GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Metivier, Becky

Title: "How to Make Your Board of Directors Cyber Smart"

Website: tylercybersecurity.com

Organization: Tyler Technologies

Date: 09 April 2019

URL: https://www.tylercybersecurity.com/blog/how-to-make-your-board-of-directors-cyber-smart

Accessed: 21 Oct 2019

Synopsis: As cyber threats continue to escalate, Boards of Directors are becoming increasingly interested in cybersecurity and risk management. This is no surprise, as the Board is ultimately held liable and responsible should a breach occur. And it's important because leadership sets the tone for the rest of the organization. They must lead by example when it comes to cybersecurity, and actively participate in, and be supportive of, the mission to be secure. As such, cybersecurity has made its way onto the agenda of many Board meetings.

Presenting to the Board is a great opportunity for CISOs, because they set policy and approve budgets. It's also very challenging because cybersecurity can be an overwhelming subject. According to Rob McMillan, research director at Gartner, "there's often a misalignment between what the Board needs to know and what security and risk management leaders are able to convey. It's critical that security and risk management leaders supply Board-relevant and business-aligned content that is not hampered by overly technical references."

How to Make Your Board of Directors Cyber Smart

Becky Metivier

 As cyber threats continue to escalate, Boards of Directors are becoming increasingly interested in cybersecurity and risk management. This is no surprise, as the Board is ultimately held liable and responsible should a breach occur. And it's important because leadership sets the tone for the rest of the organization. They must lead by example when it comes to cybersecurity, and actively participate in, and be supportive of, the mission to be secure. As such, cybersecurity has made its way onto the agenda of many Board meetings.

Presenting to the Board is a great opportunity for CISOs, because they set policy and approve budgets. It's also very challenging because cybersecurity can be an overwhelming subject. According to Rob McMillan, research director at Gartner, "there's often a misalignment between what the Board needs to know and what security and risk management leaders are able to convey. It's critical that security and risk management leaders supply Board-relevant and business-aligned content that is not hampered by overly technical references."

There's a lot of mystery and complexity when it comes to cybersecurity, and if you don't unravel some of that the Board can't possibly be aware of the risks that are presented or make the right decisions. That's why it's important to understand who you're talking to and their level of expertise. Then speak to that understanding... plus a little bit more. It's great if you know their other business involvements as well, and try to make a personal connection for them. Presenting information that is relevant to them will drive interest, and buy you more time at the table. And don't forget that if you're using graphs, make sure they are clear and easy to understand.

Building a Foundation

Ultimately, Boards need to get a basic education in cybersecurity. It's up to you to provide them with the information that they need to know, so they can understand everything else. They simply can't wrap their minds around things they can't understand. If they don't have a foundation, the rest of the subject matter is going to

be very difficult to understand. It's very important that they understand because you want them to approve the resources you need and the budget you want.

Here are a few topics that can help you build that foundation.

#1. Roles & Responsibilities

First of all describe to the Board your organization's approach to cybersecurity. How it aligns with your business strategy. How it supports it. You may find that in any executive management or Board discussion, security will seem like a road block that's getting in the way of creativity and innovation, rather than supporting it. You need to show them that this is not the case if security is part of the strategic conversation from the very beginning. Alignment can happen!

You should also speak to governance and oversight. Who should they be watching? How do these functions relate to cybersecurity risk? How do the roles interact? How are we sharing information between departments and functions? How do end-users participate in the program? They need to have a holistic view of the entire organization in terms of cybersecurity.

#2. Build Cyber Risk Awareness

Next, include information on the primary risk areas facing your organization. You should consider taking a "deep dive" into a particular topic at each presentation. For example:

- Adversaries you're facing and common attack vectors... especially social engineering;
- Mobile device proliferation and the increase in mobile malware;
- The ever-increasing complexity of malware and why it's difficult to detect a breach;
- Assets (data and infrastructure) and access to them; and
- Disruptions of operations from a security incident or emergency / disaster event.

#3. Timely Real-World Information

Let them know what's going on in the threat environment. This can include game-changing breach events, such as the Target breach or the recent Equifax breach. You can also include information on trends and future analysis. There is a wealth of great documents out there, including the Ponemon Cost of Data Breach Study and the Internet Security Threat Report from Symantec.

Share relevant "wins" for the good guys. It helps to buoy their spirits. Let them know it's not all doom and gloom, that there are some positive things going on as well.

Be sure to touch on what your peers are doing as well. This information can be gained from industry events, trade papers, etc. Consider making some friends in your competitive space. Your entire industry can really benefit from this collaboration.

#4. Expectations and Feedback

It's important to always seek feedback regarding the tone and value of content after each presentation. Over time you'll be able to go a little bit deeper into everything because they'll have more knowledge. Ask them what they want to learn more about. Remember that interest will drive awareness.

You should also set expectations. Let the Board know what information you'll be bringing them and why it's important. Then let them know how they should participate in the program.

Learn more in our blog post, *Cybersecurity Roles and Responsibilities for the Board of Directors*.

THE SAGE ADVICE GUIDE TO CYBER THREAT HUNTING

As cyberattacks continue to soar, it's time to get proactive when protecting your network. You can't simply sit back and wait for an automated alert to let you know you've been breached. You need to actively seek out potentially malicious behavior on your network. That's why we're seeing a shift to a more proactive approach... Cyber Threat Hunting. Learn how to defend your network. Learn more in the Sage Advice Guide to Cyber Threat Hunting.

Topics: Cybersecurity Culture, Risk Management