Stop the Cyber Bleeding:

What Healthcare Executives and Board Members Must Know about Enterprise Cyber Risk Management

A Governance Institute Webinar

presented by

Bob Chaput, MA, CISSP, HCISPP, CRISC, C|EH, CIPP/US, NACD
CERT Cyber Risk Oversight
Executive Chairman & Founder, Clearwater

June 30, 2021

Today's Presenter

Bob Chaput, MA, CISSP, HCISPP, CRISC, C|EH, CIPP/US, NACD CERT Cyber Risk Oversight
Executive Chairman & Founder, Clearwater

- Executive | Educator | Entrepreneur | Expert Witness | Author
- Leading authority on healthcare compliance, cybersecurity, and ECRM
- 40+ years in business, operations, technology, and cyber risk management
- 25+ years in healthcare
- Contributing author to Wolters Kluwer's *Health Law and Compliance Update* and the American Society of Healthcare Risk Management (ASHRM)'s *Health Care Risk Management Fundamentals*
- Global Healthcare Executive: GE, JNJ, HWAY
- Prior responsibility for some of largest, most sensitive healthcare datasets in world
- Industry expertise and focus: healthcare covered entities and business associates
- Member: NACD, IAPP, ISC^2, CHIME/AEHIS, HIMSS, ISSA, IAPP, ISACA, HCCA
- Author: *Stop The Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)*

Learning Objectives

After viewing this Webinar, participants will be able to:

Define Enterprise Cyber Risk Management (ECRM) and its importance

List three essential ECRM tasks the board must oversee

Discuss five essential ECRM capabilities your organization must build

Identify innovative sources of funding for your ECRM program

Describe requirements to management for an ideal ECRM board discussion

Continuing Education

Continuing education credits available

IPCE CREDIT™

In support of improving patient care, The Governance Institute, a service of National Research Corporation, is jointly accredited by the Accreditation Council for Continuing Medical Education (ACCME), the Accreditation Council for Pharmacy Education (ACPE), and the American Nurses Credentialing Center (ANCC) to provide continuing education for the healthcare team. This activity was planned by and for the healthcare team, and learners will receive 1 Interprofessional Continuing Education (IPCE) credit for learning and change.

AMA: The Governance Institute designates this live activity for a maximum of ***1 AMA PRA Category 1 Credit(s)™***. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

ACHE: By attending this Webinar offered by The Governance Institute, a service of National Research Corporation, participants may earn up to **1 ACHE Qualified Education Hour** toward initial certification or recertification of the Fellow of the American College of Healthcare Executives (FACHE) designation.

Criteria for successful completion: Webinar attendees must remain logged in for the entire duration of the program. They must answer at least three polling questions. They must complete the evaluation survey in order to receive education credit. Evaluation survey link will be sent to all registrants in a follow-up email after airing of the Webinar.

CPE: The Governance Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its Web site: www.nasbaregistry.org.

NATIONAL REGISTRY OF CPE SPONSORS

In accordance with the standards of the National Registry of CEP Sponsors, CPE credits will be granted based on a 50-minute hour.
Field of study: Business Management & Organization
Program level: Overview
Prerequisites: None
Advanced preparation: None
Delivery method: Group Internet based
Maximum potential CPE credits: 1

Disclosure Policy

- As a Jointly Accredited Provider, the Governance Institute's policy is to ensure balance, independence, objectivity, and scientific rigor in all of its educational activities. Presentations must give a balanced view of options. General names should be used to contribute to partiality. If trade name are used, several companies should be used rather than only that of a single company. All faculty, moderators, panelists, and staff participating in the Governance Institute conferences and Webinars are asked and expected to disclose to the audience any real or apparent conflict(s) of interest that may have a direct bearing on the subject matter of the continuing education activity. This pertains to relationships with pharmaceutical companies, biomedical device manufacturers, or other corporations whose products or services are related to the subject matter of the presentation topic. Significant financial interest or other relationships can include such thing as grants or research support, employee, consultant, major stockholder, member of the speaker's bureau, etc. the intent of this policy is not to prevent a speaker from making a presentation instead, it is the Governance Institute's intention to openly identify any potential conflict so that members of the audience may form his or her own judgements about the presentation with the full disclosure of the facts.
- It remains for the audience to determine whether the presenters outside interests may reflect a possible bias in either the exposition or the conclusion presented. In addition, speakers must make a meaningful disclosure to the audience of their discussions of off-label or investigational uses of drugs or devices.
- All faculty, moderators, panelists, staff, and all others with control over the educational content of this Webinar have signed disclosure forms. The planning committee members have no conflicts of interests or relevant financial relationships to declare relevant to this activity. *The presenter has no financial relationship with The Governance Institute or its parent company, NRC Health.*
- This educational activity does not include any content that relates to the products and/or services of a commercial interest that would create a conflict of interest. There is no commercial support or sponsorship of this conference.
- None of the presenters intend to discuss off-label uses of drugs, mechanical devices, biologics, or diagnostics not approved by the FDA for use in the United States.

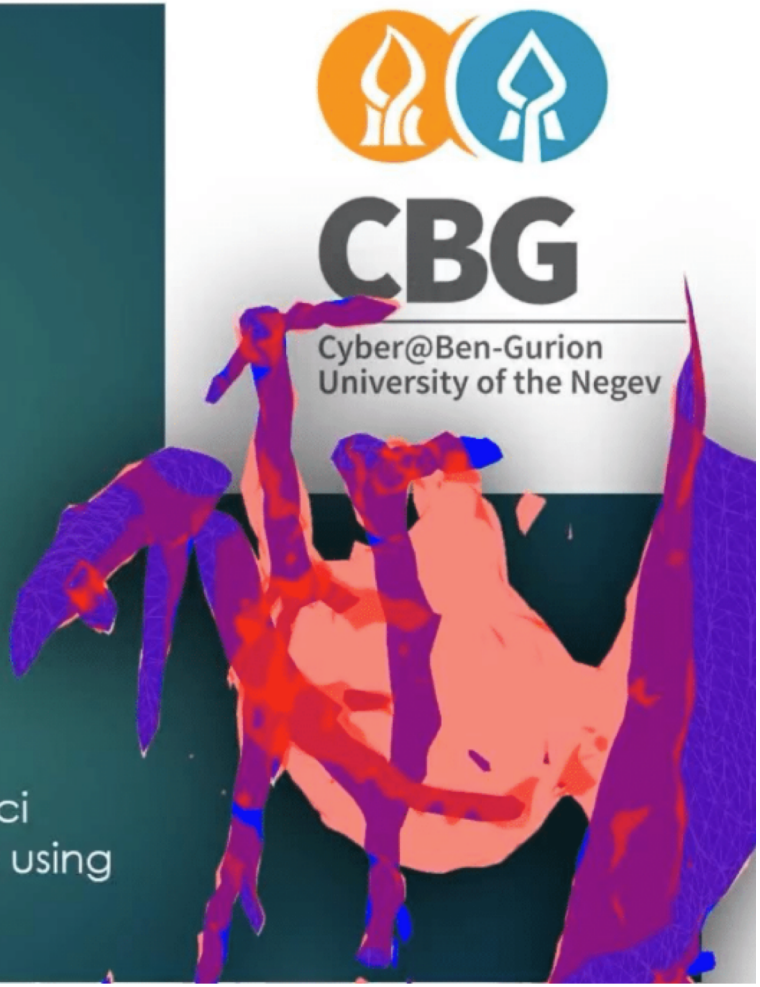
Discussion Flow

1. **Enterprise cyber risk management (ECRM) – what and why?**
2. Three essential ECRM tasks for the board
3. Five essential ECRM capabilities
4. Innovative sources of ECRM funding
5. An ideal ECRM board discussion

Demonstration:
Injecting and Removing Lung Cancer from CT Scans

Corresponding Author: Yisroel Mirsky
yisroel@post.bgu.ac.il

Full paper:
Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici
CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. https://arxiv.org/abs/1901.03597



https://www.youtube.com/watch?v=_mkRAArj-x0

The First Cyber-Driven Hospital Malpractice Lawsuit?


DAILY NEWS

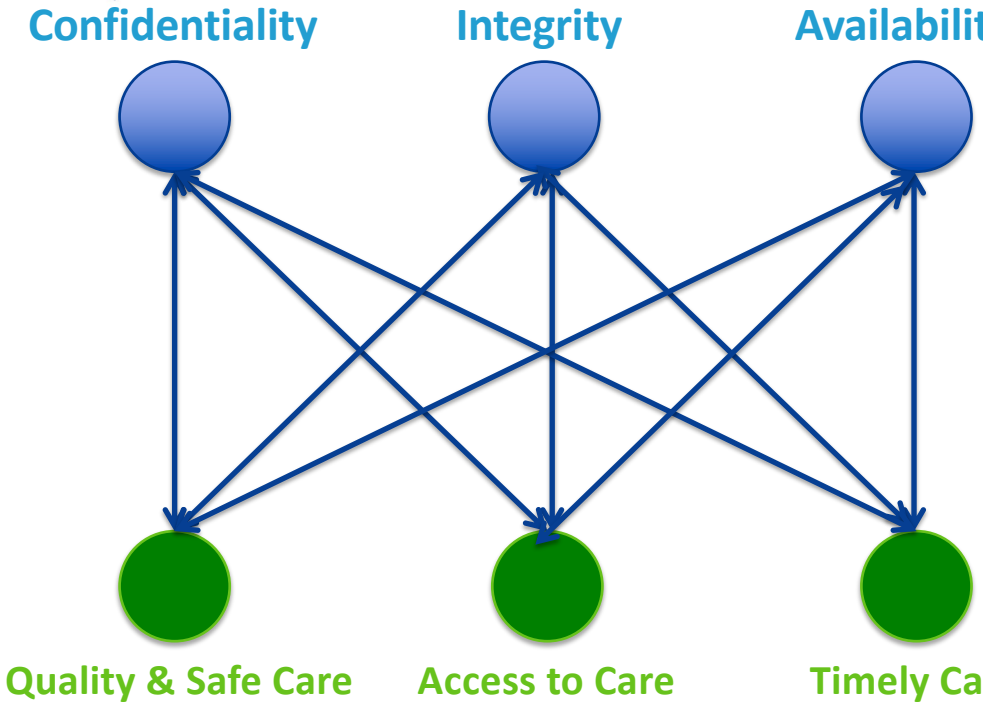
No. 49,725 THE BEST SELLING NEWSPAPER IN THE WORLD Today's Edition

National - World - Business - Lifestyle - Travel - Technology - Sport - Weather

Hacked CT Image at Gotham Memorial Results in Cancer Misdiagnosis and Death

Clinician / Executive / Board Duty of Care & HIPAA Reasonable Diligence?

Connect the Dots!



Data, Systems, & Devices…AND Patient Safety & MPL

Source: *Connecting the Dots Between Cyber Risk and Patient Safety*, https://clearwatercompliance.com/knowledge-center/white-papers/cyberse...

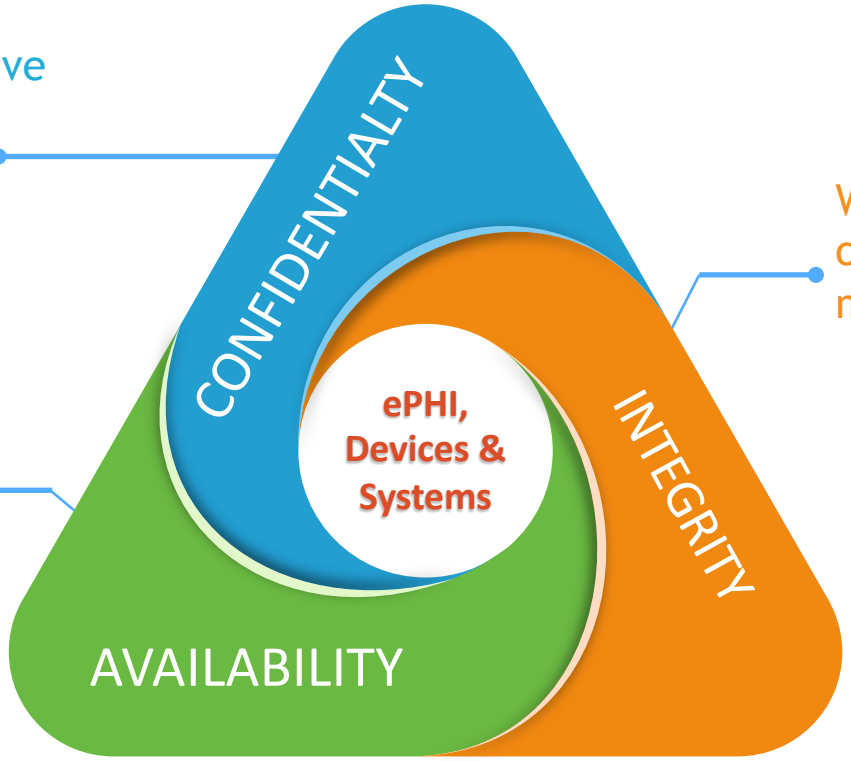
Risk Fundamentals

Our Core Cyber Risk Responsibility

What if my sensitive information is impermissibly disclosed?

What if data, systems or devices have been modified?

What if data, systems, or devices are not there when it is needed?



Don't allow compromise C-I-A!

Patient Safety – Quality of Care – Patient Satisfaction Issues

Bad Things Emanating from COMPROMISE OF		
CONFIDENTIALITY	**INTEGRITY**	**AVAILABILITY**
Identity Theft	Incorrect Diagnosis	Delayed Admission
Reputational Damage	Incorrect Treatment	Delayed Diagnosis
Relationship Damage	Incorrect Prescriptions	Delayed Surgery
Employment Damage	Incorrect Billing Charges	Delayed Prescriptions
Financial Damage	Contaminated Clinical Trial	Delayed Discharge
Anxiety	Identity Theft	Diagnosis Errors
Depression	Reputational Damage	Treatment Errors
Suicide	Death	Death

Remember the Importance of Safeguarding C-I-A

Bottom Line: ECRM is…

Not an "IT Problem"…

ECRM is assuring the **confidentiality, integrity,** and **availability** of all healthcare data, systems, and devices throughout the enterprise…

…in order to ensure our patients receive quality and safe care, and are assured access to care in a timely manner.

Polling Question #1

For risk to exist, all three of the following ingredients must be present:

a. Confidentiality, integrity, and availability
b. Quality care, access to care, and timely care
c. Asset, threat, and vulnerability
d. Reputation, finances, and regulations

Discussion Flow

1. Enterprise cyber risk management (ECRM) – what and why?
2. **Three essential ECRM tasks for the board**
3. Five essential ECRM capabilities
4. Innovative sources of ECRM funding
5. An ideal ECRM board discussion

Three Critical Tasks for Board to Oversee

1. Prioritize your unique cyber risks.
2. Set your appetite for cyber risk.
3. Manage each risk.

Sample Risk Register and Risk Appetite

Generally, **Avoid, Mitigate or Transfer**

Generally, **Accept**

Asset	Threat Source / Action	Vulnerability	Likelihood	Impact	Risk Rating
Laptop	Burglar steals laptop	No encryption	High (5)	High (5)	**25**
Laptop	Burglar steals laptop	Weak passwords	High (5)	High (5)	**25**
Laptop	Burglar steals laptop	No tracking	High (5)	High (4)	**20**
Laptop	Careless user drops	No data backup	Medium (3)	High (5)	**15**
Laptop	Shoulder surfer views	No privacy screen	Low (1)	Medium (3)	**3**
Laptop	Lightning strike	No surge protection	Low (1)	High (5)	**5**
Etc.					

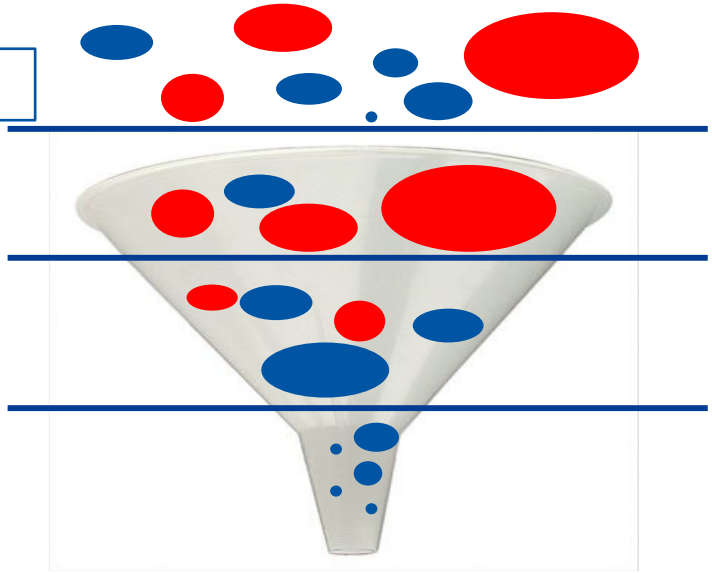
Classic Cyber Risk Management Choices

Risks of all types & sizes exist

Risk Identification ➔

Risk Treatment

- Avoid / transfer risks
- Mitigate / transfer risks
- Accept risks



Risk management is making informed decisions on how to treat risks.

Polling Question #2

When treating or managing risks, after accepting risks, the three classic remaining choices are:

a. Avoid, accept, or transfer
b. Mitigate, transfer, or avoid
c. Accept, avoid, or mitigate
d. Analyze, accept, or avoid

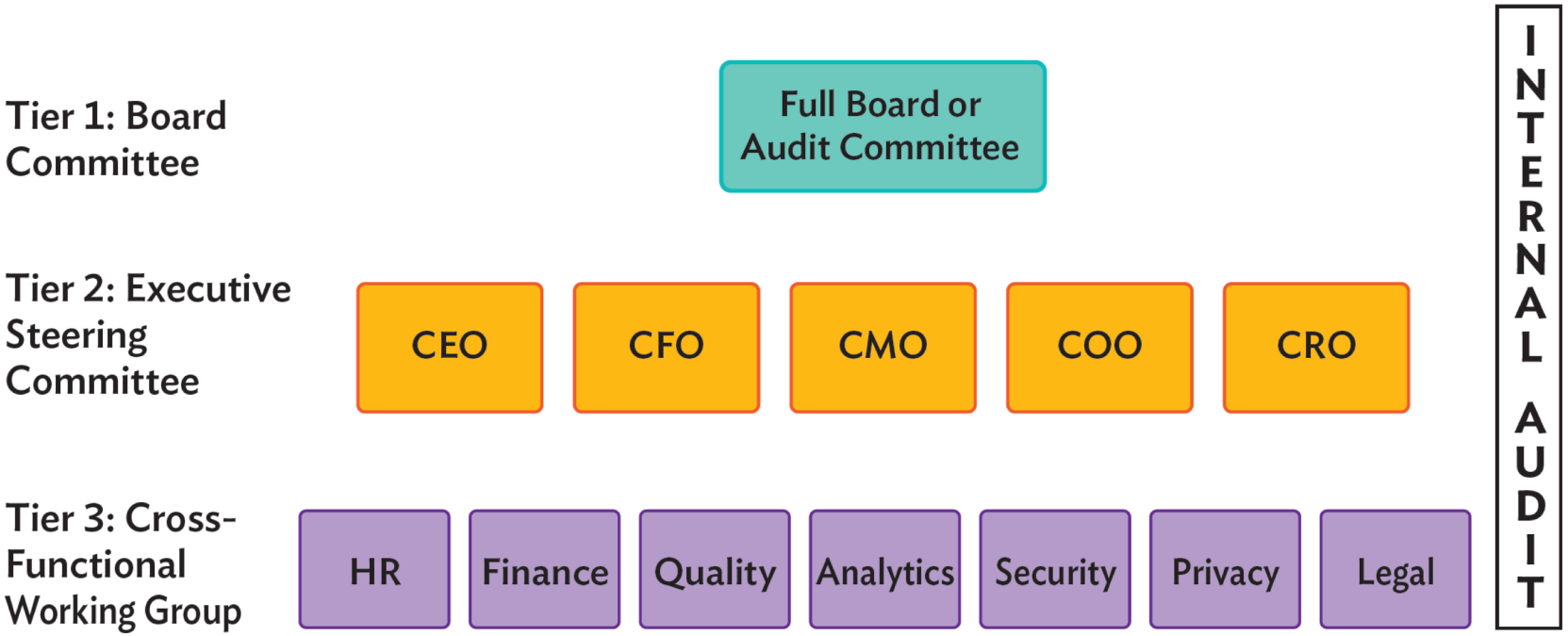
Discussion Flow

1. Enterprise cyber risk management (ECRM) – what and why?
2. Three essential ECRM tasks for the board
3. **Five essential ECRM capabilities**
4. Innovative sources of ECRM funding
5. An ideal ECRM board discussion

Essential ECRM Capabilities

1. **Governance** *(benefits and value)*
2. **People** *(skills, knowledge, & culture)*
3. **Process** *(discipline & repeatability)*
4. **Technology** *(tools and scalability)*
5. **Engagement** *(delivery & operations)*

Example of Three-Tiered ECRM Governance Structure



Source: Bob Chaput, *Stop the Cyber Bleeding*, 2020.

Discussion Flow

1. Enterprise cyber risk management (ECRM) – what and why?
2. Three essential ECRM tasks for the board
3. Five essential ECRM capabilities
4. **Innovative sources of ECRM funding**
5. An ideal ECRM board discussion

Regarding Cyber Risk Management…

I have written in previous letters about the enormous effort and resources we dedicate to protect ourselves and our clients—we spend nearly $600 million a year on these efforts and have more than 3,000 employees deployed to this mission in some way. Indirectly, we also spend a lot of time and effort trying to protect our company in different ways ***as part of the ordinary course of running the business****.*

— Jamie Dimon, Chairman & CEO, JPMorgan Chase
April 2019 Letter to Shareholders

Sources of ECRM Funding

Lower Cost of Capital

Reduced Insurance Premiums

Captive Insurance Grants

Source: Bob Chaput, *Stop the Cyber Bleeding*, 2020.

Polling Question #3

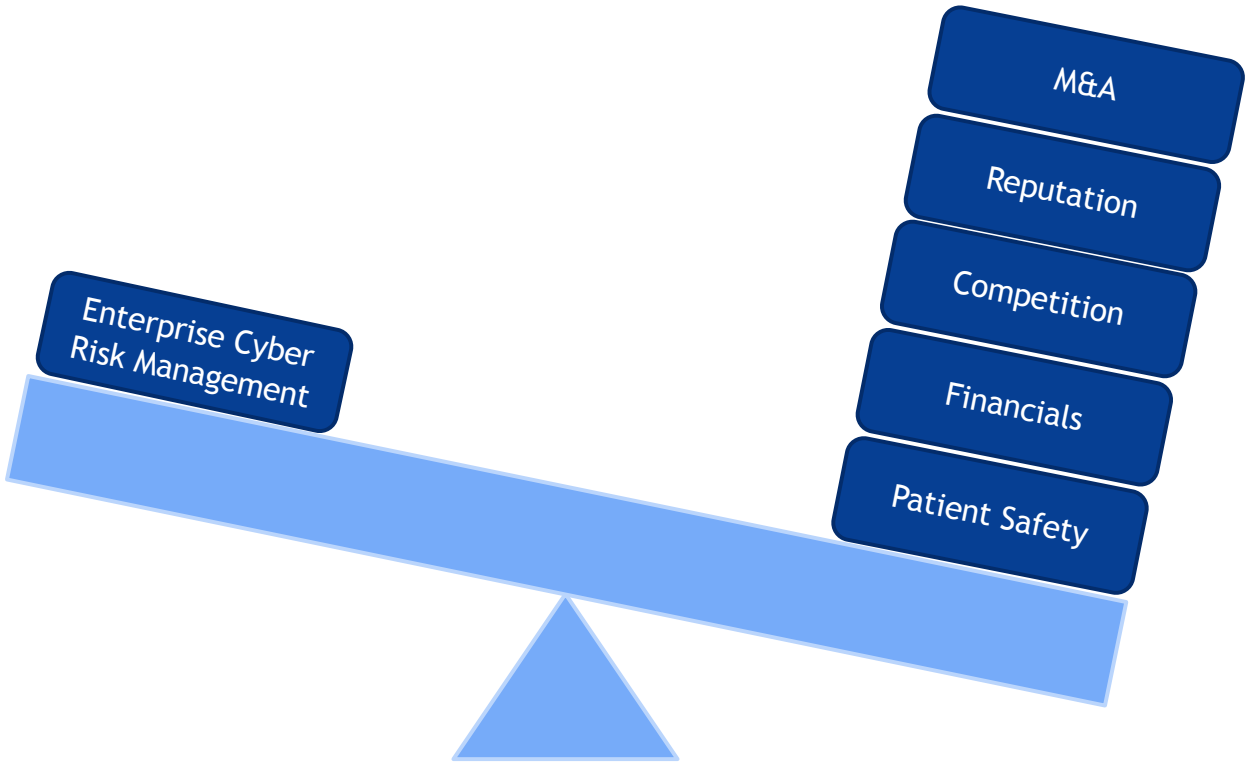
True or False: Healthcare organizations may use grants from their captive insurance company to jump-start their ECRM program.

a. True
b. False

Discussion Flow

1. Enterprise cyber risk management (ECRM) – what and why?
2. Three essential ECRM tasks for the board
3. Five essential ECRM capabilities
4. Innovative sources of ECRM funding
5. **An ideal ECRM board discussion**

Lever and Elevate the ECRM Discussion

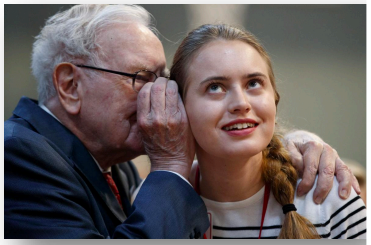


Discuss ECRM in the Context of…

Patient Safety, Quality of Care

Financials / Protecting the Balance Sheet

Non-Traditional, Disruptive Competition



Reputation

M&A Activities

Ideal Board Meeting Agenda for ECRM

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

Polling Question #4

Enterprise cyber risk management should be discussed in the context of:

a. M&A activities
b. Patient safety, quality of care
c. Reputation
d. Competition
e. All of the above

Final Thoughts

1. **Strategically**, insist on talking business; set the tone.
2. **Tactically**, require building your ECRM *program* (not undertaking a *project*) by adopting NIST-based approaches.
3. **Operationally**, ensure an OCR-Quality® Risk Analysis, starting with your "crown jewels."

Questions & Discussion

Contact Us…

Bob Chaput
Executive Chairman & Founder
Clearwater
(615) 496-4891
bob.chaput@clearwatercompliance.com

CLEARWATER
HEALTHCARE CYBER RISK MANAGEMENT

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

The Governance Institute
1245 Q Street
Lincoln, NE 68508
(877) 712-8778
Info@GovernanceInstitute.com

References

Chaput, Bob. *Enterprise Cyber Risk Management: A Toolbook for Healthcare Boards and Executives*, The Governance Institute, 2021.

Chaput, Bob. *Stop the Cyber Bleeding*. 2020.

Dimon, Jamie. "CEO Letter to Shareholders, 2018." JPMorgan Chase, April 4, 2019.

Mirsky, Yisroel, Tom Mahler, Ilan Shelef, and Yuval Elovici. "CT-GAN: Malicious tampering of 3D medical imagery using deep learning." 28th USENIX Security Symposium (USENIX Security 19), 461–478. 2019.