CyberEdBoard Talks

Reporting Business Risk to the Board of Directors

Former RSA CEO and Chairman of the Board Art Coviello on Best Practices for CISOs Presenting to the Board

CyberEdBoard Talks Excerpt
Access the full interview by becoming a member.
Visit cyberedboard.io to submit your application.

CyberEdBoard

Art Coviello
Former RSA CEO and Chairman of the Board

Coviello has more than 30 years of strategic, operating and financial management experience at high-technology companies and is one of the most recognized figures within the cybersecurity industry. He became CEO of RSA Security Inc. in 2000 and continued to lead the company following its acquisition by EMC in 2006 until he retired as executive chairman in 2015. He has played a leading role in several national cybersecurity initiatives, including as a founding board member of the Cyber Security Industry Alliance, and has served as an adviser to key government agencies as well as public-private initiatives. He is currently a partner at Rally Ventures.

The CyberEdBoard Talks series is designed to address the most critical challenges executive members are discussing in the private global ecosystem and is presented by respected industry experts and chief cybersecurity practitioners.

One of the unique benefits of CyberEdBoard is that you must be a member to access this session and all other content and engagement opportunities. “The global community continues to grow at a pace that reconfirms the critical importance of cybersecurity collaboration and executive information sharing, and we are thrilled to support each member’s unique needs within the private ecosystem,” said CyberEdBoard Executive Director Chris Ancharski.

The first edition of the CyberEdBoard Talks series was held on Dec. 12, 2020, exclusively for CyberEdBoard CISO members, who came from nine countries, including the U.S., Brazil, the U.K., India, Malaysia, Canada, Egypt, Bangladesh and New Zealand, and represented industries including healthcare, financial services, information technology, retail, aerospace, education and many others.

Tom Field of ISMG hosted the interactive fireside chat, in which Art Coviello, former RSA CEO, spoke about best practices for chief information security officers when reporting business risk to the board of directors.

In this excerpt of the CyberEdBoard Talk, Coviello discusses:

- Business risk in the digital age;
- Forces influencing the future of cybersecurity;
- Best practices for presenting to the board.

Solving Communication Problems

FIELD: What have CISOs told you about presenting to the board?

COVIELLO: Board members are just not equipped to understand technology. The other side of the problem is that CISOs tend to talk in technical terms and it goes right over the board's head. We have to figure out ways for CISOs to communicate effectively to the board. They can, but the burden, in large part, is going to be on them.

Technology Timeline

FIELD: Since the COVID-19 pandemic hit, CISOs have gained stature for enabling resiliency and security. Has the dynamic between the CISO and the board changed?

COVIELLO: It's started to. Every company has cyber at the top of its business risks, for obvious reasons. But members of the board of directors don't understand how much technology has washed over us in the last 20 years. They ask CISOs, "Why can't you guys stay ahead of the hackers?" Well, we could if technology systems remained static, but they don't. They're dynamic.

In the year 2000, we were still using AOL Instant Messenger. In 2007, the iPhone was introduced and it changed the game in terms of this onslaught of mobility that we witnessed from then on.

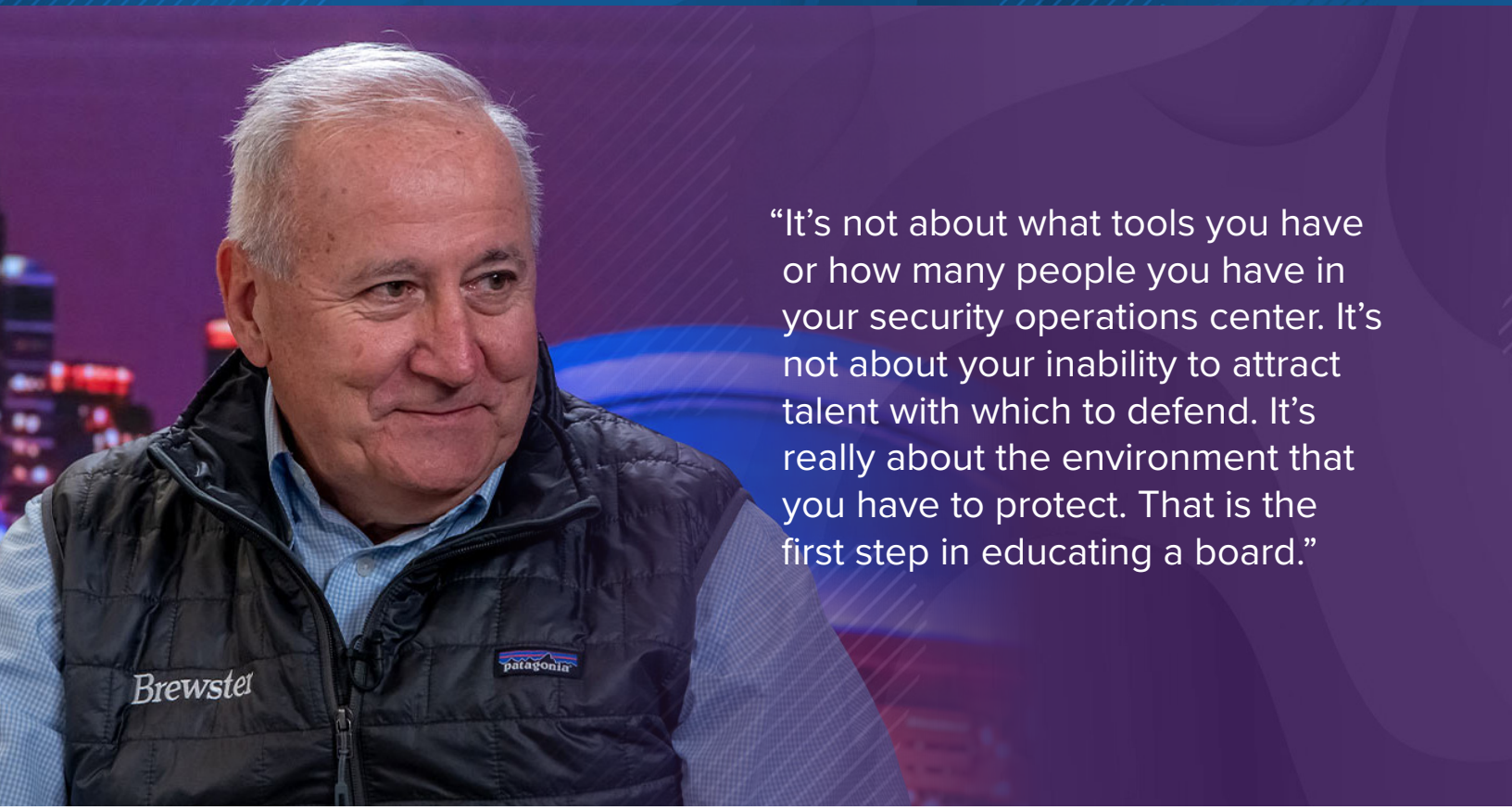
Around 2004, we saw criminal groups start to develop. By 2007, they were in full force. The more applications we were doing online, the more we were exposed and the more criminals were able to take advantage.

Fast forward to 2014. The attacks got more serious. We've always had issues with foreign governments wanting to intrude, but we started to see foreign businesses and nations attack individual companies. Within a couple months of the end of 2014, North Korea attacked Sony. The attacks were at a point where they could become truly destructive. The perimeter had started to dissolve, as workload started to shift more and more to the cloud.

Fast forward to today, and we have apps almost writing themselves. We see 5G being introduced. The speed is incredible. It's a matter of time before a terrorist gets their hands on these tools and creates havoc. Even social media has been weaponized.

How many of your boards understand this timeline and the problem it presents in terms of expansion of the attack surface and what you have to defend? Not many. So, it's not about what tools you have or how many people you have in your security operations center. It's not about your inability to attract talent with which to defend. It's really the environment that you have to protect. That is the first step in educating a board as to why this problem is so severe.

"Board members are just not equipped to understand technology. The other side of the problem is that CISOs tend to talk in technical terms, and it goes right over the board's head."



"It's not about what tools you have or how many people you have in your security operations center. It's not about your inability to attract talent with which to defend. It's really about the environment that you have to protect. That is the first step in educating a board."

Defining Business Risk

FIELD: What do business leaders need to know today about the impact of digital transformation on their security business risk?

COVIELLO: What are the risks to your assets? What is the risk to your operations? What is the risk to your good name? What is the risk to your revenue attainment?

These risks are still the same in the digital world, but the way the risk manifests itself is different. And for you to be able to defend yourself, obviously, the tried-and-true people, process and technology are critical. But what you need to protect and how is what you need to communicate to your board.

As you explain to your board how you manage risk, you need to explain how you protect your people. You could bring in strong user authentication. You could bring in identity management, how you provide access to only the right people, how you do privileged access management. These are concepts that boards can understand.

How you protect data is important. The specifics about how you protect the critical information to your business and how data is used in applications and across your infrastructure need to be articulated to the board. How are those applications protected so that the data can't somehow be corrupted or changed?

Whether you're availing your customers, your partners or third-party contractors to all of your data applications and infrastructure, it poses a risk. You have to explain to the board how you account for that risk and what capabilities you employ.

The Future of Cybersecurity

FIELD: In 2021, we're going to be dealing with a pandemic for a good half of the year, at least. We're likely to see continued market consolidation, mergers and acquisitions. How should these forces influence the message that we convey to our boards about the year ahead?

COVIELLO: There's no doubt work from home is going to continue unabated. It's going to be a permanent change. Not that we won't go back to our offices, but there'll be a substantial remainder of work from home.

And concurrent with the work from home, there's been an acceleration of workloads moving to the cloud. The combination of these things means that you have to have better identity management.

Then, you have to add the third-party risk that so many attacks are emanating from, and how you control those identities, as well.

The ways in which you connect to the cloud and configure the interaction between your employees and the use of applications are critically important in the ongoing pandemic age that we live in. It's accelerating trends that were already underway.

The other thing you need to think about is social media. Not only is that going to be a problem for governments and our electoral process, but we're not very far away from a coordinated attack between ransomware or some piece of malware combined with a social media attack. That would severely damage the reputation of a company.

Best Practices for Board Presentations

FIELD: How can CISOs explain important processes and convey urgent needs to the board?

COVIELLO: So many attacks today are based on stolen or compromised credentials, and those are the most insidious ones because, if I've got somebody's credentials, I can do whatever I want. It's not a question of malware being detected or some EDR response. I can do whatever I want.

When it comes to conveying urgency in an instance like that, you have to explain the risk to the business of the people – not nail down the complete end-to-end concept of identity management – and create urgency about that. You have to convey not only what's necessary to protect people, but also the ramifications of what happens if there are stolen credentials.

FIELD: Can you give specific examples of highly successful board presentations and unsuccessful presentations?

COVIELLO: Because businesses and the issues are so complex today and because the governance requirements are so vast, boards and managements are under tremendous pressure to get through a tremendous amount of material in a brief period of time. Good boards will communicate with management between board meetings, but they're never going to be in a position where they know anywhere near as much as the management team. That's the environment you're about to present into.

Then, yours is one of many presentations, and you might have 15 minutes, a half an hour or an hour. If it's an in-depth briefing and you come in with slides, you should be able to spend five minutes on each slide. So, if you have 30 minutes and you have 30 slides, you're going to fail. If your support materials are full of technical terms and diagrams, you're going to fail. The presentations that fail are the ones that try and convey too much information and too much technology.

Educating the Board

FIELD: Is there a single technology or product area or area of information risk that boards never seem to understand? And if so, how do you convey the importance?

COVIELLO: Let's start at the top: threat intelligence. Why do we need it? What does it do for us? Well, I'd certainly like to know what's going on in the dark web and whether somebody is purveying my credentials or not.

The one that drives everybody crazy is anti-malware. The boards think, "If I have antivirus, I should be OK." And they may not be. If it's signature-based technology, then it's only as good as the last signature. If it's more machine learning-based technology, it depends on the strength of the algorithm. Boards have a hard time understanding that, but you can educate them on machine learning and what it does.

FIELD: What's your advice when you have a great budget and support from the board, but they're ill-educated, not tech-savvy? How do you provide security awareness and training for the board members?

COVIELLO: The National Association of Corporate Directors has programs. Look at the curriculum and, based on your knowledge of the board members, help them decide which of those sessions they should take. Or bring in one of the big systems integrators, maybe a VAR you're close to – somebody that presents effectively to the board. Give the outside group the profile of the board and what you're trying to accomplish. ■

About ISMG

Information Security Media Group (ISMG) is an intelligence and education firm focused exclusively on cybersecurity. Our 30 global media properties provide security professionals and senior decision makers with industry and geo-specific news, research and educational events.

CyberEdBoard Talks Excerpt

Access the full interview by becoming a member.
Visit cyberedboard.io to submit your application.

CyberEdBoard

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io