PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID FAIRMAN
CISO, ROYAL BANK OF CANADA

HEADQUARTERS: Toronto, Canada

EMPLOYEES: 85,000+

ANNUAL REVENUE: $35.2 Billion

"We do have regular updates with our board; our goal is to give them a level of comfort that we're covering our bases and that we're measuring and managing that risk for them. It's about keeping them current so that they are able to support and challenge us."

- DAVID FAIRMAN

MAKING A MARK ON RBC'S CYBER SECURITY PROGRAM

Into his role as Chief Information Security Officer at the Royal Bank of Canada for three years, David Fairman had the opportunity to come in and build a business-focused cyber security strategy. He states, "It was an opportunity for me to take a global role at a large financial institution and really build that program ground up."

Fairman exemplifies a concise business-enabler and confident leader, who came into the organization with a strong priority of gaining deeper engagement with business leaders. He explains, "It's about understanding and having more dialogue, better relationships, more insight into what our business partners are trying to do and how they're thinking in terms of how they're operating. Understanding how we can be proactive by helping them achieve their goals, so they want to move into a new market and want to launch a new product. Then we're fully armed to support them."

THE FOUR PILLARS OF FAIRMAN'S STRATEGIC PLAN

After gaining clear alignment with executives and acquiring a solid understanding of the corporate mission and goals, Fairman put into place his strategic plan. His strategy consists of four pillars:

Cross-function operating model. Coming into the organization, Fairman knew it was not just a technology problem he needed to address, it was much broader and presented a clear business issue impacting processes and services. Multiple parties within the organization had to come to the table to recognize the role they play across the entire security program. Fairman comments, "You need to help them understand the impact their team has to the overall, bigger picture of protecting the bank."

Strategic partnerships. The first focus for Fairman rests on large vendor strategic partnerships who help the organization build cyber security capabilities. These vendors are leveraged to implement capabilities to protect customers, shareholders and employees. The second element is understanding the startup community and becoming an early adopter in key technologies to help drive their roadmap and maturity. The third part is partnerships with academia in terms of exploring research projects that may help solve emerging security challenges. The fourth is strong ties with law enforcement and intelligence agencies.

Talent and culture. Fairman strongly supports his team, comprised of positive, energized people who understand the core value resting on customer trust. He continually develops and matures this culture, and his team, by enabling a fast-paced, exciting and leading edge cyber security program.

World class cyber security capabilities. Fairman built the program around the NIST cyber security framework with an emphasis on aligning to the five pillars of identify, protect, detect, respond and recover. In regard to understanding the maturity of the program, he says, "We need to understand where we want to grow or end, and what our endpoint looks like. I'm very passionate about the API economy and providing services for our business partners and internal teams, so they can move and be as agile as they need to be, without us holding them back. We need to give them a solution."

BOARD ROOM AND BUDGET ENABLEMENT

Throughout his tenure at the Royal Bank of Canada, Fairman developed a two-way dialogue during board meetings, and empowered board members to recognize security as a true enabler. Presentations consist of a threat landscape overview, top risks affecting the bank, progress with strategic goals and the current status of key metrics.

"We do have regular updates with our board; our goal is to give them a level of comfort that we're covering our bases and that we're measuring and managing that risk for them. It's about keeping them current so that they are able to support and challenge us," explains Fairman.

When it comes to budget, Fairman advises other CISOs to make a clear case for explaining the impact in a business context. He encourages CISOs to talk about critical business processes or the critical assets at risk, and the revenue generation or criticality of the process that might be at risk. For board and executives, this approach provides a real-world case – it's meaningful.

"I think it's really beneficial to have that open conversation, which certainly helps define the budget needed in order to be successful," comments Fairman.

PHASING INTO FUTURE GROWTH

Currently in phase two of his three to five year cyber security strategy, Fairman designates a clear priority on continuing to mature his four pillars and build world class cyber security capabilities to protect the bank.

Clearing the Security Product Clutter

"You clear clutter through understanding where the industry is seeing trends. You need to understand the ecosystem and see what other large organizations are doing. Once you see a few other organizations down the path of a particular capability or solution choice, that probably says something in itself. Secondly, we have multiple innovation and accelerator labs that we leverage to test specific use cases. We have innovation labs in Orlando, New York, Toronto, San Francisco, and we are now starting to delve into Israel."