ISMG INFORMATION SECURITY MEDIA GROUP

BITSIGHT

THE DO'S AND DON'TS OF REPORTING TO THE BOARD

BitSight's Jacob Olcott: Focus on the Right Topics & Metrics

Interacting With the Board

TOM FIELD: Increasingly, CISOs are being asked to address their Boards of Directors. Where do you see them often steering wrong?

JACOB OLCOTT: There are a few mistakes that CISOs make when they're doing their Board-level presentations. The biggest one is probably that they're too focused on treating cybersecurity as an IT problem and focusing too much on talking about our firewalls and our intrusion detection systems and not focused enough on putting this into broader risk management terms. I think that's probably the most critical thing.

But a few other mistakes that are commonly made are: not providing Boards with measurements, ongoing metrics for how are we doing and how are we performing over time; not telling a story about the challenges that we as an organization are facing and putting that into language the Board will understand and then use metrics to back that up; and not focusing on the financial impact of this risk.

Again, thinking of this only as an IT problem is missing the broader picture, that financial or operational impact – talking about actual dollars and cents here.

Then the last thing I would say is CISOs really make a mistake by not engaging with the Board members themselves. Too many CISOs are trying to own cyber risk themselves. This really should be a collaborative issue. You want to get the Board on your side; you want the Board to be doing some of the thinking for you – to help you set the strategy and then have you also execute on it. So really engaging Boards in more of a collaborative conversation is crucial for a CISO's success.

The Right Cyber Topics

FIELD: Let's break this down into a number of areas. I want to start with this: What are the right cyber topics that CISOs need to be bringing to their Boards?

OLCOTT: It's a combination of storytelling and also measurements and metrics and performance-based measurements. We think that CISOs should really take the opportunity to catch up their Boards on some of the more noteworthy issues that really rise to the senior executive levels – some of the noteworthy breaches that may have occurred over the previous quarter and what their relationship to the business might be.

Certainly there has been a significant amount of new regulatory requirements that have come out, so CISOs should abe prepared to

have a conversation with their Boards about the general regulatory environment and also some specifics that might affect their particular businesses.

Then, from a metrics or measurements perspective, some of the topics that CISOs should specifically be talking about would include progress that we're making; the measurements that we're incorporating. Are we improving our performance? What goals do we have? Are we meeting those goals? Are we working towards those goals? Peer benchmarking has obviously become really important – understanding how our performance looks compared to some peers or competitors in our sector.

Then, the third issue on the performance and metrics topic is this whole idea about vendor and third-party risk. It's become so big from a regulatory perspective, but this is also an area that is a new and emerging cyber risk issue that CISOs should also be bringing to their Boards because of the impact that it can have on the business.

CISO As a Storyteller

FIELD: Talk to me now about how CISOs should be communicating these topics.

OLCOTT: The best CISOs are really great storytellers. They're able to talk about this issue in a way that businessmen and businesswomen really understand. That is one of the really crucial issues. Think of this as a story that you need to communicate to a senior executive.

The way that we tell the story is evolving and changing, too. CISOs should … really emphasize the visuals, leveraging charts or graphs to be able to show some of those measurements and metrics that we were talking about. Don't use the Excel spreadsheet version of this; really take some time to invest in the presentation. … If it's a Board-level conversation or Board-level presentation, there's obviously a lot on the agenda, so distill the essence of what you're trying to communicate in one or two pages. …

The Audience

FIELD: Talk to me now about who the CISO is speaking to.

OLCOTT: Well, the reason why folks are appointed to Boards is because they're fairly sophisticated business people. It's conventional wisdom that Boards don't understand cybersecurity or … cyber risk. But that's probably the wrong way for a CISO to think about their audience. The CISOs should think about their audience as being very sophisticated and understanding business and business risk. When I say business

risk, I mean really thinking about some of the operational and financial risks that an organization faces.

So if we think that this is probably the typical background for a Board member, we want to be able to communicate our issue in their terms … that they understand. What we know also is there are so many reports and articles that have come out that Boards are increasingly interested in trying to understand and manage this issue. … CISOs should think that their audience is going to treat cyber as a stand-alone risk, but also as a risk that could impact some of these financial and operational risks that they're used to managing. Let's treat these folks as being very sophisticated consumers. So we really have to step up our game in order to communicate with them.

Third-Party Risk Management

FIELD: Let's consider the new SEC guidance, which emphasizes third-party risk management. What and how should CISOs be communicating to the Board about third-party risk management as it relates to these regulations?

OLCOTT: Let me start with the SEC guidance, which is a great issue for CISOs to be discussing with their Boards. Ultimately what the SEC guidance is asking businesses to do is to communicate material cyber risks and incidents to their investors - material meaning a significant risk that would have a financial impact on the business. This is the exact lens the CISOs should be thinking about when managing … internal cyber risk and then reporting it up to the Board. So this is a really good topic for CISOs to be bringing to the Boards.

To your point, though, those regulation requirements do mention this idea of third-party risk management, which has obviously become critical for so many organizations. There have been so many breaches or incidents that involve third-party contractors or vendors or business associates. So what a CISO should really be focusing on in communicating this risk to the Board is, first of all, what is our third-party strategy? How do we identify who our critical third parties are? What is our diligence process to understand or evaluate their cyber risk? And then how do we continuously monitor those third parties during the lifetime of our relationship?

We're seeing that a lot of CISOs are also not only just describing their program, but they're able to use metrics to communicate either improved risk management or deteriorating risk management over time. So how are my third parties performing today? We can start to measure and manage that. And then how has this changed or

evolved over time? Those are the really crucial issues that CISOs need to be communicating to the Board.

BitSight's Role

FIELD: Jacob, one final question for you. I want to bring it back to BitSight. What are you doing to help your customers ensure that when they're talking to the Board it's a productive conversation?

OLCOTT: Well, it gets back to this issue about being able to tell a story, to leverage high-quality data, and to do that in a visually compelling way. So what BitSight is doing from a security ratings perspective is to provide insight for CISOs to communicate their own security posture, compare themselves to their peers or competitors and the sector as a whole, and then also to help CISOs communicate the security posture of their third parties in their business ecosystem up to the Board.

Being able to have quantitative, objective measurements is crucial for today's CISO, and we're happy to be able to provide that data to many of the Fortune 1,000 CISOs and beyond.