



[Return to the blog](#)

Cybersecurity Whack-a-Mole In the Boardroom



Boardrooms are faced with seemingly unending challenges related to cybersecurity oversight. The growing complexity and ever-changing persistent nature of cyber-risk is daunting, seemingly overwhelming, and hard to understand. It can feel like a game of whack-a-mole where plastic creatures randomly pop up from a console only to be “whacked down” by a player with a mallet. The faster the player strikes, the faster the creatures pop up until the game ends and is scored. It can feel entirely defensive and uncontrollable. Few of us understand or care about how whack-a-mole works, what drives the pop-ups, or what resides inside the console which operates the game. After all it’s just a game you can walk away from. Cybersecurity oversight is not.

The growing use and reliance on complex digital business systems is exacerbating cyber-risk, a systemic risk to your business, one which can result in serious, perhaps even existential damage. The interactions of information and technology have evolved from segmented IT functions into the central nervous systems controlling the most vital assets and systems of your business. Cyber-risk threatens these systems. Boards realize this is a major problem but are challenged by its enormity and complexity to find a path to better governance. Instead, they often retreat to a false sense of security offered by a “check-the-box” solution. However, the “whack-a-mole” feeling soon returns and persists-the feeling that more should be done. But how to do it?

Notwithstanding its complicated, chaotic, and ever-changing nature, cybersecurity is governable. However, today there is a disconnect between the boardroom and the cybersecurity management team (“Security”), the one with the mallet, identifying, and knocking down cyber threats. This disconnect creates a governance gap which must be closed. The Board’s responsibility for cybersecurity governance cannot be transferred to the Security team. Unfortunately, the sinking “whack-a-mole” feeling will not go away until Boards decide to make organizational, educational, and cultural changes required to close the gap.

Cybersecurity “Whack-a-Mole” Defenses

To understand the extent of the governance gap, as a Board member ask yourself the following questions:

- Can you contextualize the magnitude of various cyber-risks?
- How do you make decisions to increase cybersecurity spending?
- Does your company understand risk tolerance and has it developed a risk appetite?
- Is your Security team elevated to present to the Board?
- If so, do you understand what is being presented?
- Is it presented in plain business terms or in tech jargon?
- What is the position of the Security team in the management structure?
- Is cybersecurity an integral part of the Board’s enterprise risk strategy or is it viewed as a siloed IT function?
- Do your cybersecurity protections go beyond the company to include customer, third party, operational and software interfaces?
- Do you equate cybersecurity compliance audits with governance?

[JOIN PDA](#)

[Contact Support](#)

Forgot Your Credentials?

Existing Users/Prospects

If you cannot remember your username, [please click here](#).

If you cannot remember your password, [please click here](#).

Quick Links

[Events](#)

[Board Governance Insights Blog](#)

[Chapters](#)

[View Board Roles](#)

[Post Board Opportunities](#)

[Subscribe to Our Newsletter](#)

Upcoming Events

Tue Feb 7, 2023

[Chicago Chapter In-Person Event | Chicago Chapter New Member Breakfast](#)

Category: Chicago

Tue Feb 7, 2023

[4 Chapter Webinar: Atlanta, NY, New England, DC](#)

Category: Multi-Chapter

Wed Feb 8, 2023

[New England In-Person Event | Corporate Culture](#)

Category: New England

Thu Feb 9, 2023

[Webinar | Due Diligence for the Board Member](#)

Category: Chicago

Wed Feb 15, 2023

[Webinar | Being Board Ready](#)

Category: Greater Philadelphia

[Event List](#)

Twitter Feed

Tweets from [@PrivDirAssoc](#)



Priv...
· Jan 27



Want a variety of [#boardcandidates](#)

- Are there understandable procedures in place to respond to and report cyber breaches?
- Was the Board involved in developing and approving these procedures?
- Does your company have a framework for dealing with cybersecurity?
- Does the Board participate in tabletop exercises to train for responses to cyber breaches?

The answers to these and other questions will likely inform the need to transform your governance practice from a defensive posture-usually defined by the Security team-to an offensive governance paradigm, which includes more Board participation and becomes integral to the culture of your business. Maintain your current cybersecurity practices while you make this transition. Your Security team is probably employing many good practices to protect your enterprise. Some or all of these practices will be included in an improved offensive governance paradigm.

Reorganize to Take the Offensive

Elevate the head of the Security team to report to the C-Suite and the Board thereby signaling the importance of cybersecurity as part of strategic enterprise risk. Establish Risk Committees at both the Management and Board levels whose purpose is to evaluate new opportunities and related risks introduced by changes to the business. Changes could include new digital technologies, acquisitions, divestitures, changing third-party relationships, etc. The Management Committee should include representatives from all functional areas of the enterprise and be led by the head of the Security team. Establish clear authorities and responsibilities for committee heads. Mandate both regular and event-driven communications between the Management and Board committees.

Consider adding cyber/systems expertise to your Board but resist the temptation to delegate cybersecurity to these individuals as “checking the box” for good governance. Cybersecurity governance requires the attention of the entire Board.

Educate for Governance Success

This is the hardest element on the road to effective cybersecurity governance, but one which is essential for success. The logic is straightforward. Enterprise cyber-risk is a form of systemic risk, which can only be dealt with and contextualized by understanding the underlying system. The system in the whack-a-mole game is the console operating the plastic pop-ups. Your business system or “Ecosystem” is a regularly interacting or interdependent group of elements and subsystems which comprise your business function. Ecosystem elements include assets, processes and the people who interact with one another both internally and externally. Sound complicated? - It is! However, the Board can effectively govern by committing to an education process which captures the essence of the Ecosystem in straightforward business terms and makes it a tool for good governance. Cyber-risk cannot be contextualized and governed without understanding the Ecosystem.

Start by engaging outside advisors to work with your Management team and the Board to deconstruct, identify, and describe Ecosystem elements and how they interact with one another. Demand that this be done using plain business language. Begin with simple concepts. This advice may be subsumed under widely employed “risk assessment” studies which describe Ecosystem cybersecurity vulnerabilities. However, be careful of the impact on your cyber-spend. Risk assessment studies are important but too often only provide cyber fixes without putting them into context. You need more!

Expand the education process beyond the Board to include the C-Suite and the Security team to ensure that all key constituents develop the same contextual understanding of the Ecosystem. This is particularly important for the Security team to gain a broader understanding of risk mitigation goals of the entire business enterprise. Go to the next layer of understanding the Ecosystem once the fundamental concepts are understood. This is a continuous education process at all levels of your enterprise. Board members will find this Ecosystem education will facilitate improved communications with the Security team. Other benefits will ensue.

These include answers to the following basic questions: What are the most important assets in your business? What are the design flaws in your Ecosystem which could be improved? How resilient is your Ecosystem to the inevitable cyber-attacks? What are the Ecosystem’s cyber vulnerabilities? Can they be removed or mitigated?

In addition, understanding the Ecosystem establishes a basis for dealing with changes to your business caused by many factors, including but not limited to changes in digital systems, business strategy, addition, or deletion of lines of business, acquisitions, divestitures, etc.

Lastly, explore emerging cybersecurity tools for Boards which provide high-level contextual risk analysis and quantify financial exposure to your business. Tools which deal with the impact to your bottom line may not be fully understood or appreciated within the Security team who is usually the gatekeeper for all cybersecurity products and who may have a limited understanding of tools which transcend those which offer immediate cyber-risk mitigation.

Commit Today to a Proactive Cybersecurity Culture

Market, regulatory and legal pressures are mounting for Boards to get control of and develop better cybersecurity governance practices. Economic damage and litigation exposure is increasing at the

that can enhance the #governance of for-profit companies including - family-run, private equity portfolio companies and investment firms, or #ESOP-based organizations? PDA offers a complimentary posting service, bit.ly/PDA-BoardPosti...



same time cyber insurers are charging more and covering less. The SEC is proposing "SOX-like" disclosure requirements which will drive Board behavior. This will be a bumpy road. While finance is fundamentally limited in its dimensions, and relatively easy to understand, cybersecurity is multi-dimensional, ever-changing, and chaotic. Comparing finance to cybersecurity is like comparing a breeze to a hurricane. Pressing regulatory requirements alone will result in major changes in Board workloads and cultures which will dwarf the changes experienced with SOX compliance.

This leads to the conclusion that major changes in Board cultures are inevitable. Boards must choose to become proactive to get ahead of this problem or to remain reactive with unknown consequences. Making organizational, educational, and cultural changes today will substantially improve your cybersecurity governance. The roadmap to proactive governance is available. Without it the sinking whack-a-mole feeling in the boardroom will persist.



ABOUT ROD HACKMAN

Mr. Hackman's career has been dedicated to capital formation, M&A, financial restructurings, corporate development, and the creation of shareholder value as an advisor, entrepreneur and as a member of Boards of Directors with a primary focus on cybersecurity oversight. He served in a corporate finance role within several investment banking firms including Kidder, Peabody & Co., PricewaterhouseCoopers Securities and Hackman, Baring & Co. Mr. Hackman founded and was part of the management team of two special purpose acquisition companies both of which successfully completed business combinations. Mr. Hackman also served in the military as a line officer in the U.S. Navy where he supervised, operated, and managed shipboard nuclear reactors.

Mr. Hackman received an M.B.A. from Cornell University and a B.S. from the United States Naval Academy majoring in Applied Mathematics.

The Private Directors Association is thankful for the support from all of our National Sponsors




Share this post:



(847) 986-9350 | admin@privatedirectorsassociation.org



© 2022 Private Directors Association NFP. All rights reserved.

[Back to top](#) 

[Privacy Policy](#) | [Image Policy](#) | [Press Releases](#)

powered by  MemberClicks