BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

May 16, 2022

Cybersecurity and Executive (dis)Orders
Cognitive and Systemic Risk in the Boardroom

By Mike Wilkes

By now we should have all begun to accept the adage “it’s not a matter of ***if*** you will be breached, but rather a matter of ***when***.” Any sufficiently motivated attacker can breach even the most secure and paranoid organizations given some time and effort. FireEye, one of the most well-run and security conscious companies in the world was compromised by the Russian-affiliated APT29 (Advanced Persistent Threat) otherwise known as Cozy Bear in the infamous SolarWinds supply chain attack in December of 2020. Given this new wild west reality, where script kiddies like LAPSUS$ have joined the ranks of successful attackers able to breach billion dollar companies such as nVidia, Microsoft, Electronic Arts and Okta with a bit of clever social engineering and not much else, the governance of cybersecurity risk has ratcheted up a few notches. So, what can we do to elevate our collective resilience?

This Risk Report focuses on what boards of directors can do to:

- Understand the nature of cognitive and systemic risk and their impact at the board level
- Better understand the unique dimensions of cyber risk
- Understand emerging principles for modern cybersecurity governance

Increasingly, board members are being asked to think like chief risk officers, whether they have the skills and experience or not. Understanding cybersecurity risks demonstrated by recent supply chain attacks against SolarWinds, Kaseya, Microsoft Proxy-Logon and Okta illustrate that boards are being held accountable for effective governance and risk mitigation. And companies will not change that reality by just purchasing a few more million dollars of cyber insurance. A significant percentage of the top 20 cyber insurance providers recorded historical loss ratios in 2021 given the number of breaches and ransomware attacks that have transpired since the global pandemic sent a majority of employees into a remote work environment. Premiums are increasing significantly and many insurers are considering the option of not underwriting cybersecurity policies at all.

UNDERSTANDING THE NATURE OF COGNITIVE AND SYSTEMIC RISK

The insurance industry has been calculating risk indicators for catastrophic events such as floods, fires and earthquakes for quite a long time. But the actuarial tables for cybersecurity are only just being tabulated and recorded over the last 20 or so years. And the last two years have delivered some very surprising data with regard to impact and frequency. Consider the disruption that cognitive and systemic risk are casting upon the future of business.

Cognitive risk - among the many characteristics of cognitive risk is confirmation bias, which is especially important in board governance environments where most directors are not subject matter experts. It is perhaps one of the most pressing dimensions of risk because understanding cyber risk is a relatively new ask of executive management and boards of directors. A seat has been made at the proverbial table for the CISO and infosec professionals, but few board members are able to understand the crazy "moon language" of CVEs, CVSS scores, IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques and Procedures). In many cases board members are simply not even asking the right questions about failure and risk.

Systemic risk is an emergent property of complex systems. It is not rooted in any one component of these systems that comprise our digital economy, but rather in the density of connections and dependencies between all of the "nodes" in the network.

Together, cognitive risk and systemic risk in the boardroom can exacerbate the consequences of an unforeseen event. In February of 2021 Texas nearly dropped off the grid due to a severe winter storm. The citizens of Texas were a few seconds away from returning to the Stone Age had there been a "black start" event where the entire electrical grid experiences a cascade failure and collapse. After the storm the very next meeting of ERCOT (Electricity Reliability Council of Texas) saw half of its board members resign. This is an example of both cognitive risk (the board discussed the storm for only 40 seconds in their meeting before the storm) and systemic risk because rolling blackouts were invoked to shed load on the system which in turn took even more electricity generation offline.

Complex systems behave in ways that surprise us and the operators of the systems. This is the very definition of systemic risk, an emergent property of our increasingly interdependent critical infrastructure. Without continuous monitoring of these systems, our awareness of systems failure and breaches is significantly hampered. How we help make our ecosystem of vendors and service providers more resilient is the real challenge that must be met. Modern governance of cybersecurity risk sits squarely at the heart of that path forward.

As the risk environment changes, board members should guard against confirmation bias, a form of cognitive risk where board members may not realize the extent of the change in the cyber risk landscape and mistakenly assume that existing risk management structures and mitigation techniques are still adequate. Confirmation bias is ubiquitous, and we are all susceptible to it every day throughout our lives. In the boardroom, members should listen carefully to Chief Risk Officers, CISOs and others who brief the board on rapidly evolving cybersecurity risks. Challenge staff to make sure they are conveying not just facts but the full context around their risk analyses. What do experts - both internal and external - sense in the risk environment that may help your organization to enhance its ability to recover quickly from any disruption?

Systemic risk has grown in lock step with the complexity of supply chains, and boards should understand how that growth impacts the ability of their organization to mitigate risk.

Questions Boards Should Consider:

- Do board members fully understand how their organization's increasingly complex supply chain impacts the firm's risk environment?
- Is the organization equipped to mitigate new risks emerging from the increased number and complexity of its supply chains?
- Is senior technology risk staff going beyond simply reporting threats and providing sufficient context to enable board members to see how the risk environment might be changing over time?

WHAT IS IT THAT MAKES RISK IN CYBERSPACE UNIQUE, AND HOW DOES IT COMPLICATE BOARD GOVERNANCE?

A key characteristic of cyberspace is that, in warfare at least, the theater of operations in cyberspace is entirely man-made. Traditional warfare is constrained by natural features of the physical environment and can be used to one's advantage or disadvantage. But there are no natural features to cyberspace; in fact, it is constantly changing, adapting and transforming. In kinetic warfare a combatant delivers an ordinance to a location at a particular time. Boom! In cyber warfare, entities create the capability to deliver "an effect" at a particular point in time against a particular set of digital assets (denial of service attacks or malware infections are good examples). This is a much more "silent boom." The combination of the two is what is being termed "hybrid warfare" by analysts and experts. (See Richard Clarke's March 2022 *Board Risk Report*)

Threats and risks in cyberspace and cyber-attacks change every hour of every day. Risk assessments of partners and evaluations of a firm's own security posture require virtually real time analytics, which accounts in part for the sharp increase in attention to continuous monitoring capabilities we've seen in the past two or three years. Boards should understand the changing nature of cyber due diligence and should have a broad understanding of the tool sets that enable close to real time due diligence.

Cyber-kinetic risk management brings some new questions to boards of directors:

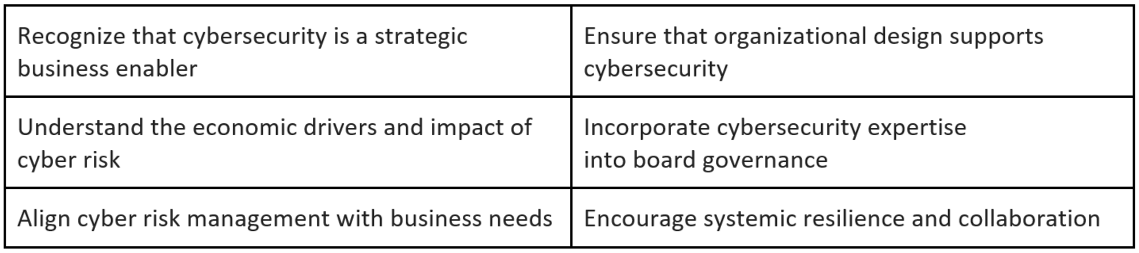
- Do you have a continuous monitoring capability for your third-party risk and service providers? Can you inventory *their* providers (4th or Nth-party risk)?
- How resilient is your organization to the loss or severe disruption of critical service providers?
- What is your current "too big to fail" scenario? If you haven't already, can you plan a tabletop exercise with your team to explore your response and options?

EMERGING PRINCIPLES FOR MODERN CYBERSECURITY GOVERNANCE

Companies that effectively manage their entire portfolio of risks, including cyber, do better in the marketplace. Regulators around the world are demanding scenario planning incorporating "severe but plausible" events with significant impact across a wide range of risk domains, including cyber risk.

Do board members need to be cybersecurity experts? Not necessarily. Board members need to understand the risk landscape and they need to know what questions to ask the C-suite as cyber risk continues to morph at lightning speed. Board members should understand where and when it is appropriate to turn to trusted advisors who understand the exposure to business disruption surfaced by threat intelligence. Of course, the board also needs to ensure that appropriate leadership is in place and that suitable resources are available commensurate with the organization's risk appetite.

The World Economic Forum and NACD published a whitepaper in March of 2021 entitled "Principles for Board Governance of Cyber Risk" which has identified six principles for modern governance which apply broadly across industries and sectors:



Recognize that cybersecurity is a strategic business enabler	Ensure that organizational design supports cybersecurity
Understand the economic drivers and impact of cyber risk	Incorporate cybersecurity expertise into board governance
Align cyber risk management with business needs	Encourage systemic resilience and collaboration

A follow-up study (see Advancing Supply Chain Security in Oil and Gas: An Industry Analysis) contains practical examples of what a holistic approach to building modern infosec programs entails. Continuous monitoring is a key ingredient to having awareness of third-party risk and changes in the security posture of supply chains and vendor ecosystems on a daily basis. All seven of the case studies provide valuable and actionable insights that every industry needs to understand in order to keep their company from getting into trouble. And there is a lot of cybersecurity risk and trouble out there that will eventually put your infrastructure and business in its crosshairs.

Questions Boards Should Consider:

- Is the cybersecurity function adequately represented throughout the business?
- Do you require management to report to the board with well-developed, written and tested plans to counter adverse cyber events? How effectively are those plans tested?
- Which board committee has primary oversight of cyber risk issues, and does it understand the changing nature of cyber risk governance?

ABOUT THE AUTHOR

Mike Wilkes

Chief Information Security Officer (CISO), SecurityScorecard

Mike Wilkes is a Chief Information Security Officer that has built, transformed and protected companies such as ASCAP, Marvel, AQR Capital, CME Group, Sony, Macy's as well as European banks and airlines. A graduate of Stanford University and author of a book for Cisco Press in 2002, he is a featured speaker at technology conferences and is a professor at NYU teaching cybersecurity courses. An avid jazz fan and musician, he is also on the board of trustees for the National Jazz Museum in Harlem. Contact: mwilkes@securityscorecard.io

***The Board Risk Report** is the monthly publication of the BRC. **SUBSCRIBE NOW** to receive complimentary world-class risk management practices delivered directly to your inbox.*

WHO WE ARE

The Board Risk Committee (BRC) is a non-profit, non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG) and Shared Assessments (SA). SFG is a strategic advisory company providing expertise to leading corporations and other critical infrastructure organizations in the area of risk management. SA is the thought leader and provider of tools, education and certifications in the third party risk management space. *The Board Risk Report is the monthly publication of the BRC.*

Contact:
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org