This article first appeared in NACD's Directorship® magazine. Further reproduction or dissemination of this document without permission from NACD is prohibited.
Copyright © 2024 National Association of Corporate Directors. All rights are reserved.

Cybersecurity Strategy Under the Microscope

This article first appeared in NACD's Directorship® magazine. Further reproduction or dissemination of this document without permission from NACD is prohibited.
Copyright © 2024 National Association of Corporate Directors. All rights reserved.

How the SEC Measures Program Effectiveness and What It Means for Boards

By Vishal Chawla and Mark DeLong

ON JULY 26, 2023, the US Securities and Exchange Commission (SEC) issued substantial new cybersecurity rules intended to ensure that businesses will not only be prepared for cybersecurity incidents but will also be transparent with their investors concerning cyber-risk strategies and governance.

Regulators have historically pushed compliance and companies have spent millions of dollars to fix compliance issues. Now, the focus will be on proactive risk management and rapid response.

One new rule highlights the change in direction: companies must report any cybersecurity incident that is "material"—traditionally, this indicates a substantial likelihood that a reasonable shareholder would consider it important—within four days of determining such materiality. To understand an incident's nature and scope, to judge the impact on operations and the relevance to shareholders, and to do so within four days, the enterprise must have foundational knowledge of what is material and proactive processes in place well before the incident occurs.

If an organization must disclose a significant cybersecurity incident, it faces the added risks of shareholder lawsuits, regulatory actions or fines, cyber insurance premium increases, and substantial reputational damage. These risks call into question whether the organization had an adequate cyber-risk management program in place. Investors who lose personal wealth due to a material incident will seek full transparency upon disclosure. Management's initial focus will be on meeting SEC requirements, followed by mitigating further risk exposure and addressing legal implications.

The proposed rule states, "Disclosure about the impact of cybersecurity risks on business strategy enables investors to assess whether companies will become more resilient or, conversely, more vulnerable to future cybersecurity risks."

The new rules will also require regular reporting about the company's governance system and processes related to material cybersecurity risk, management expertise in administering those processes to evaluate and control material cybersecurity risk, and specific cyber-risk oversight by the board.

Many companies may feel that their risk management frameworks and cybersecurity programs are best-in-class and ready to address the new rules. However, recent Office of the Comptroller of the Currency consent orders demonstrate that cyber-risk readiness has been insufficient, even under existing rules. Regulators identified significant safety and soundness issues in risk management frameworks and cybersecurity programs. First and foremost was an obvious shortfall: risk management "programs" that were not enterprise-wide did not capture end-to-end business methods and associated operational risks, and lacked comprehensive risk identification and assessment processes. Other problems included compensation and performance management programs that did nothing to incentivize effective risk management and lacked appropriate and effective controls to mitigate risks.

Considering the underwhelming state of cyber-risk preparedness in many companies as well as the new rules, management and the board should immediately ask the following

ISTOCK.COM / AISLAN13

This article first appeared in NACD's Directorship® magazine. Further reproduction or dissemination of this document without permission from NACD is prohibited.
Copyright © 2024 National Association of Corporate Directors. All rights are reserved.

questions: Have our risk management framework and cybersecurity program been reviewed, analyzed, tested, and effectively challenged by the enterprise risk management (ERM) team, internal audit, or external professionals to ensure that they are optimized to effectively reduce risks and prevent, mitigate, detect, and remediate cybersecurity incidents? If not, why? If not now, when?

Management and the board then need to move quickly to conduct an effectiveness assessment and analysis of the company's risk management environment, identify the gaps and weaknesses, and implement necessary remediation. The ERM team must drive strong alignment and collaboration with the businesses, chief information security officer (CISO), and internal audit to help understand and significantly enhance the risk posture.

Supported by common themes drawn from the proposed rules and recent consent orders, this effort should focus on the following seven facets:

1. Effective implementation of a robust enterprise risk management framework and cybersecurity program by building an enterprise- and business unit-level cyber-risk register. This is the first and most critical step as the framework establishes the basic tenets and strategies on which the cybersecurity program is founded, including what level of risk the company can or is willing to accept (risk capacity, appetite, or tolerance).

This framework does not supplant the need for audit and compliance (an historical view) but rather adds a forward-focused perspective. Cybersecurity strategies must protect the most valuable assets wherever a future breach could have the most significant potential effect, whether in terms of financial, legal, reputational, or regulatory impact.

The CISO, while working with the ERM team, should develop a cyber-risk register using a top-down risk assessment approach and NISTIR 8286 (from the National Institute of Standards and Technology, or NIST) guidance. The cyber-risk program must leverage the cyber-risk register to build an effectively designed, robust risk management program and governance model for information technology and cybersecurity, enabling the proactive reduction of risks affecting the organization. The program must include processes for risk assessment, covering all processes of the business and its high-value assets. It should also include definitions of materiality and the ability to determine the costs required to protect critical business processes and high-value assets.

As the program is developed (likely by the CISO and the ERM team), the overall portfolio of initiatives and principles for investment in cybersecurity should be presented to the CEO, CFO, business leadership, and the board for their understanding and acceptance.

2. Top-down and visible board and C-suite risk management support. For many companies, this will entail not only new processes but also a new culture (risk management instead of compliance). As with any new approach or initiative, those at the top must provide visible, sincere support. People in the organization will quickly interpret any half-hearted and haphazard communications from above as a storm that will blow over and can be ignored.

This is an opportunity for messaging from the board and management regarding how risk must be integrated into the ongoing business, including priorities, the need for risk assessments and evaluations, and the need for informed decision-making on all investments and funding.

3. Close partnerships among the various organizational silos. With the new SEC rule requiring alignment of cybersecurity and business strategy, cybersecurity programs and processes cannot be developed, implemented, and maintained by one department or unit. The CISO and ERM team may be the champions and coordinators, and they may offer a credible challenge to other parts of the organization, but they are not the sole actors. Instead, management of cyber risk must be a collaborative effort that takes advantage of organizational knowledge. The formation of business controls and methodologies must involve those who know the business the best and who will be most affected by the change, and operational management of cyber risk cannot be successful across the enterprise if any barriers exist at organizational boundaries.

4. Clearly communicated roles, responsibilities, and accountabilities. Though collaboration is a necessity, actions still need accountability. To avoid both gaps and overlaps in execution, roles and responsibilities must be clearly defined and assigned.

An effectively enacted three-lines-of-defense (3LOD) structure can bolster the definition of roles.

- In the first line, business or operational management has control of its own business processes, business process objectives, risks to achieving objectives, and controls to mitigate risks.
- In the second line, the ERM team owns the risk policies, standards, methodologies, and procedures the businesses follow to identify, assess, measure, monitor, aggregate, and report on end-to-end business process risks and controls. The ERM team should monitor the progress of cybersecurity-related initiatives

ISTOCK.COM / LEO WOLFERT

This article first appeared in NACD's Directorship magazine. Further reproduction or dissemination of this document without permission from NACD is prohibited.
Copyright © 2024 National Association of Corporate Directors. All rights reserved.

and investments, as well as the outcomes of investments and mitigation efforts.

- In the third line, the audit group is responsible for evaluating the design, effectiveness, and efficiency of governance, risk management, and control processes for the first and second lines of defense.

The ERM team must remain forward focused. If it leans too much toward compliance (perhaps acting as a pre-audit function), the overall enterprise risk management function and cybersecurity program are weakened.

5. Well-documented end-to-end business processes. Risks cannot be thoroughly assessed, and the materiality of a breach cannot be entirely evaluated, without fully understanding and documenting business processes from end to end, top to bottom, and side to side. If leaders don't know how business processes work, they cannot protect them.

Based on the results of recent regulatory examinations, the SEC's "Cybersecurity and Resiliency Observations" offers guidance on industry practices for unearthing points of exposure (e.g., the potential for data loss during the decommissioning of company hardware or software).

The NIST Cybersecurity Framework (CSF) also provides an excellent resource for the CISO and ERM team in this effort. The framework, which was recently updated for the first time in a decade, comprises three main parts: the core, organizational profiles, and tiers. The core, according to the CSF 2.0, "is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks." The organizational profiles "are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF core's outcomes." The tiers "can be applied to CSF organizational profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices."

This assembled knowledge aids not only in the identification of risks, but also in the design and implementation of controls.

6. ERM input into executive and senior business line compensation decisions. As a self-check, management should invite the ERM team to provide input on performance and compensation reviews. The ERM team is in a position to offer opinions on management's contributions to cybersecurity and other risk management efforts and results. This extra attention may help move the needle on new initiatives in a new culture. As the adage says, what gets measured gets done.

7. A high level of employee expertise in risk management across the businesses, ERM, and internal audit. Perhaps this seems obvious, but it is well worth mentioning: ensure that risk management expertise is in the right places. Again, considering the 3LOD model, a strong grasp of risk—where it can originate, how it can affect the company, how to mitigate or control it—is essential at the front line, within the ERM organization, and at the back end in audit. Managing risk to the level required by the SEC is not a game for amateurs.

The Road Forward: Effectiveness as the New Cybersecurity Benchmark

With the new rules, the SEC is taking a serious stance on cybersecurity program effectiveness in protecting risk to business strategy. It has not been shy with fines in the past and will likely issue painful sanctions to those not measuring up to fresh requirements. Since the new rule's implementation last year, investor and stakeholder lawsuits have spiked following any cybersecurity breach.

Pursuing the seven points outlined above will prepare any company to meet the most critical cyber-risk issues cited by regulators. A detailed action plan, timeline, and assigned ownership are essential to address the most significant gaps and weaknesses. While the implementation of an enterprise risk management framework and cybersecurity program will not eliminate risks, it should reduce the impact of risk to fit within a company's established materiality and risk appetite thresholds.

Change is in the wind. The time to act is now.

VISHAL CHAWLA is the founder and CEO of BluOcean Digital, a premier C-suite cyber-risk advisory firm. With extensive expertise in cyber-risk governance and board oversight, he has more than 25 years of experience in assisting Fortune 500 financial services, health care, and technology companies establish and implement business-aligned cyber governance, risk management, and board reporting solutions.

MARK A. DELONG is a seasoned enterprise risk management leader. He has held chief operational risk officer and interim chief risk officer positions at Freddie Mac and was the chief audit executive at Huntington Banks. DeLong has been a key advisor to multiple Fortune 500 firms and brings a rich expertise in ensuring business growth by designing and implementing effective enterprise-wide integrated risk assessment methodologies and practices, three-lines-of-defense models and structures, and control optimization initiatives.