Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.

© Clearwater Compliance | All Rights Reserved

Not intended for public release

CLEARWATER

Monthly Cyber Briefing

March 2023

Moderator: Jenny Davis

© Clearwater Compliance | All Rights Reserved

A Healthcare Cybersecurity & Compliance Industry Leader Focused on One Mission

We enable our clients to achieve their missions by moving them to a more secure, compliant, and resilient state.

- Award-winning cybersecurity and compliance consulting, outsourced managed services, and software focused on the healthcare ecosystem
- 500+ customers across the healthcare ecosystem including major hospital systems, large physician practice groups, digital health, medtech, and payors
- 200+ colleagues with 100+ expert cybersecurity & privacy consultants in U.S.
- Tech-enabled 24x7x365 Security Operations Center with Managed Detection & Response (MDR) Services
- Proprietary IRM|Pro® SaaS-based software platform enables efficient identification and management of cybersecurity and compliance risks
- Certified HITRUST Assessor & first approved Certified Third-Party Assessment Organization in the Cybersecurity Maturity Model Certification (CMMC) program
- Rapidly growing and profitable portfolio company of Altaris Capital Partners, a healthcare PE firm with more than $5B under management

CLEARWATER

Along with our wholly owned subsidiaries

CYNERGISTEK
A Clearwater Company

TECH LOCK
A Division of Clearwater

Redspin
A Division of Clearwater

© Clearwater Compliance | All Rights Reserved

CLEARWATER
CYNERGISTEK
A Clearwater Company
TECH LOCK
A Division of Clearwater

Not intended for public release

Logistics

- ✓ All attendees in “Listen Only Mode”
- ✓ Please ask content related questions in **“Q&A”**
- ✓ Please complete the **Exit Survey** when you leave
- ✓ **Cyber Briefings are now eligible for HIMSS & CHIME CE credit**
- ✓ **Recording & final slides housed on the On Demand page within 48 hours**

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Mac McMillan
Founder & Advisor
CynergisTek, a Clearwater Company

Bob Chaput
Founder & Executive Chairman
Clearwater

Ralph Davis
Senior Operating Partner
The Vistria Group, LP

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Cyber Update

Mac McMillan

Cyber Events Have Business Impacts

Personal Liability:

FTC holds CEO of Drizly LLC **personally liable f**or company's failure to implement appropriate security measures. Former UBER CSO found guilty of **criminal obstruction and concealment** of a felony for failing to report a major breach.

Lost Clients/Lost Revenue:

Multiple **clients move away from** Kronos software following massive breach affecting thousands of companies and millions of people. Software company Logicgate suffers third party breach resulting in **partners losing clients.**

Financial Impacts:

Yahoo agrees to **$35M penalty** from SEC for failure to disclose serious cyber incident. Employees at Tesla and PepsiCo file **class action lawsuit** against Kronos. ElektroMed, iCare Acquisition, Scripps Health, Morley Companies all reach **settlements between $825K and $4.3M** from cyber events.

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Expectations Have Changed

Federal Trade Commission

- Prioritize security and privacy as a Business Area
- Implement Bottom-Up Internal Processes and Documentation
- Focus on Data Minimization, Deletion, and Retention

Security Exchange Commission

- Cybersecurity now directly links to financial performance.
- Boards and Directors will be directly responsible for cybersecurity.
- Greater focus on financial impact of cybersecurity, updated DoJ whistleblower reporting incentives.
- Executive Bonuses have a return policy if regulatory filings are misstated.

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Corporate Cyber Responsibility

- **VISIBILITY**: Simply put, the individual responsible for cyber security should be visible to the Board.
- **CULTURE**: Expressed another way how important is cyber to the organization.
- **LEADERSHIP**: Those things that Executive management do and stand for are valued and emulated.
- **PRIORITY:** Adequate resources are given to those things consider business essential.

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Effective Enterprise Cyber Risk Management (ECRM) Board Discussions

Presenters

Bob Chaput

Founder, Executive Chairman

- Author, Cyber Coach, Board Advisor
- Faculty Member - IANS
- Part-time Faculty - Quinnipiac University
- Board Advisor – KSU Institute for Cybersecurity Workforce Development

Ralph Davis

Senior Operating Partner

- Senior Operating Partner with The Vistria Group, LP
- Senior executive and serial board member/advisor

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Session Objectives – Attendees Will Be Able to:

1. Explain key subtopics to be considered in each board/investor discussion of ECRM
2. Cite “Guiding Principles for Board-Level Metrics”
3. Discuss why it’s important to discuss overall ECRM program advancement in each board meeting
4. Describe what constitutes appropriate and effective board member education activities

© Clearwater Compliance | All Rights Reserved

Three Main Board Oversight Responsibilities

CEO and Team | Strategy | Risk Management

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Refresh on Risk

"The possibility that events will occur and affect the achievement of strategy and business objectives."

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1]

"A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs, and (ii) the likelihood of occurrence.

- The National Institute of Standards and Technology (NIST)[2]

[1]COSO. "COMPLIANCE RISK MANAGEMENT: APPLYING THE COSO ERM FRAMEWORK." November 2020. Available at https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

[2]"Risk." Glossary. Computer Security Resource Center (CSRC). National Institute of Standards and Technology (NIST). Accessed January 13, 2023. Available at https://csrc.nist.gov/glossary/

© Clearwater Compliance | All Rights Reserved

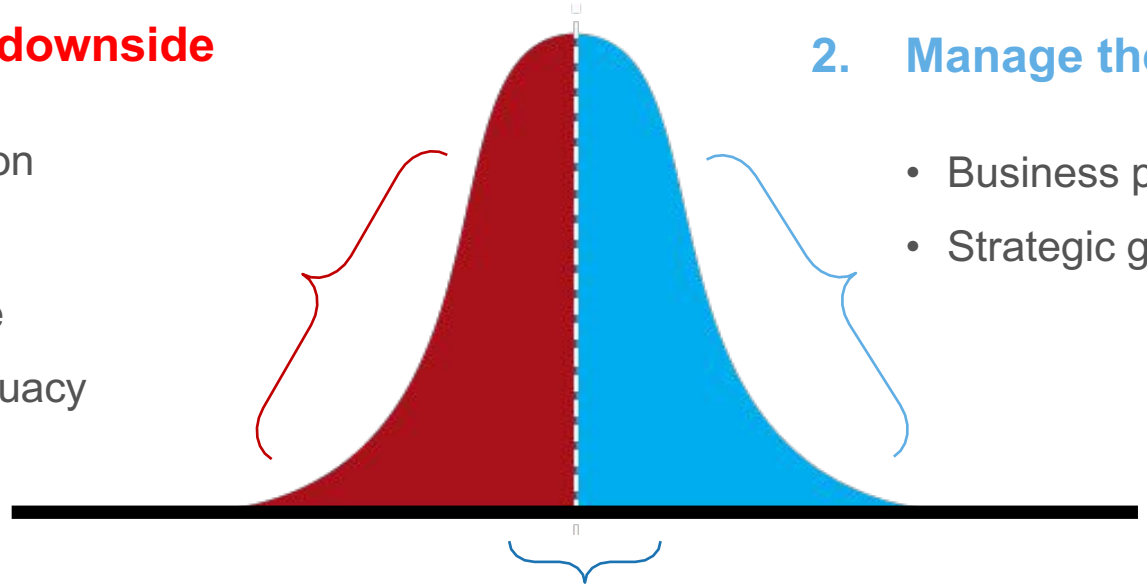
Not intended for public release

Risk Management Is About Optimizing the Bell Curve[1]

2. Manage the downside

- Risk mitigation
- Risk transfer
- Risk appetite
- Capital adequacy

Cyber



2. Manage the upside

- Business plan execution
- Strategic growth & innovation

1. Manage the expected

- Risk acceptance/avoidance
- Pricing for the cost of risk

[1]National Association of Corporate Directors (NACD) presents in Module 9 of its Virtual Director Professionalism program. Virtual Director Professionalism. National Association of Corporate Directors. n.d., Accessed January 25, 2023. Available at https://www.nacdonline.org/events/detail.cfm?ItemNumber=74119

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Mosaic of Business Risks – C-Suite, Boards, and Investors Must Consider

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Ideal Board Meeting Agenda for ECRM

1. Risks and Treatment
2. Program Advancement
3. Current Events and Board Education

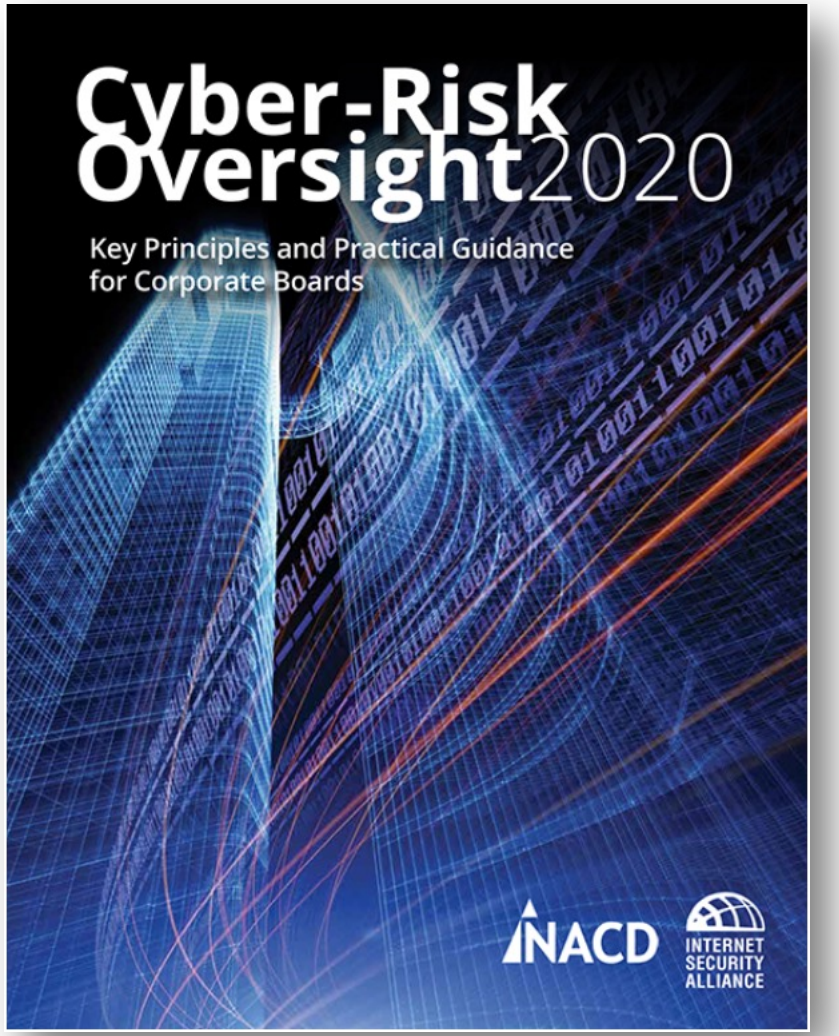
Depending on Program Maturity,
Meet Up to 90 minutes

© Clearwater Compliance | All Rights Reserved

CLEARWATER
CYNERGISTEK. A Clearwater Company
TECH LOCK® A Division of Clearwater
Not intended for public release

NACD/ISA Guiding Principles for Board-Level Metrics

- Be relevant to the audience (full board; key committee)
- Be reader-friendly: use summaries, callouts, graphics, and other visuals, and avoid technical jargon
- Convey meaning: communicate insights, not just information
  - Highlight changes, trends, and patterns over time
  - Show relative performance against peers, against industry averages, against other relevant external indicators, etc. (e.g., maturity assessments)
  - Indicate impacts on business operations, costs, market share, etc.
- Concise: Avoid information overload
- Above all, enable discussion and dialogue



© Clearwater Compliance | All Rights Reserved

CLEARWATER
CYNERGISTEK. A Clearwater Company
TECH LOCK A Division of Clearwater
Not intended for public release

1. Risk Analysis

A. How many total risks (number) have been identified in your risk register?

B. What percentage of the risks you have identified have been given risk ratings?

C. What is your categorization of risk from most serious to least serious? (i.e., what are the respective percentages of critical risks, high risks, medium risks, and low risks?)

D. What does your risk rating look like when broken down by media/asset-component group? (e.g., laptops, electronic medical devices, desktops, servers, etc.) Which of these media/asset-components show the highest average risk rating?

E. What are the top five vulnerabilities identified in your risk analysis?

F. Has your organization completed a risk analysis that will be acceptable to OCR?

© Clearwater Compliance | All Rights Reserved

Not intended for public release

2. Risk Appetite

A. What is the percentage of risks above your threshold (risk appetite)?

B. What is the number of risks above your threshold (risk appetite)?

C. Which of your entities/facilities are showing the largest number of risks above your organization's risk appetite?

D. Which of your media/asset groups are showing the largest number of risks above your risk appetite?

3. Risks Treatment

A. What is your current process to conduct risk treatment?

B. Who is authorized to make what risk treatment decisions, using what data and facts?

C. Have you documented your current risk treatment plan?

D. Would it be advantageous to contract with a third-party to develop a risk treatment plan?

E. If you have already contracted with a third-party for this task, what are the highlights of the current risk treatment plan of which the board should be aware?

F. Has your organization developed a risk treatment or risk management plan that will be acceptable to OCR?

© Clearwater Compliance | All Rights Reserved

Not intended for public release

ECRM Subtopic 2: ECRM Program Advancement

Status of Strategic Objectives

A. The strategic ECRM objective description, including costs and expected benefits

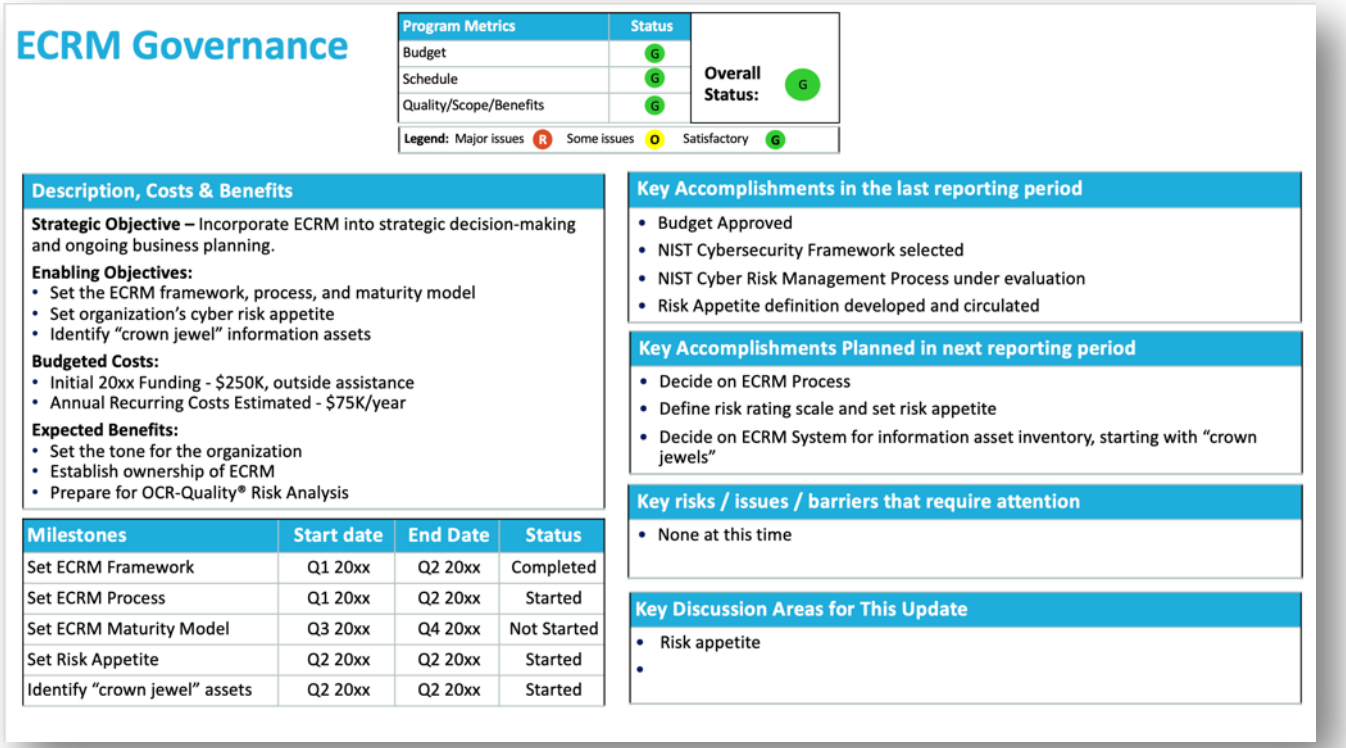
B. Enabling objectives, including target completion date, expected completion date, and current status

C. Key accomplishments toward achieving this objective during the last reporting period

D. Planned accomplishments for the next reporting period

E. Key issues, risks, and barriers that require board attention

F. Key discussion areas for this update



ECRM Governance

Program Metrics	Status
Budget	G
Schedule	G
Quality/Scope/Benefits	G

Overall Status: G

Legend: Major issues R Some issues O Satisfactory G

Description, Costs & Benefits

Strategic Objective – Incorporate ECRM into strategic decision-making and ongoing business planning.

Enabling Objectives:
- Set the ECRM framework, process, and maturity model
- Set organization's cyber risk appetite
- Identify "crown jewel" information assets

Budgeted Costs:
- Initial 20xx Funding - $250K, outside assistance
- Annual Recurring Costs Estimated - $75K/year

Expected Benefits:
- Set the tone for the organization
- Establish ownership of ECRM
- Prepare for OCR-Quality® Risk Analysis

Milestones	Start date	End Date	Status
Set ECRM Framework	Q1 20xx	Q2 20xx	Completed
Set ECRM Process	Q1 20xx	Q2 20xx	Started
Set ECRM Maturity Model	Q3 20xx	Q4 20xx	Not Started
Set Risk Appetite	Q2 20xx	Q2 20xx	Started
Identify "crown jewel" assets	Q2 20xx	Q2 20xx	Started

Key Accomplishments in the last reporting period
- Budget Approved
- NIST Cybersecurity Framework selected
- NIST Cyber Risk Management Process under evaluation
- Risk Appetite definition developed and circulated

Key Accomplishments Planned in next reporting period
- Decide on ECRM Process
- Define risk rating scale and set risk appetite
- Decide on ECRM System for information asset inventory, starting with "crown jewels"

Key risks / issues / barriers that require attention
- None at this time

Key Discussion Areas for This Update
- Risk appetite
-

One-Page Update for Each of Governance, People, Process, Technology, Engagement

© Clearwater Compliance | All Rights Reserved

Not intended for public release

ECRM Subtopic 3: ECRM-Relevant Current Events and Board Education

1. ECRM-relevant Current Events

A. Internal incidents
B. High-profile external events
C. Significant global, federal, state, or local regulatory changes
D. ECRM-related competitor moves
E. Significant changes to the threat landscape

2. Board Education

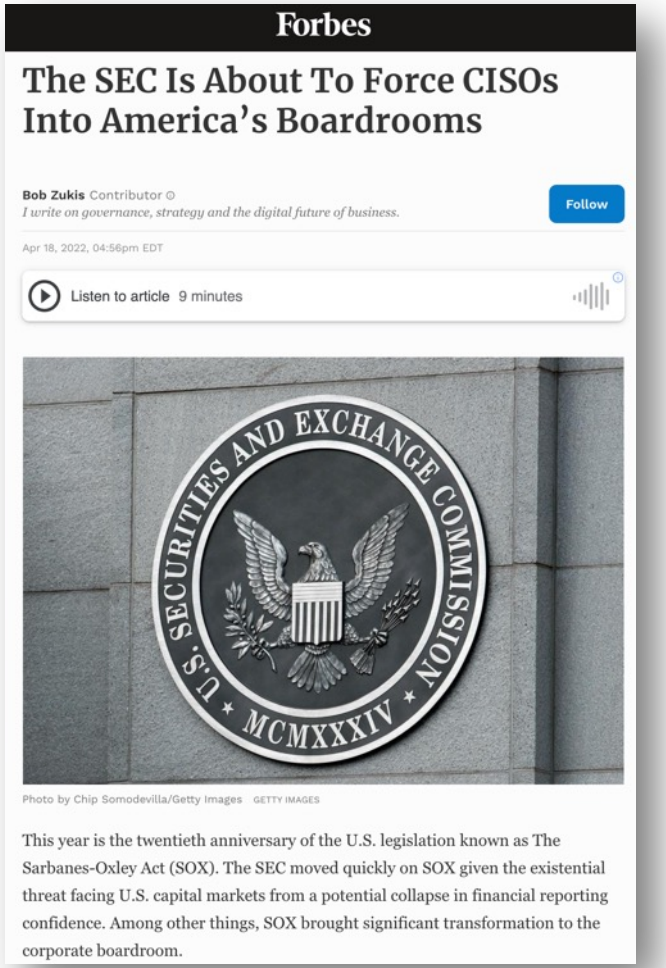
A. ECRM 101
B. In-depth briefings by outside experts
C. Outside counsel - legal implications of a breach
D. Executive risk insurance broker - potential gaps, clashes, and redundancies
E. Outside and inside experts - forecast of the cyber risk landscape, one, three, and five years out
F. FBI representatives or OCR staff - healthcare cyber risk environment
G. Briefing on the NACD Cyber-Risk Oversight Certificate
H. Briefing on the NIST Cybersecurity Framework

© Clearwater Compliance | All Rights Reserved
Not intended for public release

Board Engagement Will Increase

"Cybersecurity is already among the top priorities of many boards of directors and cybersecurity incidents and other risks are considered one of the largest threats to companies. Accordingly, ***investors may find disclosure of whether any board members have cybersecurity expertise to be important as they consider their investment in the registrant as well as their votes on the election of directors of the registrant.***

We propose to amend Item 407 of Regulation S-K by adding paragraph (j) to ***require disclosure about the cybersecurity expertise o****f members of the board of directors of the registrant, if any. If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise."*



Forbes

The SEC Is About To Force CISOs Into America's Boardrooms

Bob Zukis Contributor
I write on governance, strategy and the digital future of business.

Follow

Apr 18, 2022, 04:56pm EDT

Listen to article 9 minutes

Photo by Chip Somodevilla/Getty Images GETTY IMAGES

This year is the twentieth anniversary of the U.S. legislation known as The Sarbanes-Oxley Act (SOX). The SEC moved quickly on SOX given the existential threat facing U.S. capital markets from a potential collapse in financial reporting confidence. Among other things, SOX brought significant transformation to the corporate boardroom.

Zukis, Bob. Forbes. "The SEC Is About To Force CISOs Into America's Boardrooms". April 18, 2022. *Available at* https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/

SEC. "Proposed Rule Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure". March 9, 2022. Available at https://www.sec.gov/rules/proposed/2022/33-11038.pdf

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Mac McMillan

Bob Chaput

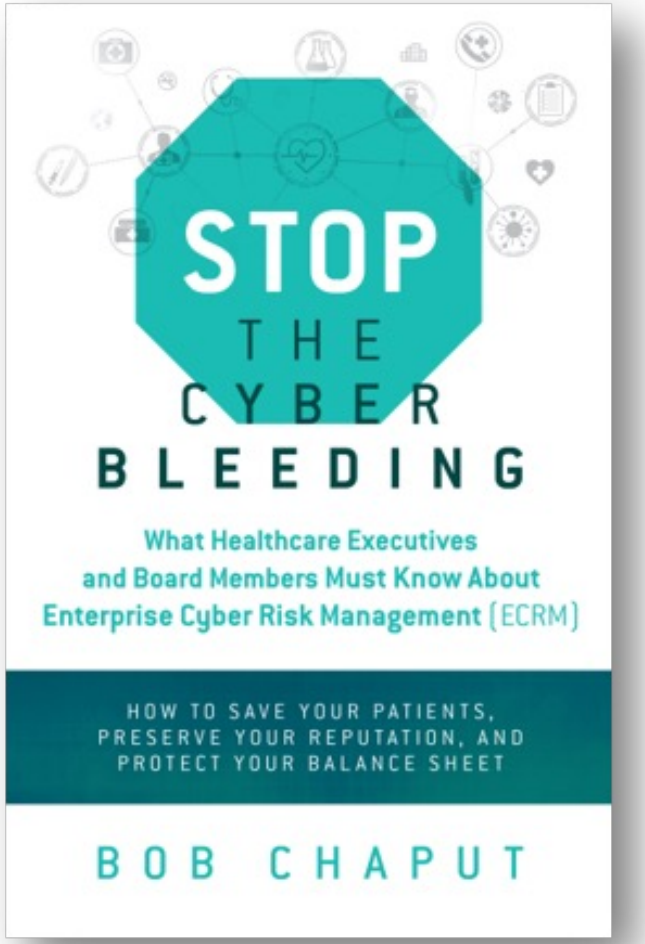
Ralph Davis

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Additional Educational Resources…

[A Must-Watch Series for Healthcare Leaders]



Available in digital, paperback, &, audio format.

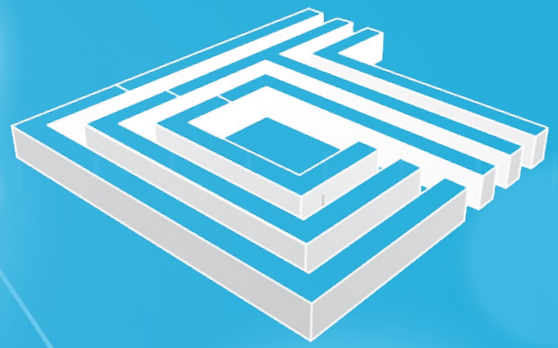
https://amzn.to/33qr17n

© Clearwater Compliance | All Rights Reserved

Not intended for public release

CLEARWATER

HEALTHCARE CYBER RISK MANAGEMENT



CYNERGISTEK

A Clearwater Company

TECH LOCK®

A Division of Clearwater

© Clearwater Compliance | All Rights Reserved

Backup Slides

Session Objectives

1. Recommend how often and for how long a Board or Board committee should meet on ECRM
2. Discuss who should lead the ECRM agenda item Board discussion
3. Explain three key subtopics that should be covered in each board discussion of ECRM
4. Cite five (5) “Guiding Principles for Board-Level Metrics” from NACD’s Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards
5. Explain why it is important to discuss overall ECRM program advancement in each board meeting
6. Identify and explain the three (3) important discussion questions under ECRM Risks and Treatment subtopic
7. Provide 3-5 examples of appropriate and effective board member education activities/topics

© Clearwater Compliance | All Rights Reserved

Where is Your C-suite and Board on ECRM?

The superior man, when resting in safety, does not forget that danger may come. When in a state of security, he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come.

—Confucius

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Who Should Lead the Board Discussion of Cyber Risk?

Recommended Meeting Schedule

TIER	BODY	MEMBERS	FUNCTION	ECRM MEETING FREQUENCY
1	*Full board* or designated board committee (e.g., *Audit & Compliance Committee* or a specific *ECRM Oversight Council*)	Full board or designated committee	Sets direction and provides oversight.	Quarterly
2	*ECRM Executive Steering Committee*	CEO + his/her full team	Ensures execution of the ECRM program.	Monthly
3	*ECRM Cross-Functional Working Group*	May include legal, risk management, finance, HR, audit, compliance, privacy, IT, clinical engineering, security, quality, and/or others.	Executes the steps to establish, implement, and mature the ECRM program.	Several times per month

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Global Risks Report 2023

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period"

"Global Risks Report 2023." World Economic Forum/PwC. Jan. 11, 2023. Available at https://www.weforum.org/reports/global-risks-report-2023/

© Clearwater Compliance | All Rights Reserved

Not intended for public release

Risk Examples

Strategic	Operations	Environmental	Financial	Legal	Reputational
Loss of market share due to increased competition	Unable to retain customers	Recession	Inability to pay down or refinance debt	HIPAA Violation	Data breach
Loss of market share due to industry consolidation	Unable to maintain acceptable profitability	Inability to recover from business interruption	Inability to maintain internal controls	ERISA Violation	Inaccurate Financial Reporting
Loss of market share due to increased in-sourcing	Unable to execute on contracts	Unable to recover from disaster	Inability to forecast accurately	FTC Violation	Loss of Credentialing
Unsuccessful integration of acquisitions	Unsuccessful at commercializing new services	Unable to fend off collective bargaining	Financial misstatement	AHRQ Violation	Incompetent Staff
Loss of market share due to service obsolescence	Unable to gain efficiencies	Unfavorable Change in Regulations	Unfavorable Impact of Foreign Exchange	Whistleblower	Disclosure of Non-Public Information

© Clearwater Compliance | All Rights Reserved

Not intended for public release