



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

Author: Microsoft Secure Blog Staff

Title: "Talking Cybersecurity with the Board of Directors"

Website: microsoft.com

Organization: Microsoft

Date: 31 January 2019

URL: <https://www.microsoft.com/security/blog/2019/01/31/ciso-series-talking-cybersecurity-with-the-board-of-directors/>

Accessed: 21 Oct 2019

Synopsis: In today's threat landscape, boards of directors are more interested than ever before in their company's cybersecurity strategy. If you want to maintain a board's confidence, you can't wait until after an attack to start talking to them about how you are securing the enterprise. You need to engage them in your strategy early and often—with the right level of technical detail, packaged in a way that gives the board exactly what they need to know, when they need to know it.

Cyberattacks have increased in frequency and size over the years, making cybersecurity as fundamental to the overall health of the business as financial and operational controls. Today's boards of directors know this, and they are asking their executive teams to provide more transparency on how their company manages cybersecurity risks. If you are a technology leader responsible for security, achieving your goals often includes building alignment with the board.

Bret Arsenault, corporate vice president and chief information security officer (CISO) for Microsoft, was a recent guest on our CISO Spotlight Series, where he shared several of his learnings on building a relationship with the board of directors. We've distilled them down to the following three best practices:



January 31, 2019

CISO series: Talking cybersecurity with the board of directors

Microsoft Secure Blog Staff

In today's threat landscape, boards of directors are more interested than ever before in their company's cybersecurity strategy. If you want to maintain a board's confidence, you can't wait until after an attack to start talking to them about how you are securing the enterprise. You need to engage them in your strategy early and often—with the right level of technical detail, packaged in a way that gives the board exactly what they need to know, when they need to know it.

Cyberattacks have increased in frequency and size over the years, making cybersecurity as fundamental to the overall health of the business as financial and operational controls. Today's boards of directors know this, and they are asking their executive teams to provide more transparency on how their company manages cybersecurity risks. If you are a technology leader responsible for security, achieving your goals often includes building alignment with the board.

Bret Arsenault, corporate vice president and chief information security officer (CISO) for Microsoft, was a recent guest on our [CISO Spotlight Series](#), where he shared several of his learnings on building a relationship with the board of directors. We've distilled them down to the following three best practices:

- Use the board's time effectively.

- Keep the board educated on the state of cybersecurity.
- Speak to the board's top concerns.

Use the board's time effectively

Members of your board come from a variety of different backgrounds, and they are responsible for all aspects of risk management for the business, not just security. Some board members may track the latest trends in security, but many won't. When it's time to share your security update, you need to cut through all the other distractions and land your message. This means you will want to think almost as much about how you are going to share your information as what you are going to share, keeping in mind the following tips:

- Be concise.
- Avoid technical jargon.
- Provide regular updates.

This doesn't mean you should dumb down your report or avoid important technical information. It means you need to adequately prepare. It may take several weeks to analyze internal security data, understand key trends, and distill it down to a 10-page report that can be presented in 30 to 60 minutes. Quarterly updates will help you learn what should be included in those 10 pages, and it will give you the opportunity to build on prior reports as the board gets more familiar with your strategy. No matter what, adequate planning can make a big difference in how your report is received.

Keep the board educated on the state of cybersecurity

Stories about security breaches get a lot of attention, and your board may hope you can prevent an attack from ever happening. A key aspect of your role is educating them on the reasons why no company will ever be 100 percent secure. The real differentiation is how effectively a company responds to and recovers from an inevitable incident.

You can also help your board understand the security landscape better with analysis of the latest security incidents and updates on cybersecurity regulations and legislation. Understanding these trends will help you align resources to best protect the company and stay compliant with regional security laws.

Speak to the board's top concerns

As you develop your content, keep in mind that the best way to get the board's attention is by aligning your messages to their top concerns. Many boards are focused on the following key questions:

- How well is the company managing their risk posture?
- What is the governance structure?
- How is the company preparing for the future?

To address these questions, Bret sticks to the following talking points:

- **Technical debt**—An ongoing analysis of legacy systems and technologies and their security vulnerabilities.
- **Governance**—An accounting of how security practices and tools measure up against the security model the company is benchmarked against.
- **Accrued liability**—A strategy to future-proof the company to avoid additional debts and deficits.

When it comes to effectively working with the board and other executives across your organization, a CISO should focus on four primary functions: manage risk, oversee technical architecture, implement operational efficiency, and most importantly, enable the business. In the past, CISOs were completely focused on technical architecture. Good CISOs today, and those who want to be successful in the future, understand that they need to balance all four responsibilities.

Learn more

Be sure to check out the interview with Bret in Part 1 of the CISO Spotlight Series, [Security is Everyone's Business](#), to hear firsthand his recommendations for talking to the board. And in Part 2, Bret walks through how to talk about [security attacks and risk management with the board](#).

The National Institute of Standards and Technology (NIST) [Cybersecurity Framework](#) is a great reference if you are searching for a benchmark model.

To read more blogs from the series, visit the [CISO series](#) page.

Filed under:

[CISO series](#), [Cybersecurity](#), [Data governance](#), [Microsoft Cloud App Security](#)

You may also like these articles