ADITYA MALHOTRA

CISO
NESS DIGITAL ENGINEERING

HEADQUARTERS: Teaneck, New Jersey

EMPLOYEES: 3,500+

REVENUE: Private

Aditya Malhotra has dedicated most of his career to information security, working in several leadership roles at enterprises such as Point72 Asset Management and Bloomberg LP. Most notably, Aditya has developed information security teams and built programs from the ground-up, aligned with the firm's business objectives, thereby charting himself as an innovative leader. Currently, he is the CISO at Ness Digital Engineering, a full lifecycle digital transformation firm offering digital advisory through scaled engineering services based out of New Jersey.

Aditya joined the organization four months ago after learning about its vision for growth, emphasis on culture, and overall business model. He saw the opportunity as a way for him to make a meaningful, tangible impact to the organization by bridging the gap between technology, business, and organizational needs. With over 15 years of experience across various facets of information security, Aditya shares his thoughts on the evolving role of CISO responsibilities and advice for leaders in similar functions.

ENGAGING WITH THE BOARD AND EXECUTIVES

Aditya believes security leaders should have direct visibility and involvement with the board to provide insights into key risks and granular visibility of the inherent versus residual risk portfolio across the entire enterprise. He says, "Security leadership has a birds' eye view on the enterprise threat landscape. They have the foremost ability to convey risk and potential impact to the organization in a language board members will understand and be receptive to."

Aditya encourages CISOs to be armed with quantitative metrics and key data points when presenting to boards. He explains, "Metrics help us understand the key areas of risks that the firm is facing today, and which of those risks require action based on criticality and priority. Managing those risks often requires investment in technology and getting additional resources, whether it's external, internal, or contingent workers. So, we are uniquely positioned to provide stakeholders visibility on the intricate nuances of enterprise risks and mechanisms to mitigate some of the major identified gaps. And that's why it is pertinent for security leaders to have a seat at the board level."

Aditya recommends explaining intricate technical nuances in simplistic terms through visual representations such as charts, graphs, or heat maps so the audience can easily ingest the material and then make an informed decision. He sees value in demonstrating different types of metrics for various stakeholders. He says, "For example, the technology leadership and the CIO function should get a different level of visibility and granularity compared to the board. Talking specifically about the board, for example, if I'm looking at our perimeter protection, the leaders would be interested in learning the different types of threats (spear phishing, malware, ransomware attacks) that are being prevented but more so interested in the ones that are circumventing our existing controls."

He continues, "An example of leveraging metrics would be when discussing a Single Sign On (SSO) solution. We cannot expect end-users to remember credentials for tens and hundreds of applications they have access to daily. Eventually, users will end up reusing the same credentials across multiple applications or storing the credentials insecurely, posing a risk for the enterprise. By implementing an SSO solution, I eliminate the need for the end-user to remember credentials for each application. In addition, when

an end-user is terminated, we disconnect one credential and not concerned about the myriad of applications the end-user has access to. These granular metrics demarcate actual data for mitigating risk and building a cohesive risk management culture across the firm. Talking about metrics, it is vital to convey the message in simple terms and give executives business-centric examples that they can understand, connect, and relate to. I feel this is the best way for leadership to grasp the content and get their support on key initiatives."

Aditya says that once you have identified the gaps, made a case for the investment, received budget approval, and implemented the solution, you need to demonstrate cyber security program maturity based on quantitative metrics that are hard to refute. According to him, risk management is a continuous process. Monitoring the current state and demarcating progress towards a future desired state in quantitative terms bridges the challenges we have experienced with rationalizing budget allocations based on qualitative metrics over the years.

BUDGET JUSTIFICATION FOR HIRING

When it comes to adding additional headcount, Aditya says it comes down to prioritizing the initiatives based on business objectives and defining a timeline to complete them. He explains, "Since I've joined, I've identified several initiatives that would assist towards building and maturing the cyber security and risk management program. Obviously, some of them are process enhancements that are easier to accomplish by bringing leaders across the enterprise together. However, others, such as maturing an Identity and Access Management (IAM) function, require dedicated personnel. Making a business case of why we need to mature an IAM program is easy. However, a tricky proposition is when you talk about why you would want to build the skillset in-house for certain programs where others can be outsourced. The decision to build the function internally versus getting support from external vendors should be adjudged based on the execution priority of the initiatives and the time to value. As I'm working towards expanding my team, my pragmatic rationale is driven by initiatives that directly correlate with business operations and their timely execution. And for that, you need resources."

Aditya adds that seeking buy-in from the CFO, CEO, and board is vital for the initiatives to succeed. When he is pitching a business case for specific initiatives, he discusses the technology or toolset investments required and resources needed to ensure the solution does not remain a standalone product but is embedded in the firm's DNA across the entire technology and business verticals. This would require building the business and technical skills in-house and ensuring the program matures over time to support and augment business operations.

He comments, "I'm a big advocate of hiring/working with people across departments who are self-driven, motivated and have a hunger to learn this ever-expanding cyber security space. This means there could be resources and advocates in other departments and functions whom I can collaborate with while working towards initiatives that demonstrate tangible progress and improvement towards risk management."

RESPONSIBILITIES AND GOALS

Aditya is responsible for cybersecurity, data protection and overall risk management across the enterprise and has identified short, medium, and long-term goals. These include implementing a comprehensive security awareness training program with phishing simulation exercises for all employees. He comments, "The main goal is to define a baseline of the risk landscape when it comes to security awareness for employees by imparting phishing simulation exercises. This will help us identify users and departments that need further proactive training to detect and thwart sophisticated threats such as spear phishing."

He is progressing towards onboarding a scalable cloud solution and provides multi-language capabilities for employees across the globe. He continues, "I'm also enhancing the vulnerability threat management program for the firm, which will involve a structured process of identifying vulnerabilities, classifying them, and proactively mitigating risks by adding compensating controls in addition to timely patching and threat remediation."

Building a Governance, Risk & Compliance (GRC) program is also a top priority to manage the multitude of third-party vendors and clients. By structuring that process, Aditya and his team will provide additional layers of visibility. The governance function manages various components of information security such as policies, procedures, standards, insider threat detection, response, third party vendor risk management and mapping of controls to established frameworks. Building a robust information security program requires support from leaders across the enterprise. As each initiative is immersed in the firm's culture, slowly and steadily, you realize a positive cultural shift towards proactive risk management. He says, "Risk management is driven by firm's risk tolerance and reducing risk to an acceptable level."

Lastly, since the organization has a significant presence in Europe, Asia and North America, a large part of his responsibility is reviewing data protection, privacy directives with legal for onboarding new clients. Like many CISOs who are now responsible for data privacy concerns, Aditya continually works towards GDPR alignment. He says this is vital to confidently tell customers their data is safe and secured if an incident does occur.

Aditya says his initiatives towards building a mature cyber security program requires constant reinforcement of foundational cyber security best practices. He explains, "The most important piece for any organization is to know what assets we have. With the growing advent of cloud applications and infrastructure, answering this basic question can be quite challenging. Understanding where all our assets are, data and how to prioritize the protection of data based on asset, data criticality and classification is key. These basic tenets should be embedded in the firm's culture, which will assist in building a proactive risk management function."

Aditya says he is driven to empower and uplift his team and continuously focuses on identifying ways to enhance the team's development and unlock their true potential. He prefers to hire people with a strong affinity for problem-solving and critical thinking. He adds, "As long as I can find a rough diamond who is eager to learn and ready to face new unknown challenges each day, I can polish them over time to carve out their true potential."

Personally, Aditya believes in continuous learning and holds a Master of Science in Information Security from Carnegie Mellon University. In addition, he has several cyber security and ethical hacking certifications. He often leverages his professional network to brainstorm upcoming cyber security challenges.