The 405(d) Program

Aligning Health Care Industry Security Approaches

Healthcare's Enterprise Cyber Risk Management:

How to engage the C-suite and Board in cyber risk management discussions

August 12,2021

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by different 405(d) Task Group members; each iteration does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

* This Webinar is being recorded and will be available for future viewing

405(d) Events and Announcements

September

- National Preparedness Month!
- 405(d) Post Volume XII release 9/16

October

- National Cybersecurity Awareness Month!
- 405(d) Spotlight Webinar- More details to come!

November

- 405(d) Post Volume XIII release 11/18

Email: CISA405d@hhs.gov

Agenda

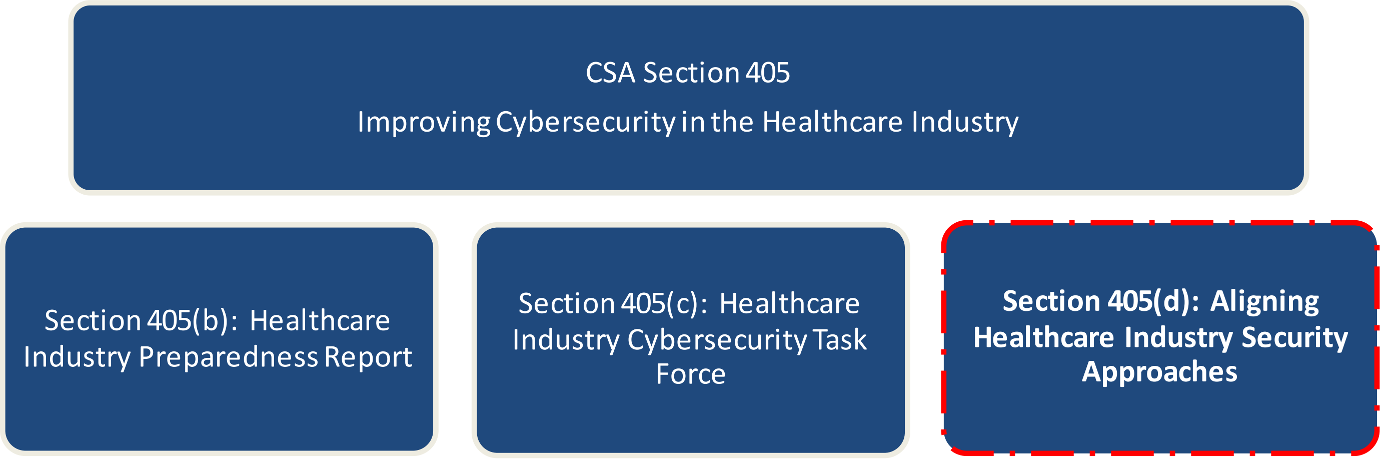
Time	Topic	Speaker
10 minutes	Opening Remarks and Introductions	Julie Chua, HHS
40 Minutes	Healthcare's Enterprise Cyber Risk Management	Bob Chaput, Ralph Davis
10 Minutes	Q&A	All
5 Minutes	Closing	405(d) Team

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



CSA Section 405

Improving Cybersecurity in the Healthcare Industry

Section 405(b): Healthcare Industry Preparedness Report

Section 405(c): Healthcare Industry Cybersecurity Task Force

Section 405(d): Aligning Healthcare Industry Security Approaches

405(d) Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over 50 awareness products which organizations across the HPH sector can leverage

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present on new and emerging cybersecurity news and topics, as well highlighting the HICP Publication!

CYBERSECURITY TOWN HALL EVENT

October 22-23

PATIENTS TRUST US WITH THEIR LIVES,
BUT DO WE PROTECT THEM FROM CYBER THREATS?

Join UChicago Medicine and United States Health and Human Services 405(d) to discuss the five main cybersecurity threats facing the healthcare industry and leading practices to mitigate them.

Town Hall Events:
Practitioners and Practice Managers:
10/22/19 1:30pm-3:00pm
10/23/19 9:00am-10:30am

IT Professionals:
10/22/19 3:30pm-5:00pm
10/23/19 11:00am-12:30pm

Telework During COVID-19
Good Practices To Protect From Cyberattacks
By Sekar Thanigaimani, 405(d) Task Group Member

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

NEW RESOURCES ALERT

405(d) "That Seems Risky" Campaign

405(d) Cybersecurity "Myth vs. Fact" Campaign

Today’s Presenters

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
- Author: *Stop The Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM)*
- Leading authority on healthcare compliance, cybersecurity, and ECRM
- 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

Ralph Davis, JD, BA

Senior Advisor and Operating Partner, The Vistria Group

- Serial healthcare board member / advisor
- Board Member and Investor - ThriveAP
- Board Advisor - Audit Compliance & Quality Committee Chairman/Member
  - Help at Home
  - Mission Healthcare
  - Medalogix
  - FullBloom
  - The Mentor Network
- Board Member - Audit Compliance and Quality Committee Chairman
  - Agape Care Group
  - Rock Dental Brands
  - Behavioral Health Group
  - HomeFree Pharmacy

Healthcare's Enterprise Cyber Risk Management:

How to engage the C-suite and Board in cyber risk management discussions

Learning Objectives

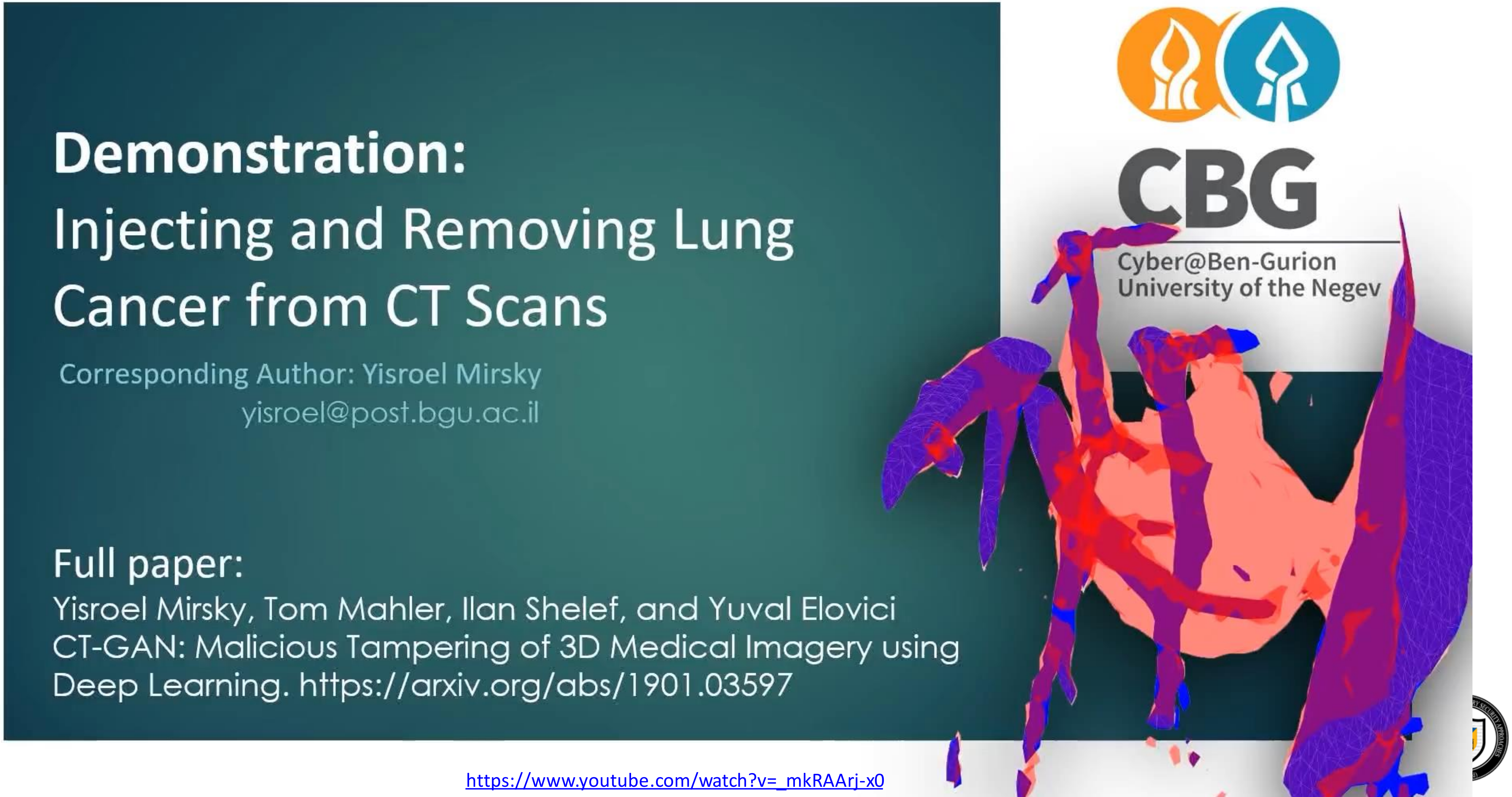
After viewing this Webinar, participants will be able to:

- **Discuss Enterprise Cyber Risk Management (ECRM) basics with the Board and C-Suite**
- **Discuss ECRM in business context**
- **Conduct a balanced business discussion about funding for your ECRM program**

Discussion Flow

1. **Basics**
2. Business
3. Budget

The Real Problem We’re Trying to Solve



Demonstration:

Injecting and Removing Lung Cancer from CT Scans

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

Full paper:

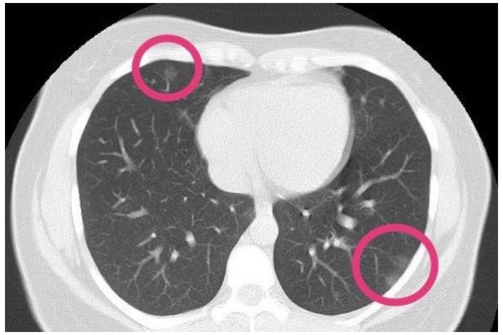
Yisroel Mirsky, Tom Mahler, Ilan Shelef, and Yuval Elovici
CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. https://arxiv.org/abs/1901.03597

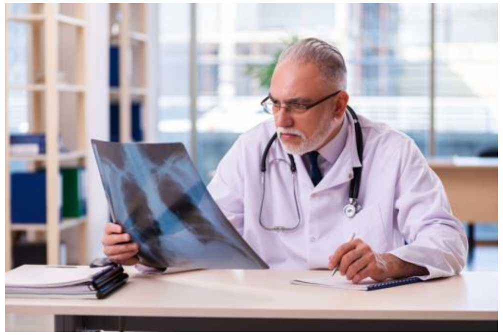
https://www.youtube.com/watch?v=_mkRAArj-x0

When Something "Cyber" Happens

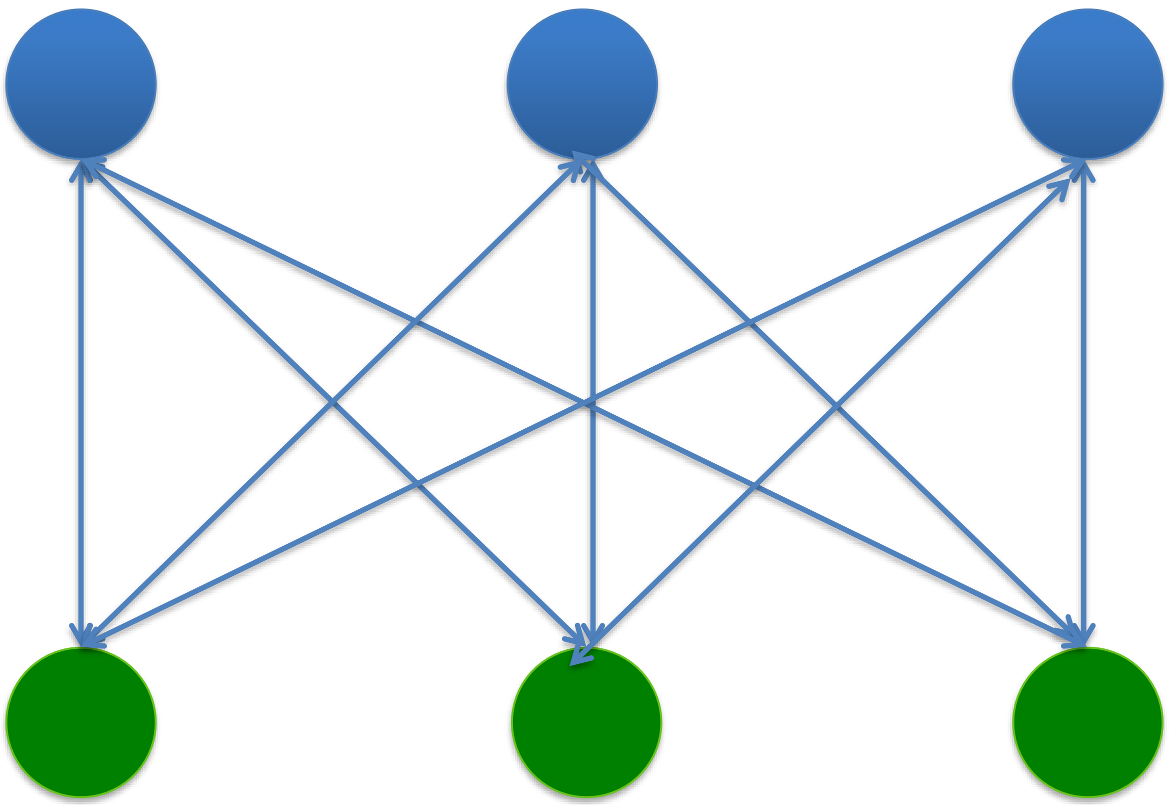
Three bad things have happened here…

- Hacked
- Compromised Integrity of CT scan images
- Fooled expert radiologists





Connect the Dots!



Confidentiality

Integrity

Availability

Quality & Safe Care

Access to Care

Timely Care

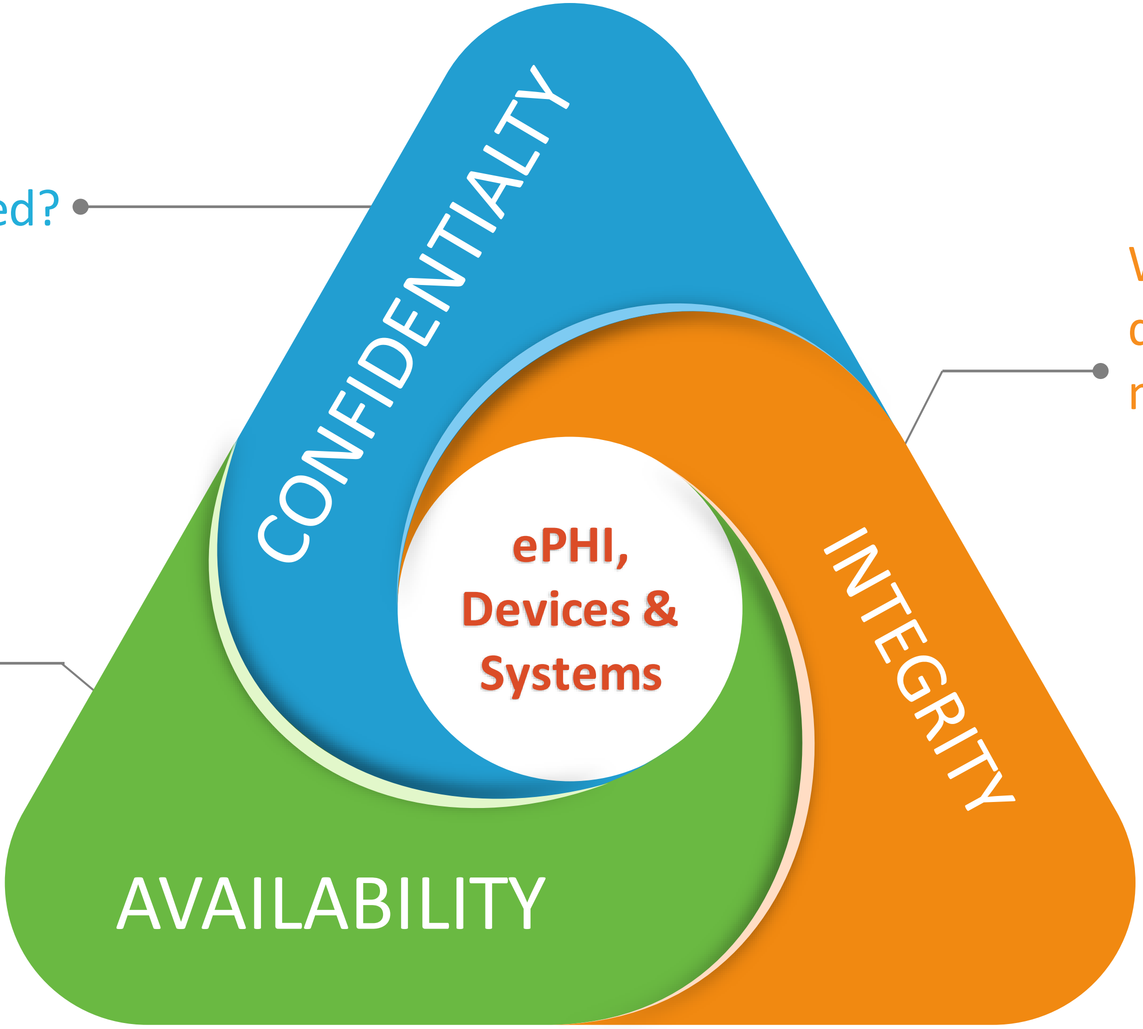
Data, Systems, & Devices…AND Patient Safety & MPL

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

Our Core Cyber Risk Responsibility

What if my sensitive information is impermissibly disclosed?

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



What if data, systems or devices have been modified?

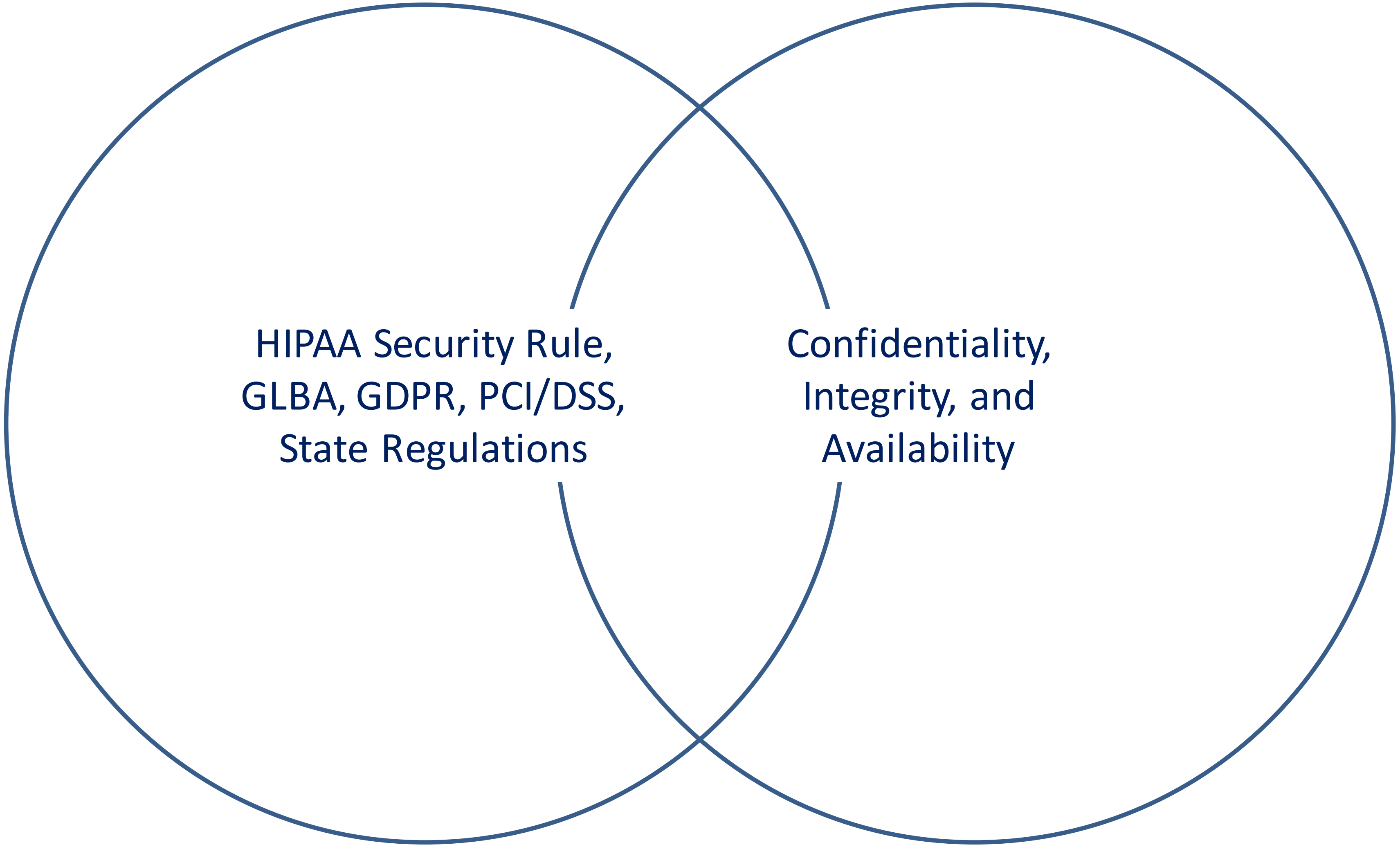
Don’t allow compromise C-I-A!

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

Compliance or Security?



HIPAA Security Rule, GLBA, GDPR, PCI/DSS, State Regulations

Confidentiality, Integrity, and Availability

Bottom Line: ECRM is…

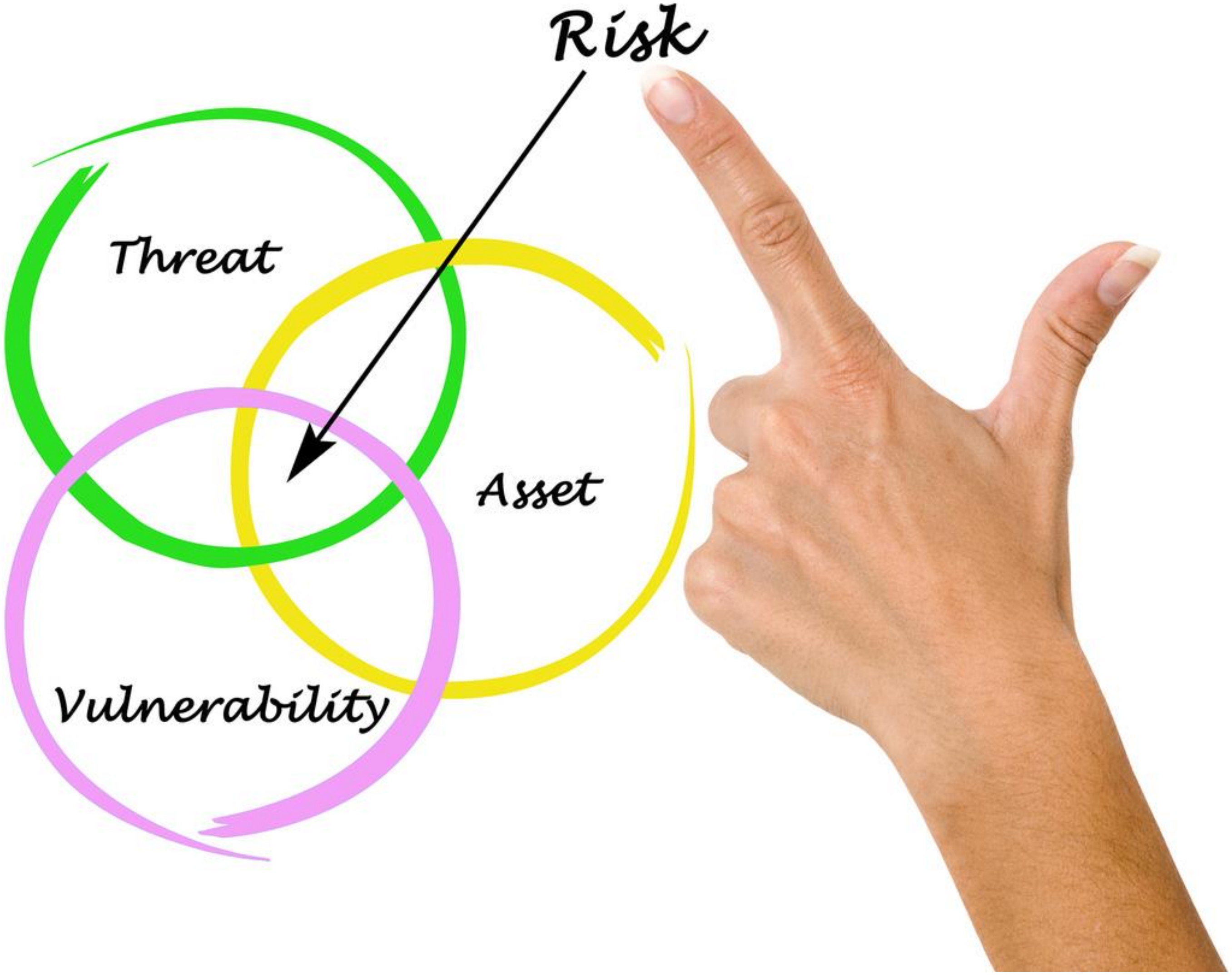
Not an "IT Problem"…

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.

Must Take a Risk-Based Approach

Risk Fundamentals



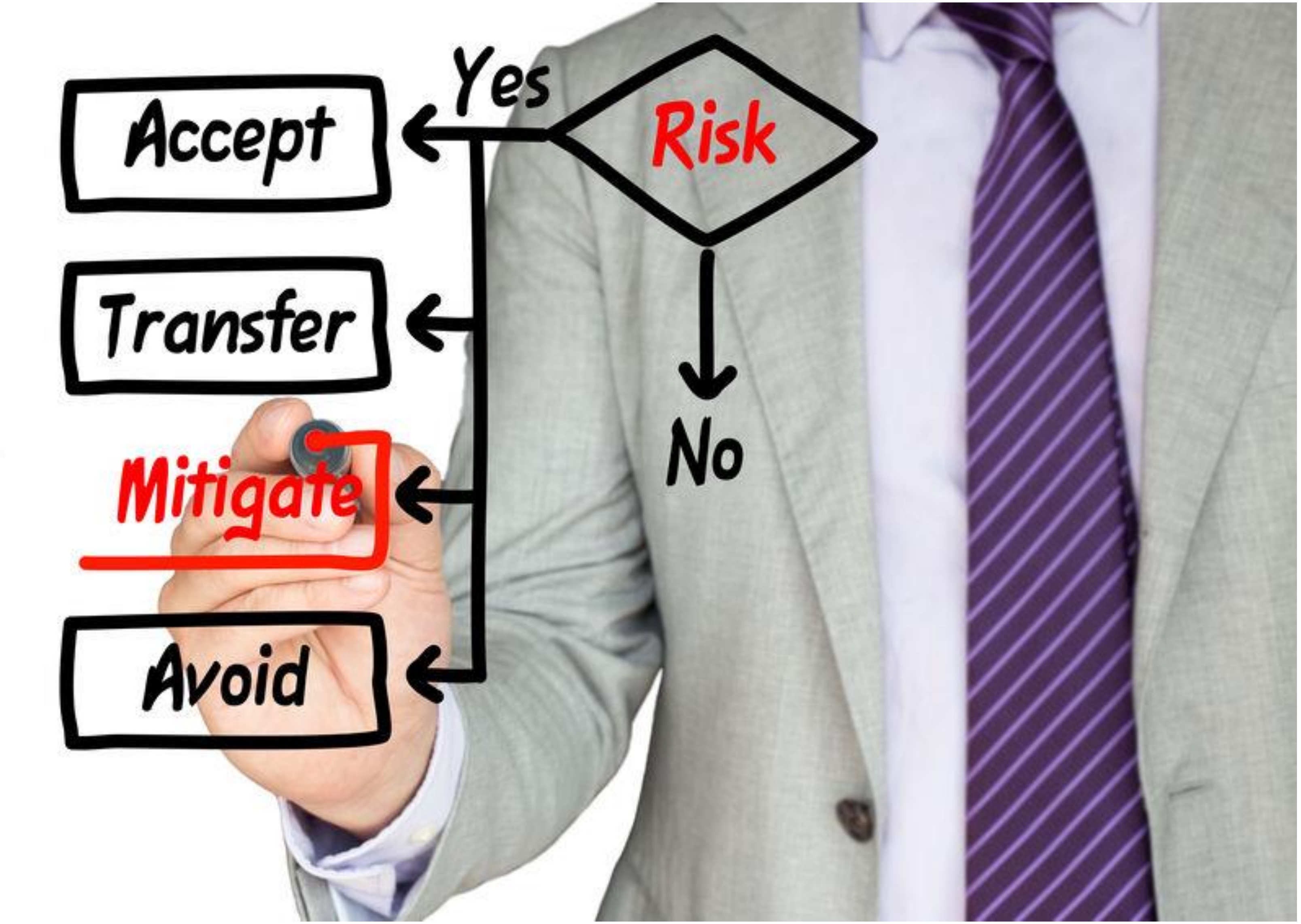
Sample Risk Register and Risk Appetite

***Generally,* Avoid, Mitigate or Transfer**

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.					

***Generally,* Accept**

OCR-Quality® Risk Management

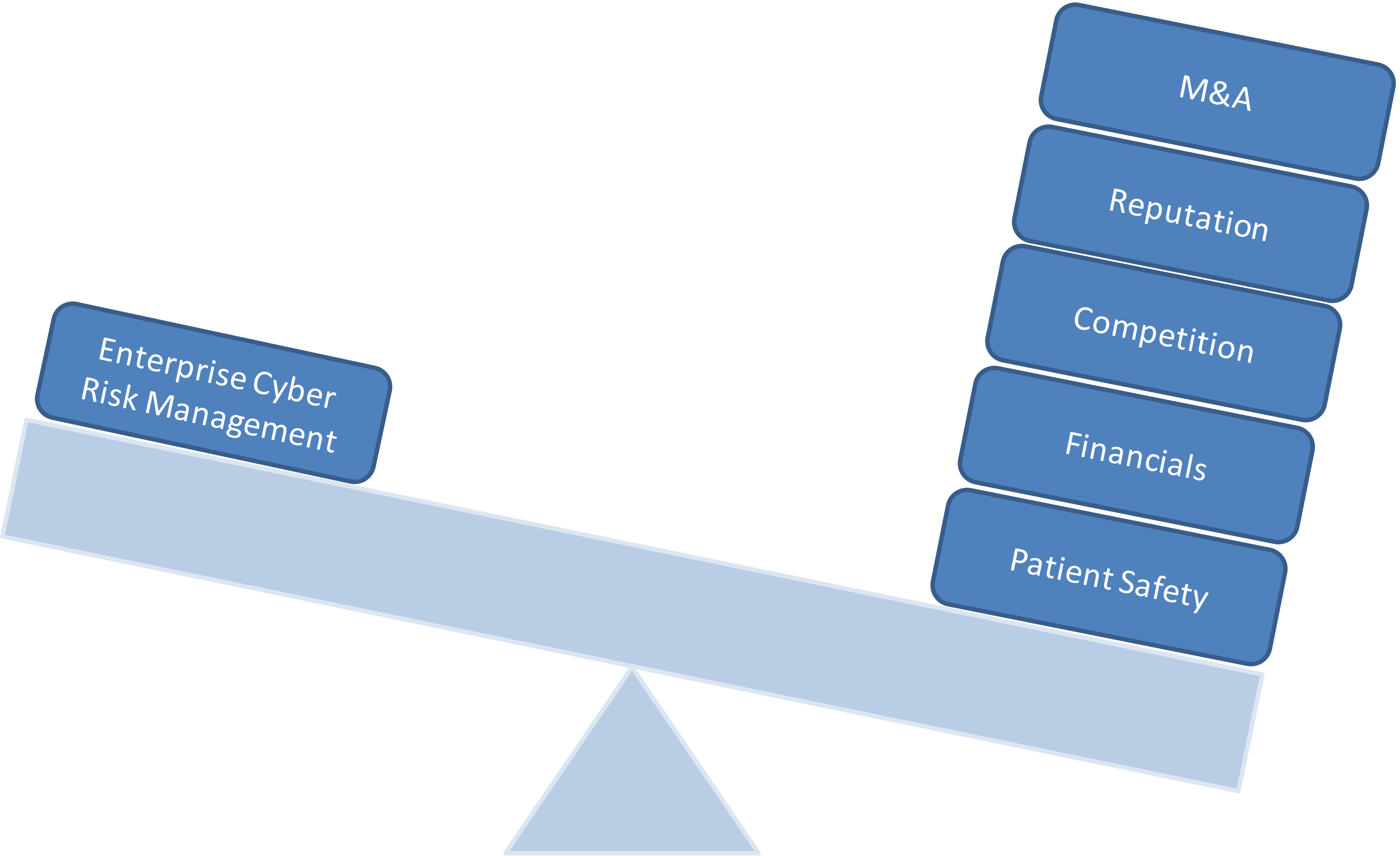


Discussion

Discussion Flow

1. Basics
2. **Business**
3. Budget

Lever and Elevate the ECRM Discussion

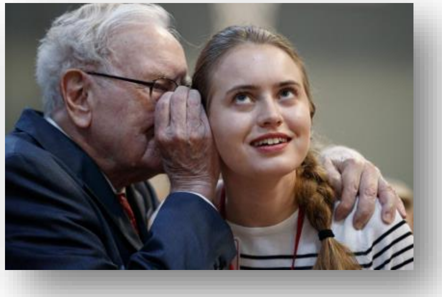


Discuss ECRM in the Context of…

Patient Safety, Quality of Care

Financials / Protecting The Balance Sheet

Non-Traditional, Disruptive Competition



Reputation / Brand

M&A Activities

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)*

Discussion

Discussion Flow

1. Basics
2. Business
3. **Budget**

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

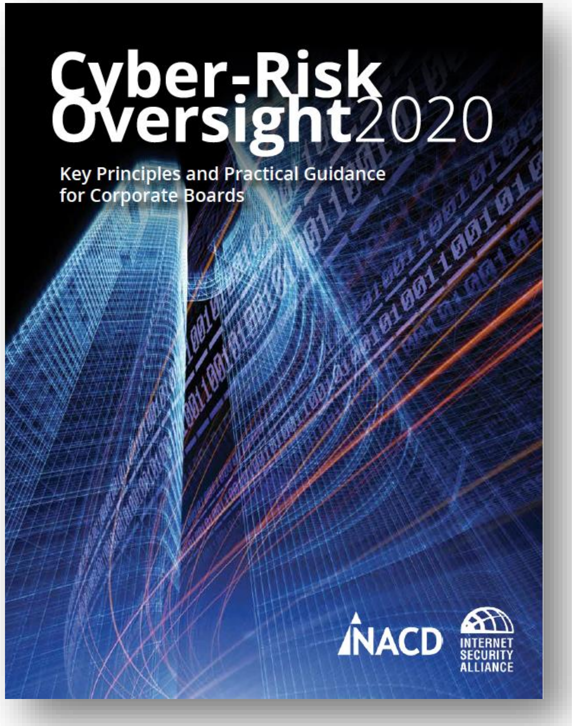
Source: Bob Chaput, *Stop the Cyber Bleeding,* 2020.

How to Best Help Your C-Suite and Board Become ECRM Enablers

"The primary focus and responsibility of a board is governance, and broken down to its essence, governance is all about patient-safety and mitigation."[1]

Context

Your Role

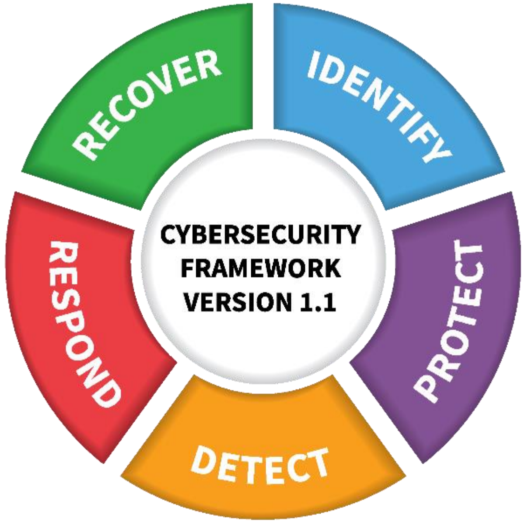

Cyber-Risk Oversight 2020

Key Principles and Practical Guidance for Corporate Boards

NACD

INTERNET SECURITY ALLIANCE

Best Practices



[1] Mike Myatt, author of Hacking Leadership, https://boardmember.com/boards-prioritizing-cybersecurity-risk/

Top Reasons for NIST-based ECRM

1. Internationally Recognized Best Practices
2. Standard for the U.S. Government
3. National Standard Across Industries

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.”

References

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.

Open for Questions

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

Contact

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

Ralph Davis
Senior Advisor and Operating Partner
The Vistria Group
(312) 420-0048
rdavis@vistria.com

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.