Secureworks®

WHITE PAPER

Board-Level POV: Negotiating Need to Achieve Acceptable Security Risk

Cybersecurity needs to be a business conversation and we are starting to see priorities shifting amongst board members, who are increasingly expressing concerns about cybersecurity and pushing for open dialogue with business leaders.

Yet the historical divide between the boardroom table and the security bullpen has created poorly aligned nomenclature between the two worlds. Because the bridge between the two worlds is still being built, clear and transparent conversations are essential. Clarity of terms is especially important in cybersecurity because, when negotiating needs, it is easier for people to say no to something that they don't understand. As an advocate for the security of your business, your data, and your customers, your objective in the negotiation process is to remove as many paths to 'no' as possible.

So how do you make it easy for someone to say yes to enabling your needs? Articulate it in clear terms where the ask, the cost and the outcome are free from ambiguity. Through hundreds of consulting engagements, Secureworks® has identified 4 things that CIOs need to be able to coherently discuss security with the board and negotiate a balance between productivity, strategy execution and security posture improvement that achieves an acceptable risk tolerance.

1. Articulate Current Position

The objective of this part of the negotiation is to instill confidence in the board and demonstrate that you are the subject matter expert. As such, you may be tempted to pad your current position reporting with loads of data to highlight how your security strategy is performing. Remember that the subject matter is foreign to the board; more data and statistics may obscure your message or lead to confusion. To increase board receptivity and build confidence that both you and your strategy are correct, offer enough context to make the data relevant to likely business risks and the strategic goals of your organization. This is done by talking to the following items:

- **The threat horizon** – What threat group types would target your organization and why?
- **Inherent risk** – What is it about your organization (i.e. data types and volume) that makes you an attractive target?
- **Current security posture** – Where is your security strategy doing well and where do you have potential vulnerabilities?
- **Current costs** – What are you spending – operational costs and capital cost – and how you plan to budget for risk reduction?
- **Current vulnerabilities** – What vulnerabilities need to be addressed to reduce risk?
- **Current legal and regulatory environment?** What government, industry or laws do you need to adhere to and how are you managing them?

In order to communicate to the board in a more effective manner, avoid discussing the tactical components of your security strategy, use a revenue and margin lens and focus on business impact. A single slide that clearly and coherently articulates current position will help you to bridge the cybersecurity world to the business world with a little more ease, allowing for a better conversation.

2. Articulate Your Need

By now, you have addressed your current posture in a board friendly way that has given them confidence in you as the subject matter expert. The next step is to ask for what you need and demonstrate how it will move the needle for your security posture. This is more than a simple request. The fastest route to a negative response comes from someone who doesn't understand the ask. As you develop your ask, follow these guidelines:

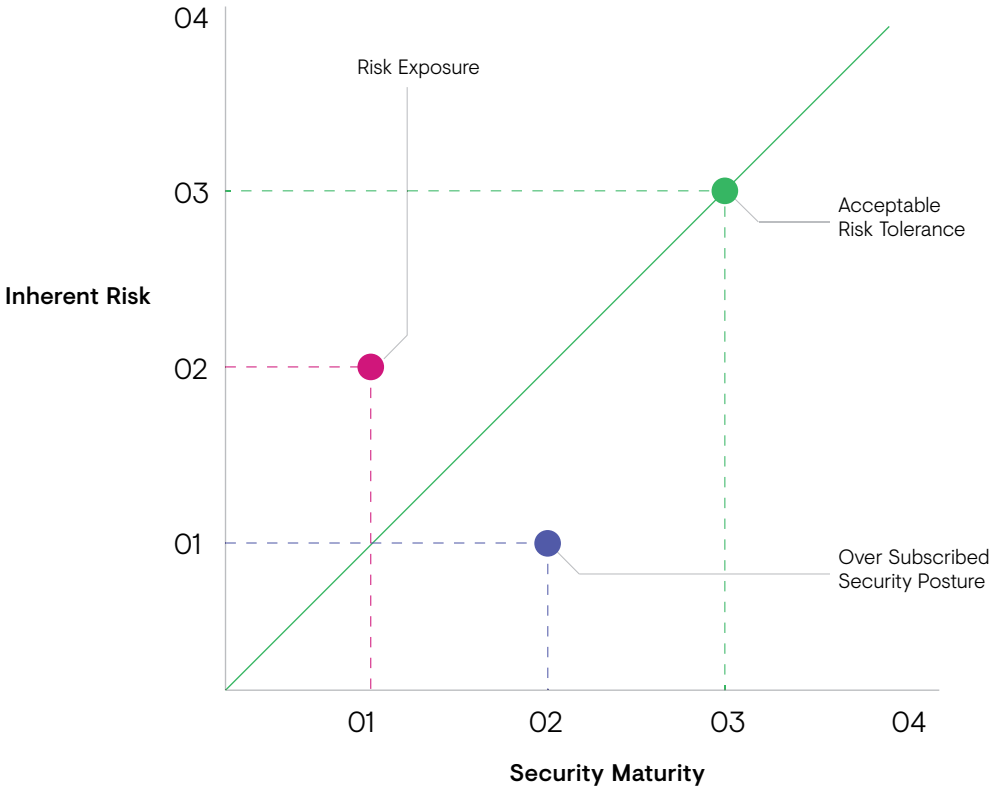
- **Make it easy to understand** – Avoid technical jargon and keep it high level.
- **Align to your current vulnerabilities** – If you didn't mention it in the current state, you shouldn't be mentioning it now.
- **Have a timeline to completion** – You need to show when the organization will start seeing the benefits and a comprehensive roadmap that will align with the overall strategy.
- **Show how it aligns to the business objectives** – If it does not align to a board priority, they will not see the point.
- **Be willing to compromise** – The board does not want ultimatums. Present a few options, each of which has the above four points. This way you are more likely to find a mutually beneficial position to agree upon.

While there may be more you are looking to demonstrate during your ask, we recommend keeping it relatively simple. Extraneous detail makes it easier to miss the point.

3. Articulate the Cost as a Risk-Benefit Analysis

There is a reason cost is not included in point 2 above. Cost is an easy break point for many people. If they see a big cost, they can be quick to react in a negative way without understanding the big picture. As such it is important to present the cost as a cost benefit analysis. This can be done in different ways but the easiest is using security posture maturity versus inherent risk. In **Figure 1** below you can see the importance of balancing security posture needs with inherent risk. The green line represents a balanced security posture, the red dot represents underinvestment in your security program and as such unnecessary risk. The blue dot represents a security posture that is oversubscribed and could be adjusted to be made more efficient. There is a point in which oversubscription is beneficial: when you are preparing for company transformation, or perhaps a merger or acquisition, whereby your inherent risk will increase in the near future. Being oversubscribed ahead of a major change reduces any latency in which you are exposing the business to unnecessary risk.

Figure 1



As you explain the financial impact to the board, demonstrate that the proposed benefits are not unnecessarily oversubscribing, but rather closing any risk gaps that currently exist or mitigating any potential risk to the business that may arise from organization objectives and priorities. The latter plays a very significant role when it comes to digital transformation. As mentioned in the Digital Transformation Executive Report, building a culture of innovation that starts with security in mind will require a momentary oversubscription in your security posture. This oversubscription will align to an acceptable risk tolerance as your digital transformation initiatives operationalize. This needs to be included as you discuss and negotiate cost with the board.

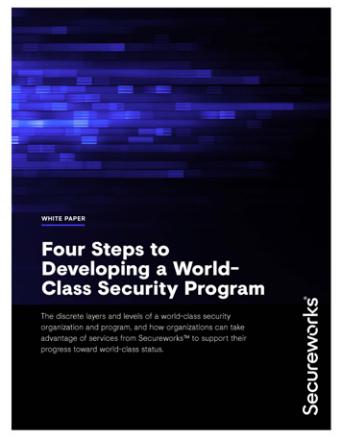
4. Explain the Outcome by Aligning to Business Strategy

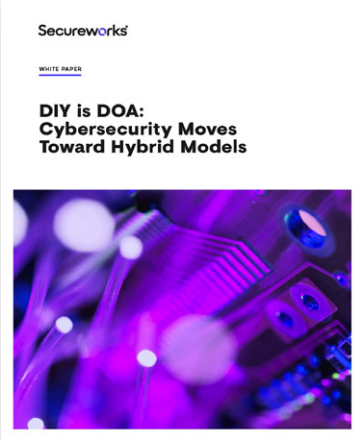
Now that you have shown the cost of your ask to the board you must carefully articulate the expected outcomes of your ask. This is tricky to negotiate for two reasons. First, not all initiatives have a clear route or a direct outcome, and some asks can impact other objectives. For example, perhaps you want to leverage a managed service provider to provide some networking support. This would enable you to focus on developing a new virtualized network to improve your organization's scalability and agility to run critical system testing. In this example the outcome of your ask is not to provide networking support but rather to free up resources in your organization to enable innovation. Be clear in how the outcome of your ask aligns to business needs. The second challenge to outcomes is to define in simple language the parallel between your ask's outcome and the business. Again, someone is more likely to object to something that they don't understand. Finally, you must also tie the way you present the outcome back to how you articulated your current posture. This creates a common language of communication, and ensures that you have a template to report on, moving forward.

If you can develop these four elements in your presentation to the board, your negotiations should improve, and your objective of achieving balance between productivity, strategy execution, improved security posture and ultimately an acceptable risk tolerance should become possible.

Want to learn more?

Click on the assets below to continue learning





Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp