input and feedback drive adoption of the tool, that is a big advantage. We ask them for a simple input. Even if it's something that we don't go with, the fact that we are asking creates a sense of inclusion and contribution.

Amy Berman is the director of security engineering at MongoDB, where **Felix Chen** is a cybersecurity education and advocacy senior analyst and **Lena Smart** is the chief information security officer. **James Kaplan** is a partner in McKinsey's New York office, and **Charlie Lewis** is an associate partner in the Stamford office.

Comments and opinions expressed by interviewees are their own and do not represent or reflect the opinions, policies, or positions of McKinsey & Company or have its endorsement.