



# 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*



## 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.



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

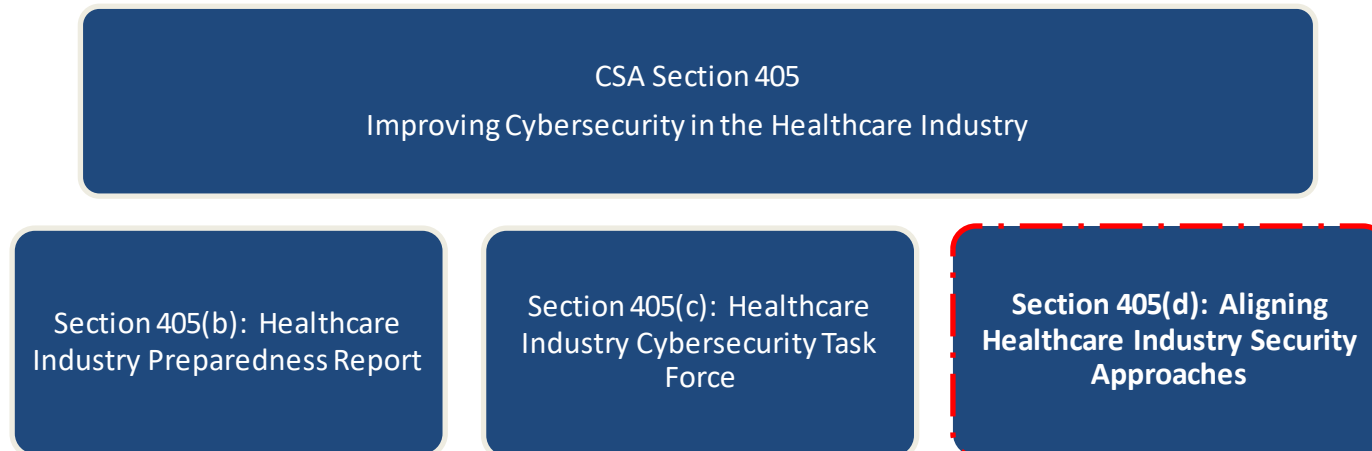


# Cybersecurity Act of 2015: Legislative Basis

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](mailto:CISA405d@hhs.gov) !



# 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!



## 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

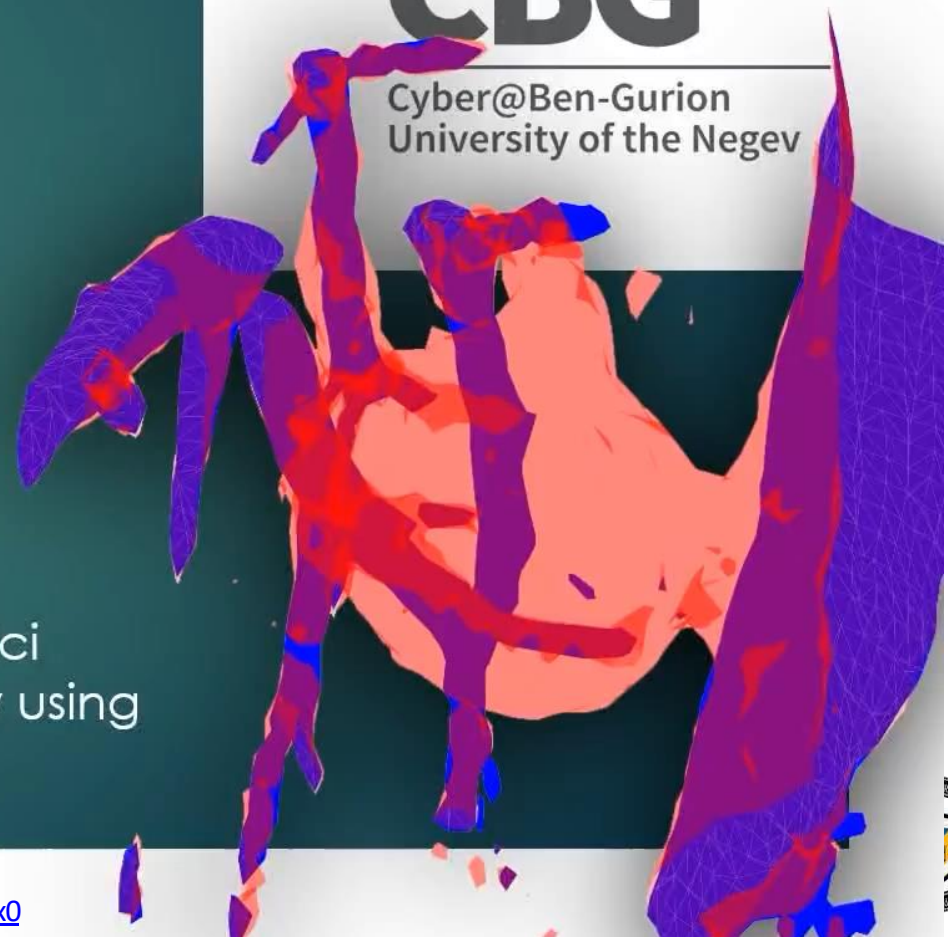
### Full paper:

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>



# CBG

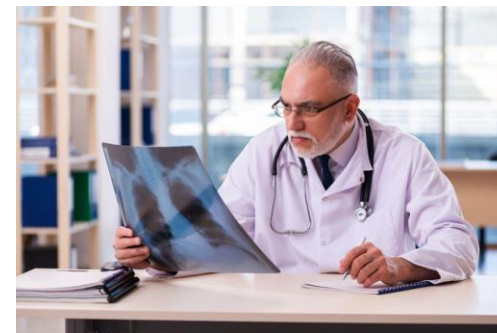
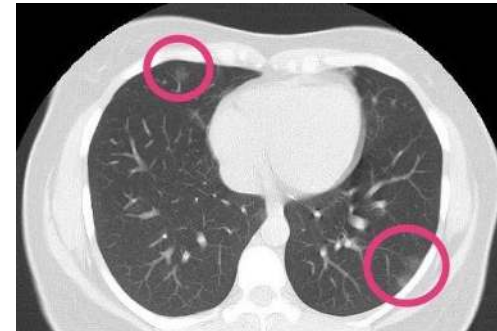
Cyber@Ben-Gurion  
University of the Negev



# When Something “Cyber” Happens

*Three bad things have happened here...*

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

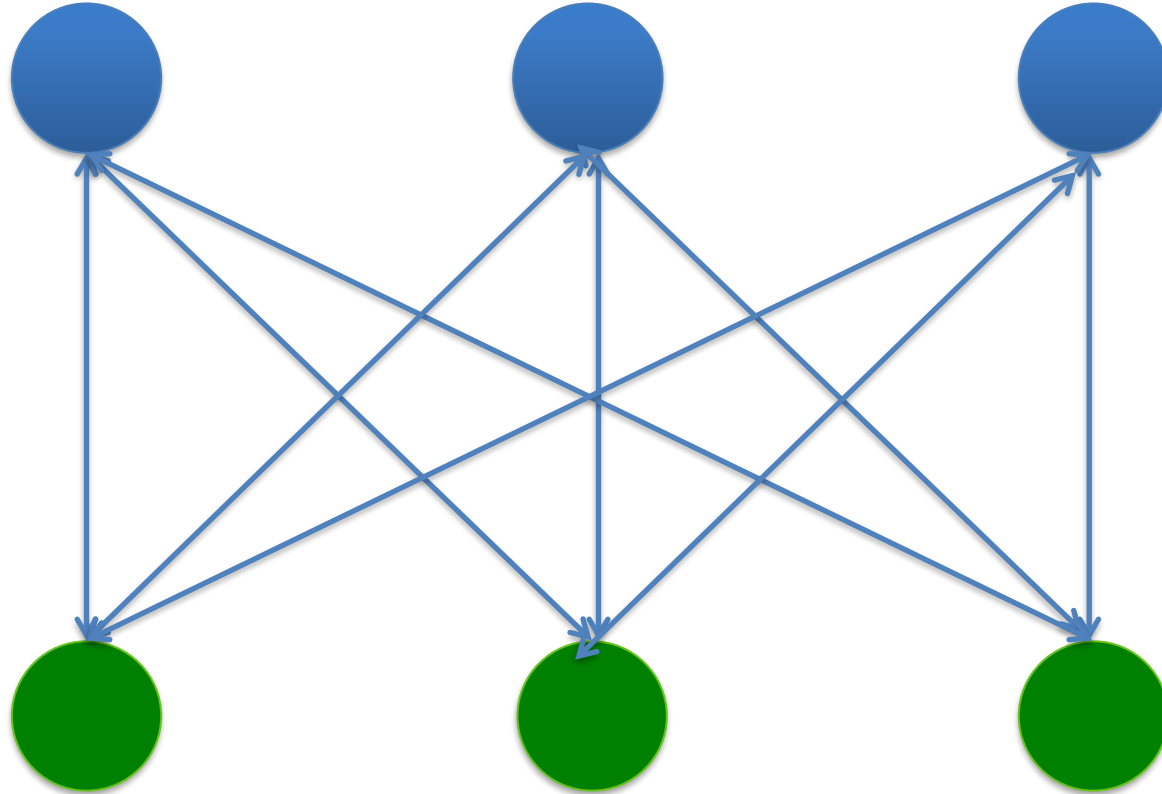


# Connect the Dots!

Confidentiality

Integrity

Availability



Quality & Safe  
Care

Access to Care

Timely Care



## Data, Systems, & Devices...AND Patient Safety & MPL

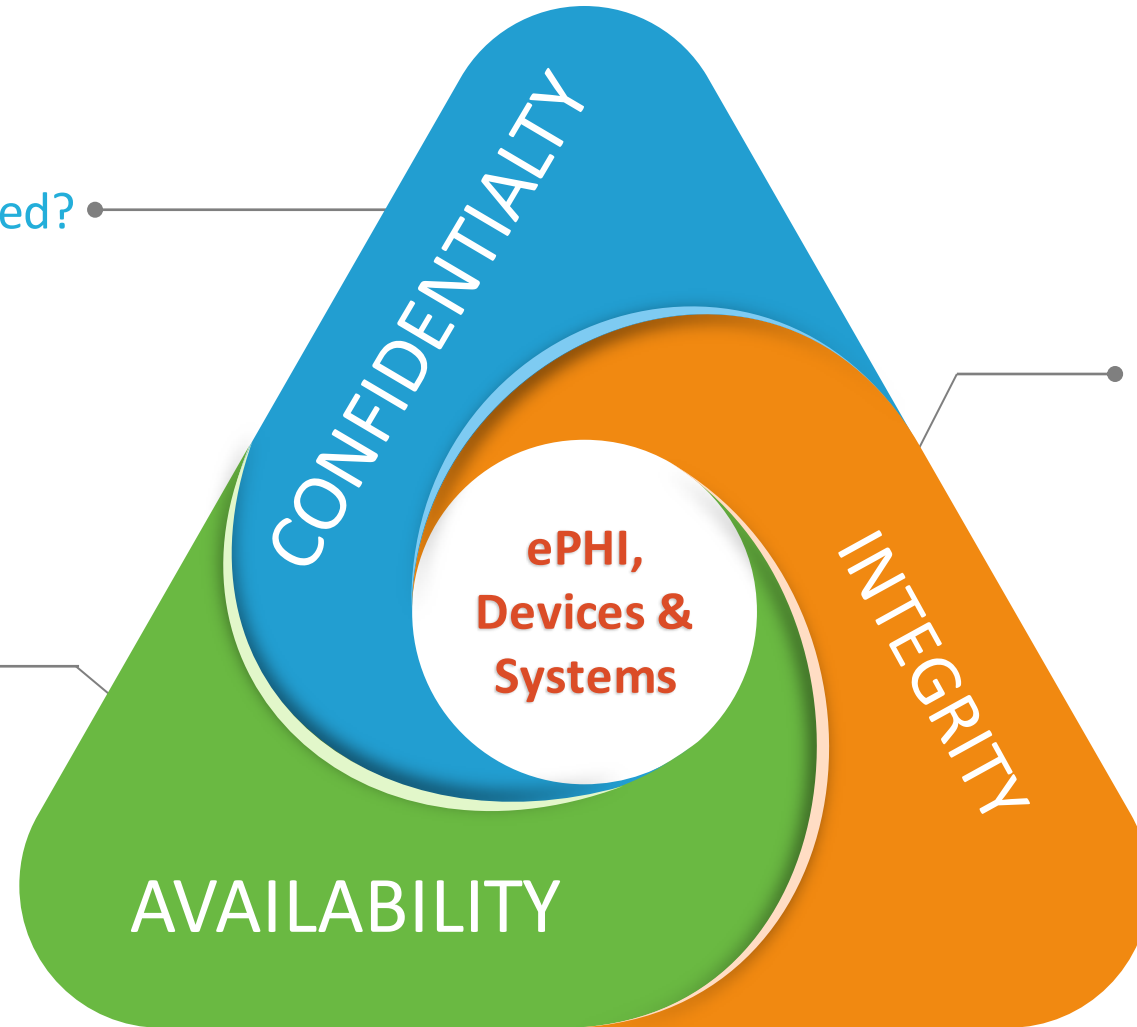


# Our Core Cyber Risk Responsibility

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!



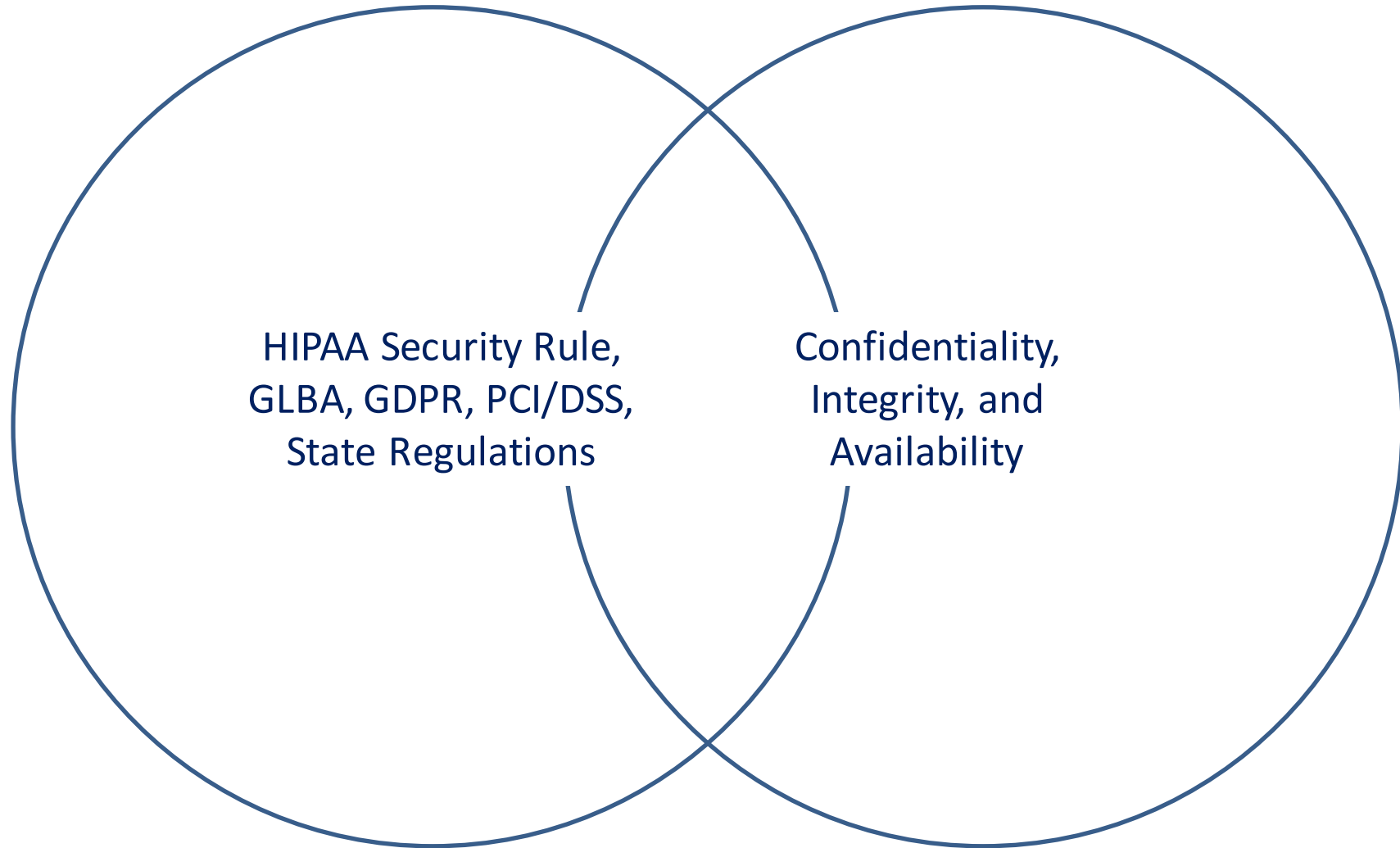
## Patient Safety – Quality of Care – Patient Satisfaction Issues

<b>Bad Things Emanating from COMPROMISE OF</b>		
<b>CONFIDENTIALITY</b>	<b>INTEGRITY</b>	<b>AVAILABILITY</b>
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?



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

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



# OCR-Quality® Risk Management



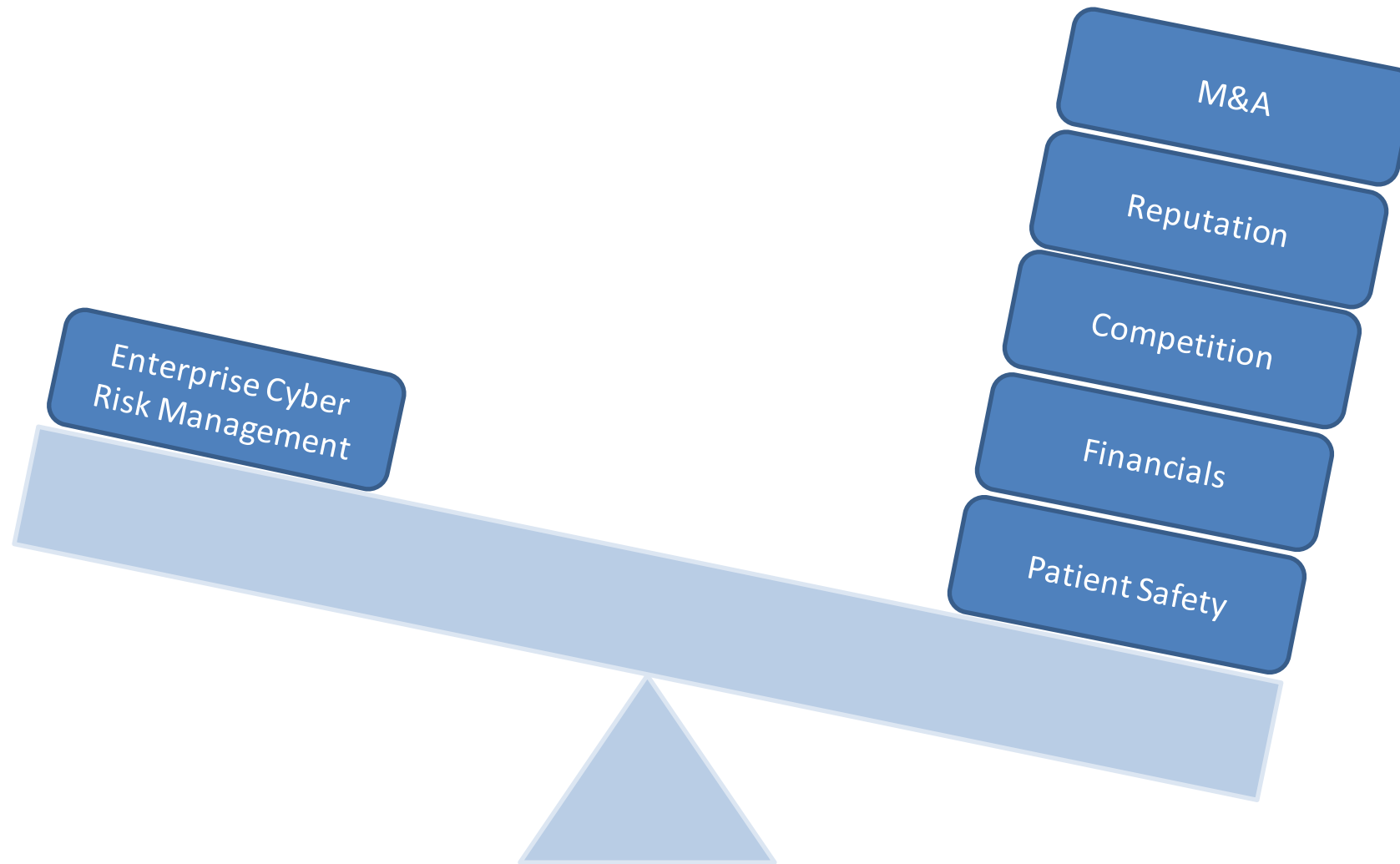
# Discussion



# 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...

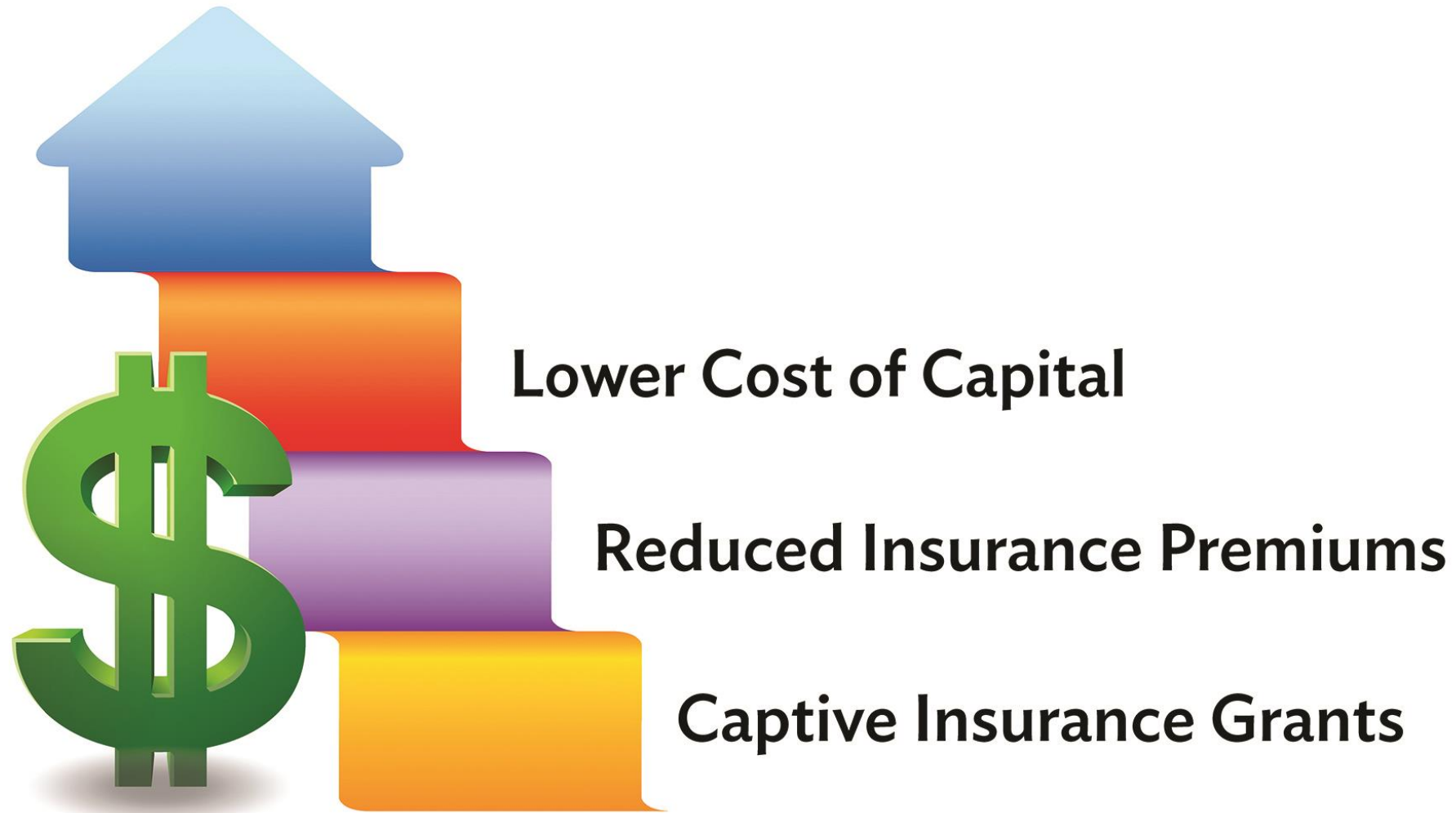
*I have written in previous letters about the enormous effort and resources we dedicate to protect ourselves and our clients—we spend nearly \$600 million a year on these efforts and have more than 3,000 employees deployed to this mission in some way. Indirectly, we also spend a lot of time and effort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



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



# 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](https://www.linkedin.com/company/hhs-ask405d)



## Contact

### **Bob Chaput**

Executive Chairman & Founder  
Clearwater  
(615) 496-4891

[bob.chaput@clearwatercompliance.com](mailto:bob.chaput@clearwatercompliance.com)



### **Ralph Davis**

Senior Advisor and Operating Partner  
The Vistria Group  
(312) 420-0048

[rdavis@vistria.com](mailto: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](http://www.phe.gov/405d).

