LOST IN TRANSLATION: THE REALITY GAP BETWEEN THE BOARD OF DIRECTORS AND CYBERSECURITY

SECURE CONTROLS FRAMEWORK

WHITE PAPER SERIES

CONTEXT

The purpose of this white paper is to provide information regarding a fundamental flaw in how the board of directors (BOD) of many public and private organizations fail to obtain the right level of information needed to make informed decisions, despite aggressive efforts to become more educated on cybersecurity. The result is that the BOD is unable to sufficiently advise the organization on the right course of action that benefits both shareholders and employees.

BACKGROUND ON THE PROBLEM

Cybersecurity is an important topic for the BOD, as the risks posed are significant. Currently, most BODs are either educating its members on cybersecurity or recruiting new hires to the BOD that are already well-versed in the cybersecurity side of Governance, Risk & Compliance (GRC). This level of expertise is needed to ask the tough questions of the executive leadership team, especially the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). Unfortunately, there is a lack of common terminology and understanding of industry frameworks that exacerbates the gap between BOD knowledge and cybersecurity operations.

As organizations engage and ramp up their BOD to understand the complex and technology driven risks relevant to cybersecurity, a unique gap is emerging. As noted in a panel on Board Governance at a recent Enterprise Risk Management Summit in Portland, Oregon, organizations are taking steps to close the knowledge gap, but there is a disparity in the level and type of information received by the BOD, as well as conciseness in what the BOD needs to understand current and emerging risks to the organization.

Fig. 1

While the primary purpose of the BOD is to "ensure the company's prosperity by collectively directing the company's affairs, meeting the interests of its shareholders and stakeholders," the BOD also establishes internal financial policies, such as options allocations, compensation methodology, and ultimately the hiring and firing of the C-level executive team.[1] Although the initial purpose of the BOD is rooted in overseeing the financial performance and investments of the organization, the BOD agenda is often consumed by a majority of non-financial matters that may have significant financial impacts, as noted during the Enterprise Risk Management Summit discussion. One panelist indicated the BOD's read-ahead packet routinely is "more than 300 pages of material each quarter." The information expected to be consumed and understood by the BOD is critical in helping the organization establish, maintain, and adjust the risk appetite to ensure management decisions are in-line with the industry, competitors, and geo-political fluctuations. However, these functions are not being effectively executed consistently by the BOD due to the large volume of information and frequently, the inadequate detail missing from pre-read packets. Interestingly, one point of frustration among panelists was the feeling that information often received on the technology direction and strategy, specifically in the area of cybersecurity was frequently "dumbed down" for the BOD and pre-read material was overly simplistic, rather than an expected level of detail needed to make informed decisions.

DUMBING DOWN VS SIMPLIFYING?

CIOs and CISOs often will not willingly "focus on the bad" when discussing cybersecurity with the BOD. Unfortunately, there is a misconception that bringing up poor results or unfavorable information in front of the BOD can be perceived as a career-limiting opportunity for a CIO or CISO, rather than as an opportunity to demonstrate leadership and initiative. Often these reported deficiencies may result in difficult discussions concerning lack of a cohesive technology/cybersecurity strategy or poor technology maintenance/use. For some IT leadership, it can be perceived as being more beneficial to gloss over systemic failures and highly summarized content, rather than discussing issues and determining course of actions to correct those issues. This may be a contributor to why the average tenure of technology executives is significantly less than C-suite peers, where a CIO's average time at a company is approximately 4 years and a CISO's is 1.5 years.[2]

1. Roles and Responsibilities of Board of Directors - https://www.brefigroup.co.uk/directors/directors_roles_and_responsibilities.html

[2] https://blogs.wsj.com/cio/2017/02/15/cio-stats-length-of-cio-tenure-varies-by-industry/
https://www.cio.com/article/2984607/security/the-average-ciso-tenure-is-17-months-don-t-be-a-statistic.html

Given the broad governance and oversight role the BOD has across all lines of business, there will always be a gap between the detailed skillsets of the organization's cybersecurity practitioners and the BOD. However, technology leadership often mistakenly approaches the preparation of BOD pre-read material with an overly simplistic "we've got this!" summary. Fear of negative reception frequently leaves the BOD with no actionable information for managing cybersecurity risk and the result is a failure to leverage the BOD discussion in a strategic manner regarding cybersecurity. Additionally, this limits their ability to ask more detailed questions both at an operational and strategic level, in providing oversight of cybersecurity matters.

The BOD expects the CISO to raise the conversation up to a level that allows Directors to debate intelligently. Currently, while the BOD is told of action plans and approaches to reduce cybersecurity risk through a series of "dumbed down stoplight charts and technology solutions to be purchased to address issues," as identified by one Enterprise Risk Management Summit panelist, many organizations' technology leadership miss the opportunity to have a rich, forward-looking discussion around a unified cybersecurity and privacy strategy. This is especially true for those companies impacted by the European Union General Data Protection Regulation (EU GDPR), where the concept of Cybersecurity for Privacy (C4P) is crucial and an organization can proactively manage both cybersecurity and privacy concerns in an efficient and integrated manner.

Communication Gap Scenario

This dumbing down of concepts often aggravates cybersecurity practitioners, who are tasked with designing, building, implementing and maintaining solutions to address the organization's applicable statutory, regulatory and contractual cybersecurity and privacy obligations. These cybersecurity practitioners often base the organization's day-to-day operations on leading cybersecurity frameworks to define and implement best practices for how people, processes and technology are implemented. The two most common security frameworks that companies align with tend to be ISO 27002 and NIST 800-53.

Fig. 2 "MAYBE WE SHOULD TRY A DIFFERENT SECURITY APPROACH THIS YEAR."

In a real-world scenario, as mentioned at the Enterprise Risk Management Summit, a board member from a large healthcare organization, spoke about how the BOD conducted annual risk assessments based on the Center for Internet Security (CIS) Critical Security Controls (CSC), formerly known as the SANS Top 20. These twenty controls are used to direct enterprise-level discussions on risk at the organization.

While there is nothing wrong with the CIS CSC as a framework, the healthcare organization runs its day-to-day operations against the NIST 800-53 framework, a comprehensive cybersecurity framework currently in use with well over 500 controls that are broken down into twenty-six different families of controls to better organize the content, which is used to comply with HIPAA, PCI DSS, as well as other statutory, regulatory and contractual obligations.

While it is impractical for the BOD to have the knowledge or review 500+ security controls as part of their Director duties, the fact that a completely different framework was used to report on and evaluate risk leaves much lost in translation, when discussing "what right looks like" for cybersecurity at the tactical, operational and strategic levels. This is especially important when discussing C4P to govern both cybersecurity and privacy needs, since they are absolutely intertwined and must be discussed in detail to avoid assumptions on the part of all parties involved.

Viewed in a slightly different context, this is akin to the finance department using Generally Accepted Accounting Principles (GAAP) for how day-to-day accounting is performed, while the BOD uses International Financial Reporting Standards (IFRS) to measure financial performance and provide direction. While these are both considered industry standards for accounting, they will account for revenues and expenses differently that results in very different financial pictures for recipients of the information. Asking the financial team to then shore up shortcomings in financial performance identified under IFRS would create confusion, frustration, and ultimately disengagement. As this routinely occurs within the technology sector, one must ask the question, "why is this tolerated within cybersecurity and IT but not within other business functions?" Isn't that a question the BOD should be asking the CIO and CISO?

Personal Liability Concerns

Control gaps that are lost in translation have real-world implications for Directors as, under most US states' laws, Directors have fiduciary duties to act with a degree of care that is prudent. Under this standard, Directors must act on an informed basis, in good faith and in the honest belief that their actions are in the best interests of the organization. This concept extends to oversight functions as well where a Director may be considered in breach of those duties if the BOD fails to implement or govern appropriate internal controls. This could also be applied in the context of cybersecurity incidents that occur due to a lack of appropriate controls.

A lack of a solid risk framework based on comprehensive and defendable cybersecurity and privacy controls creates a significant liability for Directors. Rather than a "point solution" to manage cybersecurity and privacy controls, CIOs and CISOs should leverage a holistic approach to cybersecurity and privacy control management so that strategic, operational and tactical concerns can be captured.

Simple Steps To Minimize Translation Issues

Regardless of the industry, executive management needs to understand that cybersecurity will remain a top agenda item for BODs for the foreseeable future. BOD members will continue to educate themselves on cybersecurity technologies and concepts so they can drill down into what is required for the organization to properly address cybersecurity and privacy risks. However, this will only be successful if the CIO and CISO educate the BOD with the appropriate information and sufficient detail, allowing the BOD to initiate conversations on how the organization should best secure technology, data and personal privacy details, both from a customer and employee perspective.

Transparency and good communication are required so the BOD is equipped with clear facts and situational awareness. This requires the CIO and CISO to be open and more strategic about the risks the organization accepts, as well as the likely risks that are not being formally tracked or addressed. This may sound counter-intuitive, but risk registers often only capture a fraction of the risks that are known or are summarized up to such a high level that the risks are diluted. In example of that, a fundamental control breakdown that affects tens of thousands of workstations, servers and applications may be described in a single risk entry or bullet point in the agenda, but the underlying issues are not identified or tracked as risks. Generally, this summarization approach does not adequately capture the right level of risk and precludes the BOD from fully understanding the true extent of risk exposure and the appropriate level of attention needed from the Directors.

"Transparency is a target that is achievable only through consistent and balanced conversations with the Board. Executing the conversations from a perspective of sharing the right information to enable a rich discussion focused on the security risks and efficient strategic options will be the Rosetta stone. While stop light charts will always find some use in boardroom level discussions", noted by one of the panel participants. "The security conversation can't remain just as a stop light discussion. Cybersecurity and technology leadership need to articulate what it means to not address or to fully address the risks we are seeing in the industry." However, to do that well is difficult and the first step required is orienting BOD members on the framework being used and how it is being applied (e.g., the control set that the organization actually uses to design and maintain secure systems and operations).

What Does the Future Look Like?

With the potential fine for non-compliance with the EU GDPR, an organization stands to lose up to 4% of its gross worldwide revenue or €20M, whichever is greater. With such a potential impact, organizations should ensure that the BOD is getting not only accurate information, but also the sufficient level of detail required to make informed decisions.

Through using a strategic approach to rightsize the people, processes and technology required to implement a unified set of controls, a BOD and CISO should move away from "tool purchasing" budgetary conversations to focus on a risk-based, integrated cybersecurity and privacy strategy that address Capability Maturity Model (CMM) targets that are specific to the cybersecurity and privacy frameworks currently being used.

As the media continues to publish successes and failures of emerging technologies, BODs are starting to anticipate some of these next-level discussions. For example, in addressing blockchain (used as a "ledger of trust" to create an identity access and control mechanism across applications and extended enterprises), conversations should not be centered around whether the organization starts to accept bitcoin as a payment mechanism, but rather about how the technology is being used to solve complex security problems and how that technology may or may not fit into the cybersecurity and privacy strategy as an enabling technology. This is where strategy is king and the CISO and CIO will be able to advise and lead the BOD to a more informed decision regarding use of any technology. It is the difference between leading with a plan or aimlessly experimenting with the latest technologies.

In the ever-changing risk landscape, a more cohesive, multi-year cybersecurity strategy is more important than ever before. A well devised strategy can also account for hot topic "disrupters" that make the headlines, such as Artificial Intelligence (AI), blockchain, cryptocurrency, etc. that can distract a BOD and allow them to focus on areas or technology that have a significant impact on the organization. However, the technologies themselves should never be misconstrued as the primary driver for a cybersecurity or privacy program and should always be underpinned with a risk and control framework that can help control the complexity and ever-changing demands of technology.

About The Authors

Tom Cornelius CISSP, CISA, CIPP/US, CRISC, PCIP, MCITP, MBA

Technology without strategy is chaos - Tom brings order through applying leading practices and aligning technology, cybersecurity and privacy requirements with business objectives. He brings a proven record of building and leading successful technology teams at several Fortune 500 organizations. Tom is the Senior Partner at ComplianceForge, an industry leader in cybersecurity and privacy documentation. He is also the founder of the Secure Controls Framework (SCF), a not-for-profit initiative to help companies identify and manage their cybersecurity and privacy requirements.

Derek Thomas CISA, CCMP, MBA

An experienced leader with over two decades of managing information risk, cybersecurity and compliance operations at several Fortune 500 organizations. Derek is the Managing Director for Scott Perry CPA, a niche CPA firm, focusing on Public Key Infrastructure (PKI) certificate security audits and is involved in the evolution of practices for how distributed ledgers can solve the conundrum of the web of trust for identity management. Derek also serves on the Oregon ISACA Board of Directors, connecting local industry leadership across multiple disciplines.

Special thanks to Andy Kuykendall for his excellent editorial skills for this article.

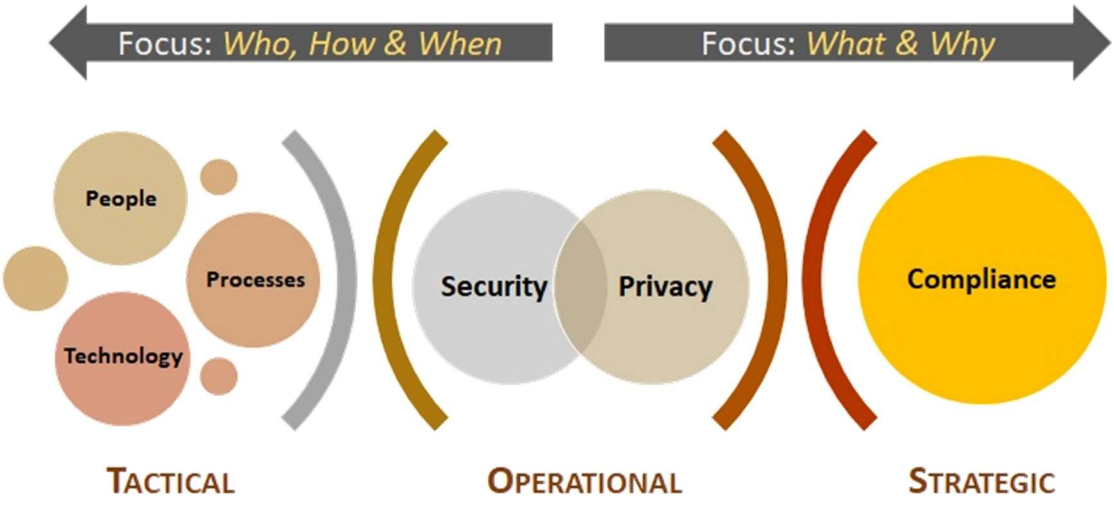
Secure Controls Framework (SCF)

The SCF focuses on internal controls. These are the cybersecurity and privacy-related policies, standards, procedures and other processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.

SCF | SECURE CONTROLS FRAMEWORK

The mission of the SCF is to provide a powerful catalyst that will advance how cybersecurity and privacy controls are utilized at the strategic, operational and tactical layers of an organization, regardless of its size or industry.

You can learn more about the SCF and download it for free at https://www.securecontrolsframework.com



*Cartoon graphics reprinted from the Enterprise Risk Management Summit handouts on Board Governance.