

# What Boards Should Know About Healthcare's Emerging Security Risk

Cris V. Ewell, Ph.D.  
Chief Security and Privacy Officer  
NRC Health

*Prepared for*  
The Governance Institute Leadership Conference | February 15, 2022



The Governance Institute®

A SERVICE OF **nrc**  
HEALTH

1

## Learning Objectives

- Discuss the most common healthcare security threats
- Review questions that boards can ask their security executives to assess maturity of security program and risk to the organization
- Assess your organization's security strategy and ability to prepare for the data threats and attacks
- Identify common healthcare security shortcomings and resource failures
- Define how to navigate this complex environment and create a plan that can adapt to the emerging threats

The Governance Institute Leadership Conference | February 15, 2022

2

2

## What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the current and potential regulations, risks and threats that could affect our business or industry?

3

## What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the current and potential regulations, risks and threats that could affect our business or industry?

4

**PAGE 2**

**The Governance Institute's Leadership Conference – Hybrid Event  
February 14–15, 2022**

# HIPAA and other compliance requirements

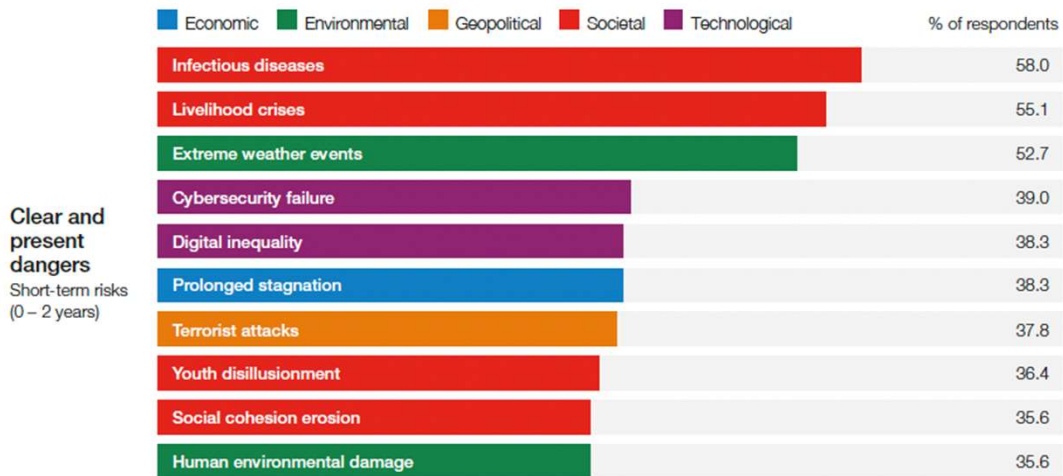


The Governance Institute Leadership Conference | February 15, 2022

5

5

# Global Risk Horizon



World Economic Forum 2021 Report

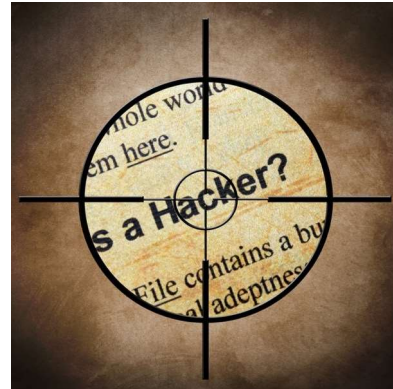
The Governance Institute Leadership Conference | February 15, 2022

6

6

## Why is healthcare a target?

- Cybercriminals view healthcare organizations as a soft target
- Ongoing shift from paper to electronic health records Increase in the use of network connected devices
- Attackers are increasing their sophistication
- Insurance fraud is harder to detect than identify fraud



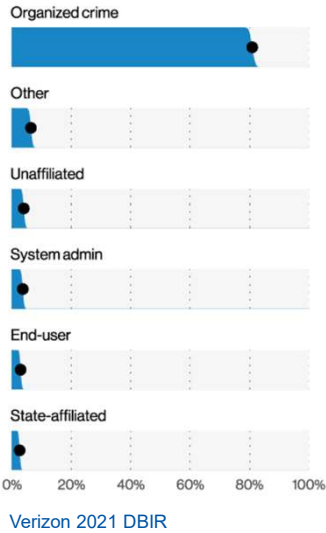
7

## Threat Landscape



8

# Threat Actors



Role	Motivation	Targeted Data
<ul style="list-style-type: none"> <li>Organized Crime</li> </ul>	<ul style="list-style-type: none"> <li>Profit</li> </ul>	<ul style="list-style-type: none"> <li>Payment card data</li> <li>Personally Identifiable Information (PII)</li> <li>Protected Health Information (PHI)</li> </ul>
<ul style="list-style-type: none"> <li>Insider</li> </ul>	<ul style="list-style-type: none"> <li>Disgruntled</li> <li>Personal gain</li> <li>Espionage</li> </ul>	<ul style="list-style-type: none"> <li>Intellectual property</li> <li>Strategic plans</li> <li>Customer contacts and PHI</li> <li>Company funds</li> </ul>
<ul style="list-style-type: none"> <li>Nation State</li> </ul>	<ul style="list-style-type: none"> <li>Economic growth of their country</li> <li>Innovation without R&amp;D</li> <li>Cyber warfare</li> </ul>	<ul style="list-style-type: none"> <li>Intellectual property</li> <li>Military secrets / designs</li> <li>HR and clearance records</li> <li>Critical infrastructure</li> </ul>
<ul style="list-style-type: none"> <li>Hacktivist</li> </ul>	<ul style="list-style-type: none"> <li>Idealism</li> <li>Influence change</li> <li>Service disruption</li> </ul>	<ul style="list-style-type: none"> <li>Sensitive business communications</li> <li>Executive documents that could cause embarrassment</li> </ul>

9

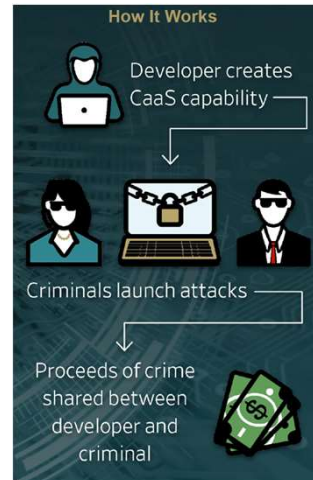
# Techniques for Compromising Data



10

## Cybercrime as a Service (CaaS)

- **Keep up with the basics:**
  - Patch software on a timely basis, follow backup best practices, manage third-party risk, and train staff.
- **Understand the adversary:**
  - Know which tactics, techniques, and procedures groups offering such services use to compromise firms.
- **Detect and prepare:**
  - Maintain visibility into the environment to identify problems and have a robust incident response plan.



[www.wsj.com/pro/cybersecurity/research](http://www.wsj.com/pro/cybersecurity/research)

The Governance Institute Leadership Conference | February 15, 2022

11

11

## Shadow Broker

- Claims to possess even more exploits stolen from the NSA-linked Equation Group
- Claims to possess much more data and exploits and has launched a subscription-based “service.”



The Governance Institute Leadership Conference | February 15, 2022

12

12

# Cyber Attack Examples

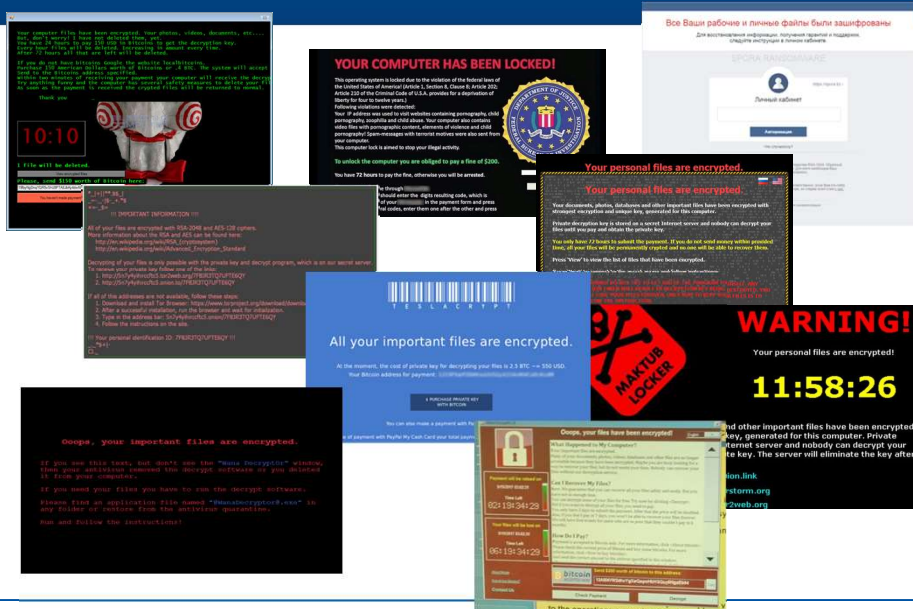


The Governance Institute Leadership Conference | February 15, 2022

13

13

# Ransomware



The Governance Institute Leadership Conference | February 15, 2022

14

14

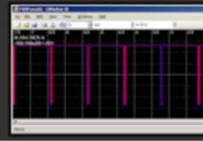
## Paging Incident

Saturday, 30 May 2009

### Hacking a pager (part 1)

I bought this weekend a pager for 2...  
find out. The case mentio...  
much!

I plug my scope on the digit...  
second exactly.



**Unencrypted pagers a security risk for hospitals, power plants**

For most of us, pagers went out when cell phones came in, but some companies are still using them and when the messages sent without encryption, attackers can listen in and even interfere with the communications.

### Data Protection Risks of Using Pagers in Healthcare

Posted on: September 26, 2016 Posted in: Healthcare, Mobile Security, Security

Posted by: Christopher Budd (Global Threat Communications)



Doctors and pagers are two things that have been closely linked since the introduction of pagers in the 1960s. For decades, the doctor checking his (and later his or her) pager has been a staple in movies and television.

And while you might have expected pagers to have gone way like rotary telephone (or any kind of wired telephone) you'd be wrong to think they have. Pagers are still in use today, especially in healthcare.

The Governance Institute Leadership Conference | February 15, 2022

15

15

## Key facts on WannaCry

- The malicious program (WannaCry) encrypts files and demands ransom
- Launched on May 12, 2017
- Infected 230,000 hosts in 150 countries
- Distributed using ExternalBlue exploit
- Spreads via SMB (fileshare), RDP (remote desktop) and phishing attacks
- Demands \$300-600 in Bitcoins

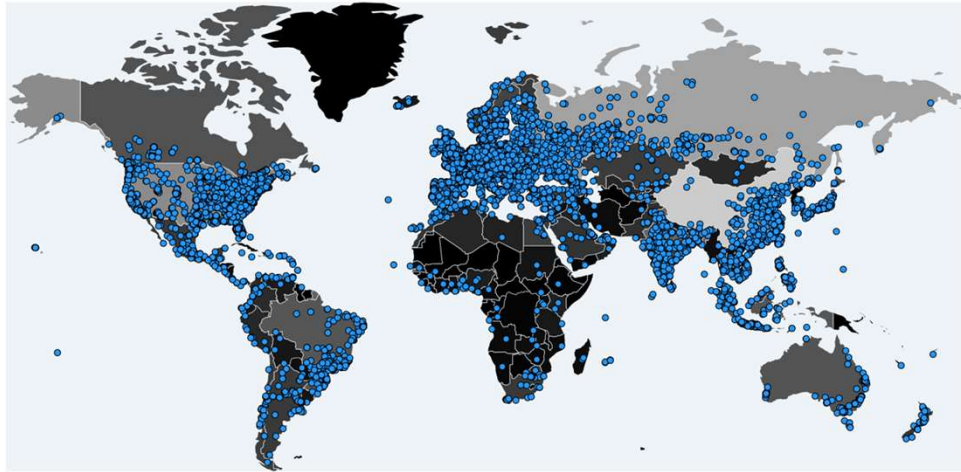
The Governance Institute Leadership Conference | February 15, 2022

16

16



## WannaCry Infections after 24 hours



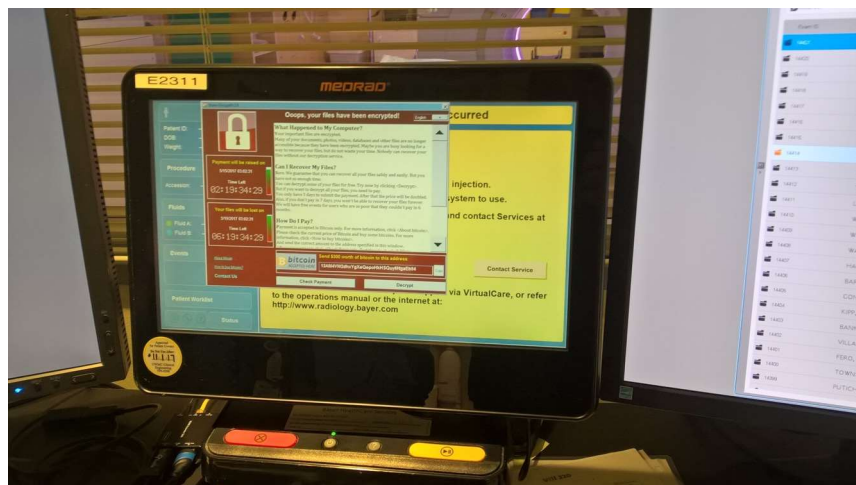
The Governance Institute Leadership Conference | February 15, 2022

17

17

## CT Injector

- Attack using WannaCry malware



The Governance Institute Leadership Conference | February 15, 2022

18

18

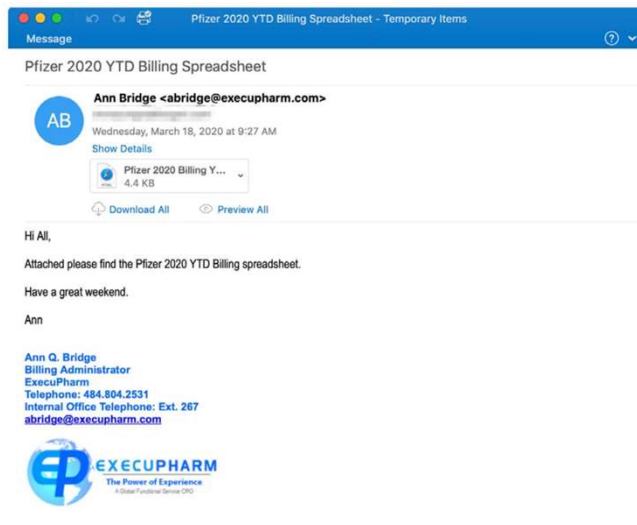
## DNA Sequencer

- Attack over RDP from Russian Federation



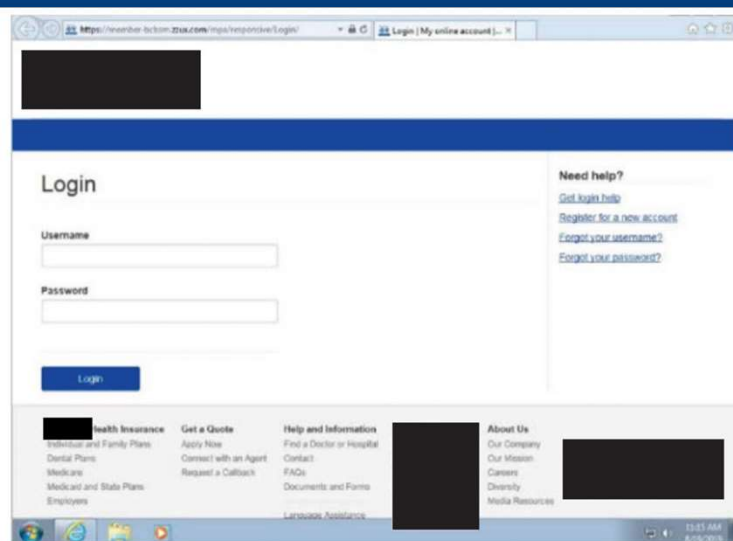
19

## Pharma: IP, financial data and PII risk



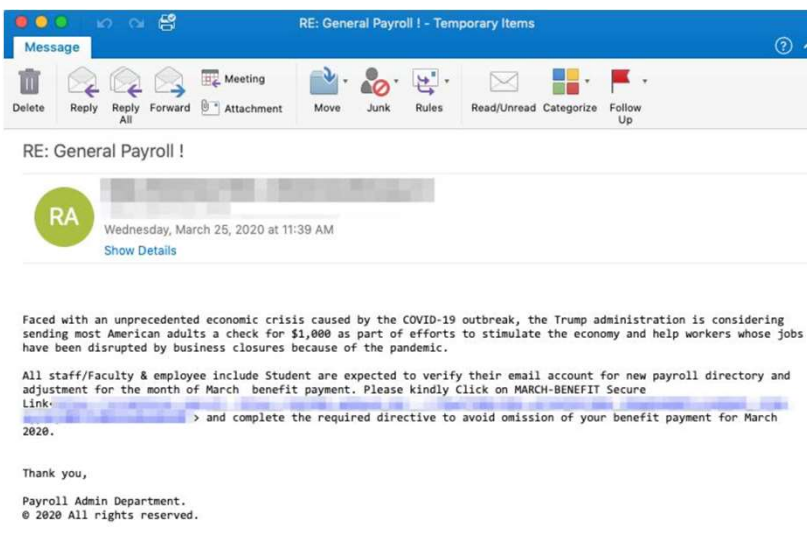
20

## Cloned portals



21

## Hospital



22

## What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the current and potential regulations, risks and threats that could affect our business or industry?

23

## Information security is a strategic business enabler



- Determine which board committee should have primary oversight of information security risk issues
- Hardwire information security risk considerations into key operational and strategic decision-making process
- Analyze information security issues with respect to their strategic implications and as part of enterprise risk
- Identify opportunities to use information security as a market differentiator/ business driver

24

## Information Security Strategy and Road Map

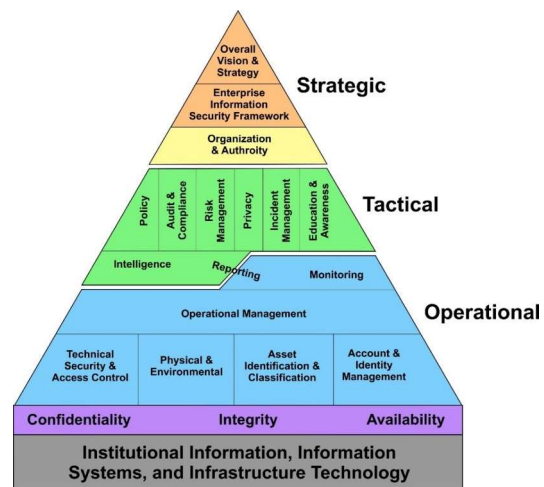
- How did you create your organizational information security strategy and road map?
- Is it aimed to comply with mandatory regulations or was it tailored to your organization's business strategy and technology?



25

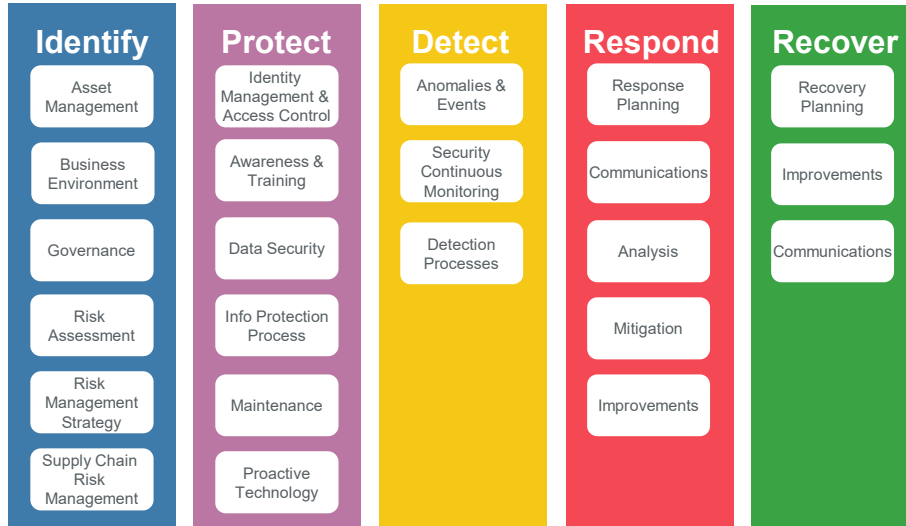
## Information Security Strategy and Road Map

- Adopt critical new practices that make sense and are nimble enough to stay ahead of the evolving threats
- Ensure that the organization does not implement controls that have little effect against identified threats
- Based on actual conditions, business objectives, and risk appetites specific to each organization



26

# NIST CSF Core Functions



27

# Factor Analysis of Information Risk (FAIR)



28

## What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the current and potential regulations, risks and threats that could affect our business or industry?

29

## Ensure organizational design supports information security

- Information security function is adequately represented across the business, internal groups and leadership
- Set expectations that information security/risk functions are to receive adequate staffing and funding and monitor the efficacy of these determinations
- Inspire an information security culture and encourage collaboration between the cybersecurity function and all stakeholders
- Ensure an accountable officer has authority and responsibility to coordinate information risk strategy throughout the organization and that the organization has a comprehensive plan for data governance



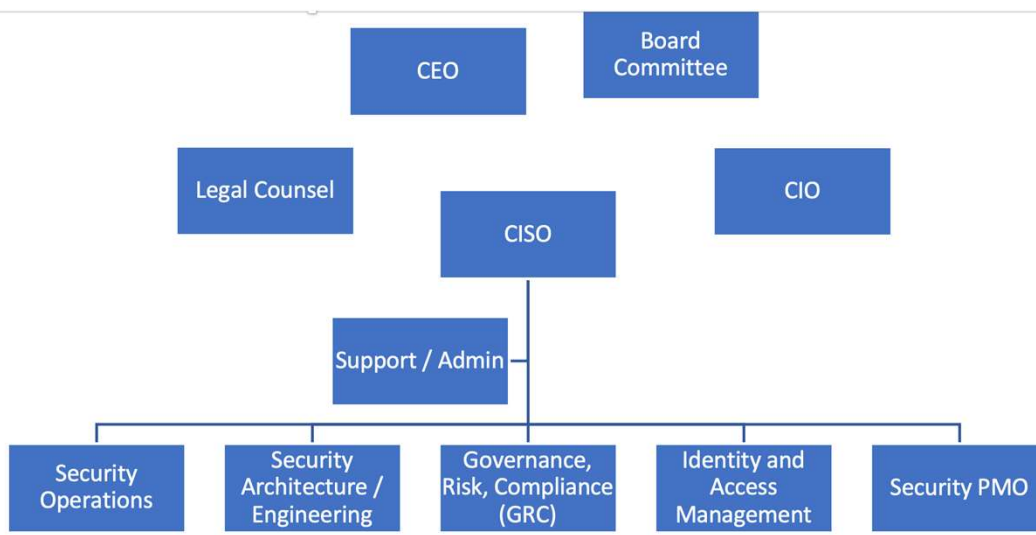
30

## Establish a culture of cybersecurity and resilience



31

## Example security Org chart



32



## Incorporate cybersecurity expertise into board governance



- Build relationships with internal stakeholders who can provide expertise to guide strategic cybersecurity decisions
- Increase board of directors' base level of knowledge on information security risk
- Seek out third-party advisers and assessors—who report to the board regularly
- Consider periodic audits, reviews of information security strength and benchmarking by independent third parties
- Get regular updates on recent information security incidents, trends, vulnerabilities and risk predictions

33

## What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- **Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?**
- Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the current and potential regulations, risks and threats that could affect our business or industry?

34

## Understand the economic drivers and impact of cyber risk

- Review and approve the organization's cyber-risk appetite, or tolerance
- Instruct management to establish a consistent framework, using industry-accepted risk quantification models
- Require continuous examination of comparative measurements and metrics
- Base information security risk management decisions on the potential impact and likelihood of risk events and functional loss or exposure



The Governance Institute Leadership Conference | February 15, 2022

35

35

## Align information security risk management with business needs



- Critically review the organization's business strategy and drivers in the context of their information security risk implications
- Require management to report to the board
  - Information security implications of their activities
  - Well-developed, written and tested plans to counter adverse information security events
- Require management to
  - Integrate cyber-risk analysis into significant business decisions along with effective assurances of the information's quality and comprehensiveness
  - Provide roadmaps on how the company makes determinations of risk materiality that inform regulatory obligations

The Governance Institute Leadership Conference | February 15, 2022

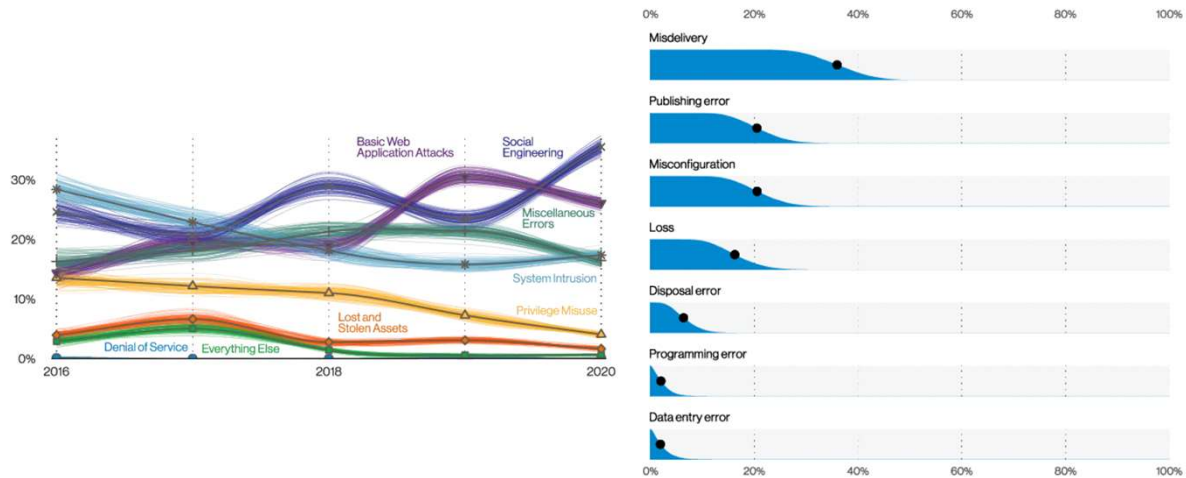
36

36

PAGE 18

The Governance Institute's Leadership Conference – Hybrid Event  
February 14–15, 2022

## Incident information



The Governance Institute Leadership Conference | February 15, 2022

37

37

## Audit, Assessments, and Compliance

- Do we have a third party assess the information security program maturity?
- Have we closed all high-risk findings from last external penetration test, audit, or assessment?
- Do we baseline the organization against NIST or some other standard?



The Governance Institute Leadership Conference | February 15, 2022

38

38

## Encourage systemic resilience and collaboration

- Develop a 360-degree view of the organization’s risk and resiliency posture
- Develop peer networks, including other board members, to share best governance practices across institutional boundaries
- Ensure management has plans for effective collaboration, especially with the public sector, on improving cyber resilience
- Ensure that management accounts for risks stemming from the broader industry connections
- Encourage management participation in industry groups and knowledge and information-sharing platforms



39

## Risk Management



40

# How do you measure the impact and relevancy of the security controls?



41

# Security Performance (Example)

- Reduction in patching time
- Exposure to malware
- Mean time to resolve

Vulnerability Management KPI

		Last	Current	Trend
Vulnerability Management	Improve High Risk Applications			↑
	Reduce Network Environment Risk			→
	Maintain Program Health			↓

42

## Third party risk

- 1. What is the average vendor score?
- 2. What is the score for critical vendors?
- 3. Is it trending up or down?



Score / Impact		
83 0 percent 100	B	\$4M
68 0 percent 100	D+	\$37.4M
86 0 percent 100	B	\$46.1K 🟡
88 0 percent 100	B+	\$25.1K 🟡
83 0 percent 100	B	\$5.3M
90 0 percent 100	A-	\$28.1K 🟡

43

## Is there any value in these KPIs?

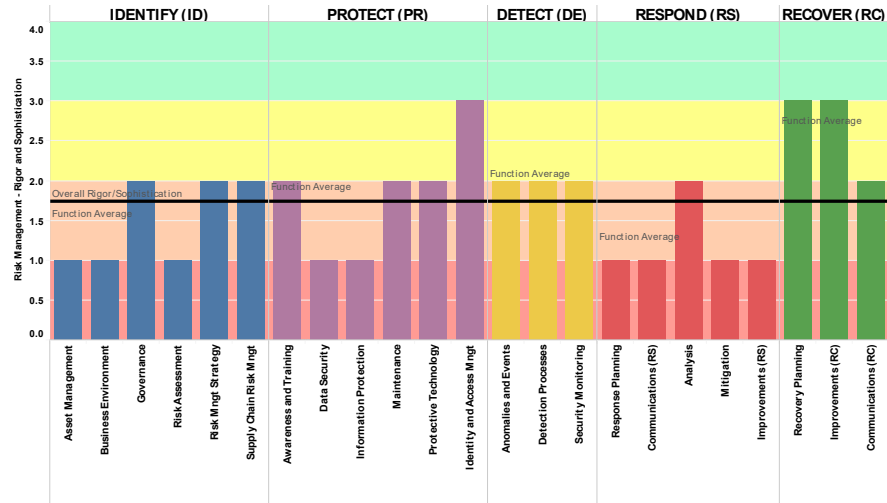
- Level of preparedness
- Unidentified devices on internal networks
- Intrusion attempts
- Security incidents
- Mean Time to Detect / Resolve / Contain
- First party security ratings
- Average vendor security rating
- Volume of data transferred using the corporate network
- Number of users with “super user” access level
- Number of days to deactivate former employee credentials
- Patching cadence
- Access management
- Company vs peer performance
- Vendor patching cadence
- Mean time for vendors incident response
- How quickly can we identify and respond to incidents?
- Number of spam emails blocked
- Qualitative measures of risk
- Perimeter Attacks Blocked
- Unpatched Vulnerabilities
- Number of communication ports open

44

# NIST CSF Risk Management Sample Measurement

Rigor and sophistication of risk management

- 1 - Partial
- 2 - Risk Informed
- 3 - Repeatable
- 4 - Adaptive



45

# What should a board know about their security program?

- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the capabilities to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- **Are we investing the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?**
- What are the current and potential regulations, risks and threats that could affect our business or industry?

46

## Investments

- What is in your security budget?
  - Staff, training, security controls and third-party expertise for example
- Investment can significantly reduce the likelihood of an expensive and disruptive incident
- Even with limited value, benchmarking against peers on the overall level of security spending might provide some information
  - Variables such as maturity level and tolerance for risk can vastly differ between organization



47

## Final thoughts / Review



- Information security is a strategic business enabler (not just an IT function)
- Understand the economic drivers and impact of cyber risk
- Align information security risk management with business needs
- Ensure organizational design supports information security
- Incorporate cybersecurity expertise into board governance
- Encourage systemic resilience and collaboration

48



## What should a board know about their security program?

- Is our **cybersecurity strategy** based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have **appropriate** internal and external **expertise** to lead and deliver the strategic and tactical duties of defending our organization's network and data?
- Do we have the **capabilities** to identify risks, detect threats, measure our program's effectiveness, respond to attacks and recover from disruption?
- Are we **investing** the right amount in cybersecurity skills, technologies and resources to ensure data security without diminishing returns?
- What are the **current** and potential regulations, **risks and threats** that could affect our business or industry?

49

## Questions



Cris V. Ewell, PhD  
Chief Security and Privacy Officer  
NRC Health  
cewell@nrchealth.com



50