AGENDA

Opinion

How the Board Can Get Involved With the Cyber-Security Program and CISOs

By Virginia Gambale December 14, 2020

Virginia Gambale
Virginia Gambale is a board member at Jetblue and Nutanix and founding member of AttackIQ Informed Defenders Council.

The board usually does not have an understanding of security operations unless the organization has been breached or a vulnerability is discovered. As board members, we're invested in the company's success and have helped the business grow. A key part of the organization's being successful includes a strong security program that protects customers.

CISOs must be transparent, informing leadership and board members on the balancing act of keeping the company secure on a tight budget. A recent meeting I attended with the AttackIQ Informed Defenders Council discussed these challenges and solutions for building better engagement between CISOs and the board when it comes to cyber security. Below are a few considerations for board members to be better engaged and involved with the CISO and security operations.

Build a relationship and ask questions

Building a relationship with your CISO allows you and your fellow board members to become better informed, as well as align priorities for the company. Whether in-person or virtual, one-on-one meetings show that you're interested in learning more about the security program. Furthermore, this time allows you to ask any questions.

Between new threats, technology advancements and cyber-crime groups, it is hard to keep up with the latest trends. These conversations offer the opportunity to better understand the landscape, hostile attackers and how the security team can defend themselves effectively. For instance, a security framework known as Mitre ATT&CK is a well-known resource to CISOs and security leaders but may be unfamiliar to the rest of the C-suite and board. Ask the CISO to describe the framework in an easily digestible way and how the company is leveraging it, if applicable. No question is a bad question, and it shows that you're interested in learning more.

Know how the security operations work

You and your fellow board members should have an understanding of the cyber-security program. If the organization suffers a breach, it can lead to financial loss or reputation damage, among other severe consequences. Ask the CISO to share security incidents competitors were victims of. The CISO should analyze what went wrong, how this impacted the company and what can be done to avoid a similar fate.

With budgets shifting due to the economic outcome of a global pandemic, it is important to also discuss with the CISO if the technology in place can protect the organization. Unfortunately, cyber attacks are up by 92% and the average data breach now costs $3.86 million. If consumers' data is exposed, companies also face fines under GDPR or CCPA which may add additional fees in the hundreds of millions to pay the costs of reparations and litigations. As resources are limited, advise the CISO to use a security optimization platform that shows where the company may be overinvesting, and what is actually working.

Ensure everyone is aligned

Leadership and board members should be aligned on all priorities, including cyber security. To keep everyone updated, ask the CISO to provide resources and reports showing how well security operations are running, or changes that must occur. This should include articles to read before an upcoming meeting discussing new vulnerabilities or threats to the company, quarterly reports describing progress made and plans for the security program.

Furthermore, a weekly e-mail update on where the company stands security-wise can be beneficial so the board is aware of potential gaps or attacks that were stopped as the landscape is constantly evolving and threat actors quickly adapt their form of attack.

As board members, we often are thinking of the business's outcome and de-prioritize security. Cyber security enables and ensures the business's uninterrupted functioning and allows it to take advantage of new innovative technologies to better serve customers. Whether security is not a priority because it's intimidating or our plate is full, there needs to be a shift. Building a rapport with the CISO and having a thorough understanding of the organization's security program ensures the company is set up for success.