Speaking to the Board of Directors About Security

Today's threat landscape has caused the paths of the Board of Directors and the CISO to intersect on a more frequent basis. Regulatory environments, FCC pressure and best practices have all impacted the Board of Directors, increasing their involvement in security and risk. Additionally, board members have seen what has happened when a company experiences a breach, when security was not a priority, and how these breaches have led to significantly damaging legal, financial and reputation consequences to the organization. This has led to many Board of Directors delving into cyber security risk and taking a more proactive stance.

A recent SANS webinar with Carol Mills of WhiteHat Security's Board of Directors, vAmour's CISO Demetrios Lazarikos (Laz) and John Pescatore of SANS, dove deep into the increasingly important topic of speaking to the Board of Directors about security. The transcription of the webinar is what inspired this Q&A whitepaper.

Q: Why should a CISO want to talk to the Board of Directors?

Having CISO's presence with the Board of Directors will give the Board the visibility they need to provide support to a successful Information Security program. They need to understand what is at risk for their organization quantified in dollars, and need to be informed on what is happening in the environment that the CISO is working in.

Q: What could it mean if the Board of Directors is not talking to the CISO?

If a CISO is not being asked to present in front of the Board of Directors, it is likely that one of two possible things is happening. The first scenario is that the Board of Directors are getting their information some other way, possibly from an external expert or someone who is less informed about the security infrastructure and ongoings of the organization. This could mean the proper information is not being conveyed, and the Board of Directors has the wrong perception regarding the organization's Information Security program and current risk levels. The second possible explanation is that the maturity of the Board of Directors, and the maturity of the organization's InfoSec program, hasn't evolved to the point where security is in their line of sight. This could lead to a lack of support for the organization's InfoSec program, lack of awareness of the organization's risk posture and lack of proper measures being taken to ensure security.

If a CISO has not been placed on the agenda for the Board of Directors, then the Board is lacking in their duties. If the CISO isn't the person presenting and answering questions relative to security and risk, then who is? If the CISO is not part of developing what is being presented to the Board, things can get lost in translation.

Q: Who usually gets the Board of Directors talking about security?

The General Council typically informs the Board of Directors on developments in best practices, regulatory environment and on-going Board of Directors structure. If the Board does not already have a risk committee, the General Council would likely be the person advising that security be added to the agenda. Additionally, as part of the financial and fiscal responsibilities of the Board of Directors, there are likely private sessions between the CFO and the different audit committees of the Board to discuss internal audits and processes.

Q: How can the CISO get the Board of Directors to start speaking about security?

The CISO should suggest that an internal security audit of the organization could provide the Board with an understanding of where the organization is in the maturity model from an Information Security standpoint. Additionally, the results can be incorporated into the recurring presentation to the Board of Directors, establishing security as a regular topic. The caveat here, as a CISO, would be to prepare to address questions regarding security events and performance if there is an increase in attacks or if performance is poor.

The key thing not to do to get the Board of Directors speaking about security is to go directly to the Board. Going around the General Council, CEO or CFO can damage the relationship and lead to lack of confidence in the CISO.

Q: What should the CISO know before presenting to the Board of Directors?

Before presenting security to the Board of Directors, a CISO needs to understand the way risk is already being presented to the Board. Former Board decks or audit forms regarding risk from the General Council will provide guidance and direction. These reports should be used to comprise a framework about cyber risk, similar to the way the Board has seen other types of risk presented. Once you have established a successful framework when presenting to the Board, do not continue to change it. Maintain a similar framework as you continue to meet.

The CISO needs to develop an understanding of what is driving the business, how the organization makes money and how the organization operationalizes and supports their existing or new clients. With that information, the CISO should be able to put Information Security into terms that the Board of Directors can relate to and be familiar with.

Q: What else should the CISO take into consideration when presenting to the Board of Directors?

Boards of Directors often think about spend, along with many other factors, as it relates to industry norms and how the competition is performing. The CISO should leverage the interest in benchmarking and present how the organization is performing as it relates to the industry, if the organization is behind the curve, if they are spending more or less than their peers and if the organization is more vulnerable.

Q: What should be discussed and what information can influence the Board of Directors?

Members of the Board are intelligent and experienced in finance, business and strategy. These roles rarely include experience in cybersecurity and it is very likely that they do not have the background to understand the technical nature of Information Security. As a result, the discussion should not be a technical one; it should be a discussion about risk, loss and reducing loss exposure, expressed in business terms. Everything needs to be translated from the security perspective to what is happening at the Board level in terms they are familiar with without overwhelming them with technical terminology or appearing condescending.

What should be presented to the Board of Directors is how the actions of the security team enable business initiatives and how they tie into the goals of the company. These presentations should demonstrate that these efforts could result in increased revenue, profit, market share, market penetration, and increased efficiency, similar to how other divisions in the business and the operations side of the organization would present to the Board.

This discussion should include warnings of upcoming changes, threats and financial results if risk levels continue to rise, provide recommendations on actions required to avoid information loss, and demonstrate what is being done to prevent attacks or deal with attacks more quickly and efficiently. Information regarding what percent of the business is secure, if the data hosted is strongly protected (i.e. encryption, authentication, servers, networks, operating tools and applications, etc.) and what percent of the people and suppliers have been reviewed for security will demonstrate the value that the Information Security team provides to the organization.

Additionally, the CISO Should prepare a dashboard of the major critical issues, minor issues, related loss exposure to those issues, what is being done today and over the next *n* months to address and resolve those issues, and what it would take financially to resolve them. These details, along with metrics demonstrating the strength of the Information Security program, the number of attacks the site is experiencing and the frequency of those events, will provide the Board of Directors a quantifiable measure of the performance of the Information Security program and actionable suggestions to support and improve the program.

When speaking to the Board of Directors, it is essential to tie lower level technical security details together for a high level abstraction and translate them to be more meaningful.

Q: What should the CISO's goal be in presenting to the Board of Directors?

The goal in presenting security to the Board is to drive change that will increase the effectiveness of what is being done to reduce risk, to get their backing and to help them realize the strategic importance of security. A CISO should aim to say, "We are maintaining the same level of protection, keeping risk at a constant level while using less resources," or, "With risk increasing and with the increase in resources we've been given, we have been able to reduce risk to a tolerable level."

The end result of this conversation is not necessarily to increase budget, but to gain support that would prevent impact to the business. This should be explained in terms of risk and expense calculations. This needs to cause the Board to consider what and how much they are willing to lose.

WhiteHat SECURITY®