WEST

Summit & Awards

20 YEARS

Effective Cybersecurity Governance for Boards Navigating Risk and Ensuring Business Resilience

Myrna Soto

CEO & Founder Apogee Executive Advisors

Corporate Director Global CISO Emeritus

Keynote Presentation

Presentation Overview

- Changing Landscape in the Board Room (Cybersecurity & Enterprise Risk)
- Confirmed and Adopted SEC Rules regarding Cybersecurity(Board Governance)
  - Disclosure Requirements
  - Who , What and Why
- Protection - Resilience
- How you can elevate your engagement
  - Communicating Risk
  - Balanced Scorecard Approach
- Live Q&A

Introduction to Speaker

- 30 Year Technology Industry Veteran, Global CISO Emeritus (Comcast Corp, MGM Mirage Resorts, American Express etc) within Multiple Industries
- Fortune 50 Company experience – Large Scale Cybersecurity Program & Operational Experience
- Venture Capital & Private Equity Advisor/ Investor in Early-Growth Stage companies
- Corporate Director – Serving on the Boards for 4 publicly traded organizations most defined as Critical Infrastructure industries
- Serve on four privately held Boards and serve as a Board Advisor to multiple organizations
- Non-Profit Board Experience
- Recent Operational Executive for an MSSP & Chief Strategy & Trust Officer at a Cybersecurity Technology Provider
- Faculty member for NACD (National Association of Corporate Directors) , World50 and Athena Alliance
- Founder and CEO of Apogee Executive Advisors

My Personal Journey

Elevation of Cybersecurity in the Boardroom

- Boards are now paying attention to the need to participate in cybersecurity oversight. Not only are the consequences sparking concern, but the new regulations are upping the ante and changing the game
- Boards have a particularly important role to ensure appropriate management of cyber risk as part of their fiduciary and oversight role
- As cyber threats increase and companies worldwide bolster their cybersecurity budgets, the regulatory community, including the SEC, is advancing new requirements companies will need to know about as they reinforce their cyber strategy

Boards Taking Cybersecurity SERIOUSLY

Progress is being made – the numbers however still indicate more progress is needed

- 33% of board members believe the organization is at risk of a material cyber attack
- 75% of respondents felt the investment their organization has made in cybersecurity is adequate
- 70% cybersecurity is a top priority
- 76% reported that cybersecurity matters are discussed at every board meeting, or more often than that

However, research also uncovered attitudes and beliefs that must change

- Only 23% of board members think the risk of an attack on their organization is very likely
- About 47% believe their organization is unprepared for a cyber attack, begging the question “what are they doing about this?”
- 33% of board members say they interact with the CISO only when they are presenting to the board
- There is clearly room for improvement in aligning board members with the organization’s cybersecurity priorities

SEC Rules on Cybersecurity

WHO?

The SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule adopted July 26, 2023 impacts public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934.

THE RULE REQUIRES:

- Prompt reporting of "material cybersecurity incidents" within four (4) days of a materiality determination;
- Annual filings to include disclosures of material cybersecurity incidents;
- Companies to describe their processes for identification and management of cybersecurity risks;
- Description of management's role in implementing cybersecurity policies and procedures; and,
- Description of the board's oversight

CONFIRMED : SEC Regulations

Changing the Board's Role

Why:

The SEC hopes to provide investors with more timely and consistent disclosure regarding material cybersecurity incidents and greater availability and comparability of disclosure by public companies across industries of their cybersecurity risk management, strategy and governance practices in order to better assess the cybersecurity risk of said companies.

New SEC Regulations Have Changed the Board's Role

Disclosure requirements : Material Cybersecurity Incidents

"Material" – an incident would be material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available.

"Cybersecurity Incident" – means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrants information systems or any information residing therein.

The rule amends Form 8-K to require a registrant to disclose the following information about a material cybersecurity incident . The material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations

The incident must be disclosed within four business days after the registrant determines that it has experienced a material cybersecurtiy incident.

Determining the incident was "material" rather than the date of discovery is the triggering event to start the clock. The SEC expects registrants to be diligent in making a materiality decision as promptly as possible.

New SEC Regulations Have Changed the Board's Role

Disclosure Requirements : Duty to Update

- The Rule requires companies to update incident disclosures via an amended Form 8-K. Specifically, companies must:
- [File] a statement identifying any information called for [in Form 8-K] that is not determined or is unavailable at the time of the required filing and then file an amendment to its Form 8-K containing such information within four business days after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available.
- The Rule provides for a delay for disclosures that would pose a substantial risk to national security or public safety, contingent upon a written notification issued by the U.S. Attorney General.

New SEC Regulations Have Changed the Board's Role

Disclosure Requirements :Cybersecurity Risk Management, Strategy and Governance Disclosure

Risk Management Processes

The rule requires registrants to disclose:

- The registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes;
- Whether and how the described cybersecurity processes have been integrated into the registrant's overall risk management system or processes;
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and,
- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

New SEC Regulations Have Changed the Board's Role

Cybersecurity Risk Management, Strategy and Governance Disclosure

Governance

Regarding governance of its cybersecurity programs, the rules require management to disclose:

- the board's oversight of risks from cybersecurity threats
- identify any board committee or subcommittee responsible for such oversight,
- the processes by which the board or such committee is informed about such risks.

New SEC Regulations Board Oversight

Cybersecurity Risk Management, Strategy and Governance Disclosure : Things not in the Rules

- The SEC initially considered requiring one or more members of a company's board of directors to possess expertise in cybersecurity, and for the company to disclose the specifics of such expertise in its public filings. Ultimately the SEC did not adopt this requirement.
- Nonetheless, the SEC underscored that the board continues to be responsible for oversight of cybersecurity risk management.
- Given the more robust reporting requirements concerning cyber risk management processes, boards must have a meaningful ability to understand cybersecurity concepts and terminology in order to adequately exercise their oversight function.

New SEC Regulations : Action Steps

For Board Members (and the CISOs role in facilitating)

Review Current Cybersecurity Processes (Policies and Procedures):

- Are they clear in describing the assessment, identification and management of material risks from cybersecurity threats?
- Have they been integrated into the registrant's overall risk management system or processes?
- Does the company engage assessors, consultants, auditors, or other third parties in connection with any such processes?

Do they include oversight and identification of material risks from cybersecurity threats from any third-party service provider?

Work with the Board of Directors to:

- Ensure there is a process for reporting of cybersecurity risks and their ongoing oversight
- Document a process for the Board to follow for considering cybersecurity risks as part of its business strategy, risk management and financial oversight

Consult with Compliance and Legal regarding SEC Filings

Become familiar with the annual reporting requirements concerning risk management process and material incidents so that your company is ready when the deadlines arrive .

Fundamentals of Cyber Risk Governance

Board Member Fundamentals

Confirm that you can and they (Board Members) can affirmatively answer the following questions:

1. Has your organization met relevant statutory and regulatory requirements?

2. Has your organization quantified its cyber exposures and tested its financial resilience ?

3. Does your organization have an improvement plan in place to ensure exposures are within your agreed-upon risk appetite?

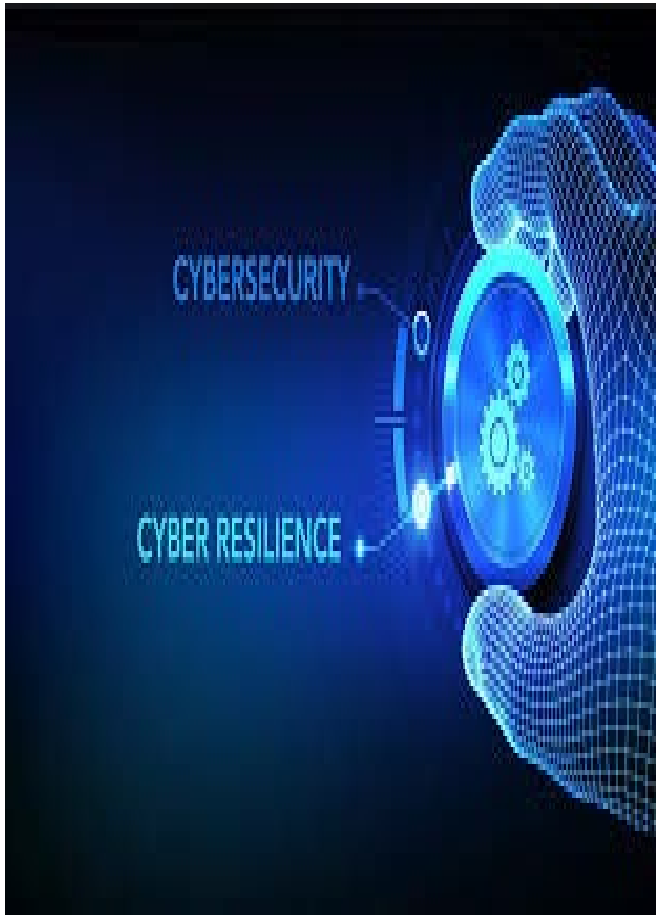
4. Does the board regularly discuss concise, clear, and actionable information regarding the organization's cyber resilience supplied by management?

5. Does your organization have incident response plans in place that have been recently dry-run exercised, including at board-level?

6. Are the roles of key people responsible for managing cyber risk clear and aligned with the three lines of defense?

7. Have you obtained independent validation and assurance of your organization's cyber risk posture?

The Right Conversation : Resilience



Boards are having the wrong conversation (some of them…..) steer the conversation in the Board Room

- Board interactions with the CISO are lacking
- Boards have been focused on protection when they need to focus on resilience
- Boards view cybersecurity as a technical topic, but it has become an organizational and strategic imperative
- The composition of most boards today creates additional vulnerability when it could create stronger oversight
- Failing to show that cybersecurity is a priority for the board sends an unwanted message

Cyber Resilience is the top Priority

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges.

Instead of only focusing on digging deeper fortifications to keep the risks out, business leaders would do well to build their resilience from the inside. The most effective way to achieve this by setting the tone at the top, and supporting employees with skills, tools and a culture that empowers cyber resilience.

What your Presentation Material Should Cover

Help them answer these key questions: The board needs to explore these questions on on a regular basis include:

- What are the "crown jewels" of the organization?
  You can't effectively protect everything. So, which assets are priorities?
- What are the organization's most significant vulnerabilities? Answers will range from employees' digital habits to security tech stacks to weak points in the digital supply chain.
- What is our financial exposure?
  The conversation will likely focus on ransomware and cyber-insurance to start. But it needs to evolve to an understanding of brand risk, impact on innovation and — of course — the ability to drive new growth.
- What is the long-term goal of our cybersecurity efforts?

While defending against the thousands of threats attacking your networks every day, the real goal needs to be on building the trust to manage the organizations highest risks.

Don't show performance indicators to the board; show them KRI's

Evaluating your Presentation Materials

- From my work, I see that a change in mindset from protection to resilience is needed and to drive that change, operational leaders must change how they report to the board.
- Managers focus on measures taken for cyber protection, but boards need to know about cyber resilience. Managers think their boards want to know about operational metrics, but directors really want to know the business risks the managers anticipate and what action plan is in place to mitigate the risk.
- Managers report on metrics they can calculate, but boards need a broader assessment of where the next cyber issue might occur and those might not be quantifiable. Directors need information about the business impact of the cyber risks, both from a risk-identification and a risk-likelihood perspective.
- Qualitatively reporting the general business risks from cyber threats and vulnerabilities in the context of how it might disrupt the organization, and discussing the importance of the risk with the board enables directors to assess if attention is placed on the right risks and mitigation strategies.

Evaluating your Presentation Materials

- Cyber risk is dynamic. What is a risk today may not be a risk tomorrow, or it might be the biggest risk tomorrow. To make that assessment, boards want to have the right conversations with those who know both the cyber risk and the business impact of that risk.
- It's not really about how protected we are, but how resilient we are.
- A Balanced Scorecard for Cyber Resilience is the starting place for the discussions about how the business will continue operations when an event occurs.

Reporting Capabilities

Develop a balanced Scorecard Reporting Mechanism for your Board

- Performance indicators from different perspectives of the company that provide leaders with complex information that is easily understood.
- The main purpose of their scorecard was to provide insight into financial and operational performance by combining information about core activities that might otherwise be isolated from each other.
- By looking at these indicators together in a single framework, the leaders are able to draw conclusions that might otherwise be missed. Our work extended these ideas into the cybersecurity realm to provide insight to boards about cyber resilience.

Board level balanced scorecard for cyber resilience combines financial, technological, organizational, and supply-chain indicators, and an aggregated indicator of resilience.

Mechanisms to Facilitate said reporting …….

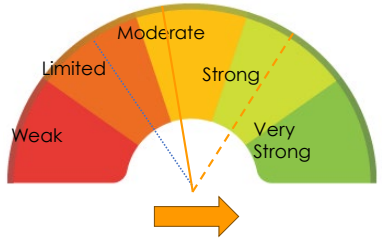
Critical Security Capabilities

Example Only
Data Has been Manufactured for presentation purposes

Example Only

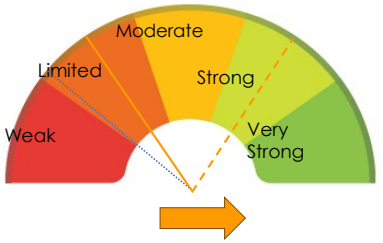
KEY SUMMARY:

- **Cyber Readiness** improved due to enhancement initiatives, including blocking access to third-party personal webmail and multi-factor authentication for privileged accounts on servers. Actions are underway to get certain consolidated gap action plans back on-track.
- **Product Security** improved due to continued remediation of Top 10 risk action plans.
- **Third Party** improved due to expanding the phishing training and awareness program to contingent workers and mitigation activities related to the Log4j vulnerability remediation.
- **Governance & Compliance** significantly improved from Limited to Moderate due to establishing new capabilities to validate control operating effectiveness and ensure controls are incorporated into new enterprise projects prior to go-live.
- **Resiliency** improved due to enhancements to the Business Continuity Management Program, including automation of planning and recovery workflows. A feasibility assessment is underway for implementing a process to fully restore from backup to reduce ransomware risk.
- **Physical Security & Safety** improved due to implementation of CLEAR for colleague vaccination tracking, as well as ongoing enhancements to physical security incident management.



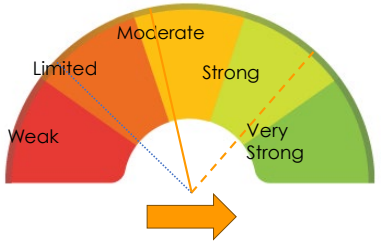
Category	Status
KRI Action Plans	Y
Consolidated Gap Action Plans	Y
Maturity Action Plans	G →
Risk Action Plans	G
Penetration Test Action Plans	G
Phishing Simulations	G
Technology Implementation	G
Staffing	G →

Governance & Compliance



Category	Status
KRI Action Plans	G →
Consolidated Gap Action Plans	G
Maturity Action Plans	G →
Risk Action Plans	G →
Penetration Test Action Plans	G
Staffing	G →

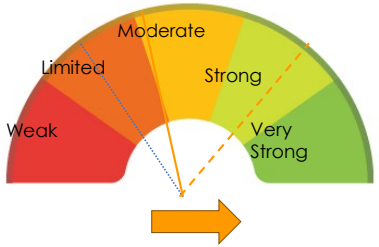
Resiliency



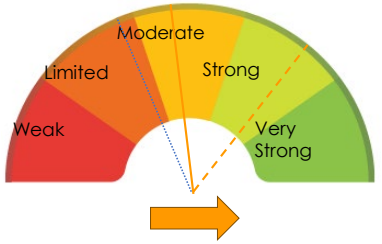
Category	Status
KRI Action Plans	G
Consolidated Gap Action Plans	G
Maturity Action Plans	G
Risk Action Plans	G
Technology Implementation	G
Staffing	G

NEW Q3 2023!

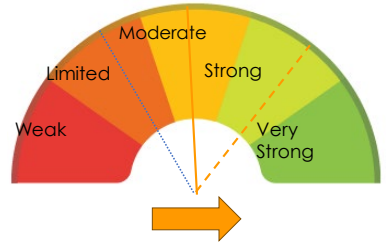
Physical Security & Safety



Category	Status
KRI Action Plans	G
Consolidated Gap Action Plans	G
Maturity Actions Plans	G →
Risk Action Plans	G
Staffing	G



Category	Status
KRI Action Plans	G
Consolidated Gap Action Plans	G
Maturity Action Plans	G
Risk Action Plans	Y
Staffing	G



Category	Status
KRI Action Plans	TBD
Consolidated Gap Action Plans	G
Maturity Action Plans	G
Risk Action Plans	G
Staffing	G

What Can you do ?
How to Increase Expertise in your Board Room

Increase Cybersecurity Expertise in your Boardroom

- Develop a common language for discussing the complex issues of cyber risk and resilience
- Keep cyber resiliency on the board's agenda and in discussions with management
- Build wider bridges between cybersecurity executives and board members
- Embrace and engage 3rd Party Ecosystem – leverage these partners in the Board Room

Navigating the Board Conversation

Ways to galvanize your role with the Board and prepare for a potential board role in the future

- C-Level Tools that focus on investments (ROI of Investments, Program ROI or Ways to Measure Business Value) *
- Learn the principles of ERM – this is the language of Board Members (Cyber Risk should be incorporated)
- Position yourself as a Business Leader, who just happens to be a technical leader as well – not visa versa Business Leadership
- Build and Leverage Internal Comms
- Metrics Measures Dashboards