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 Support Forum| September 10, 2022

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

What should a board know about their security program?

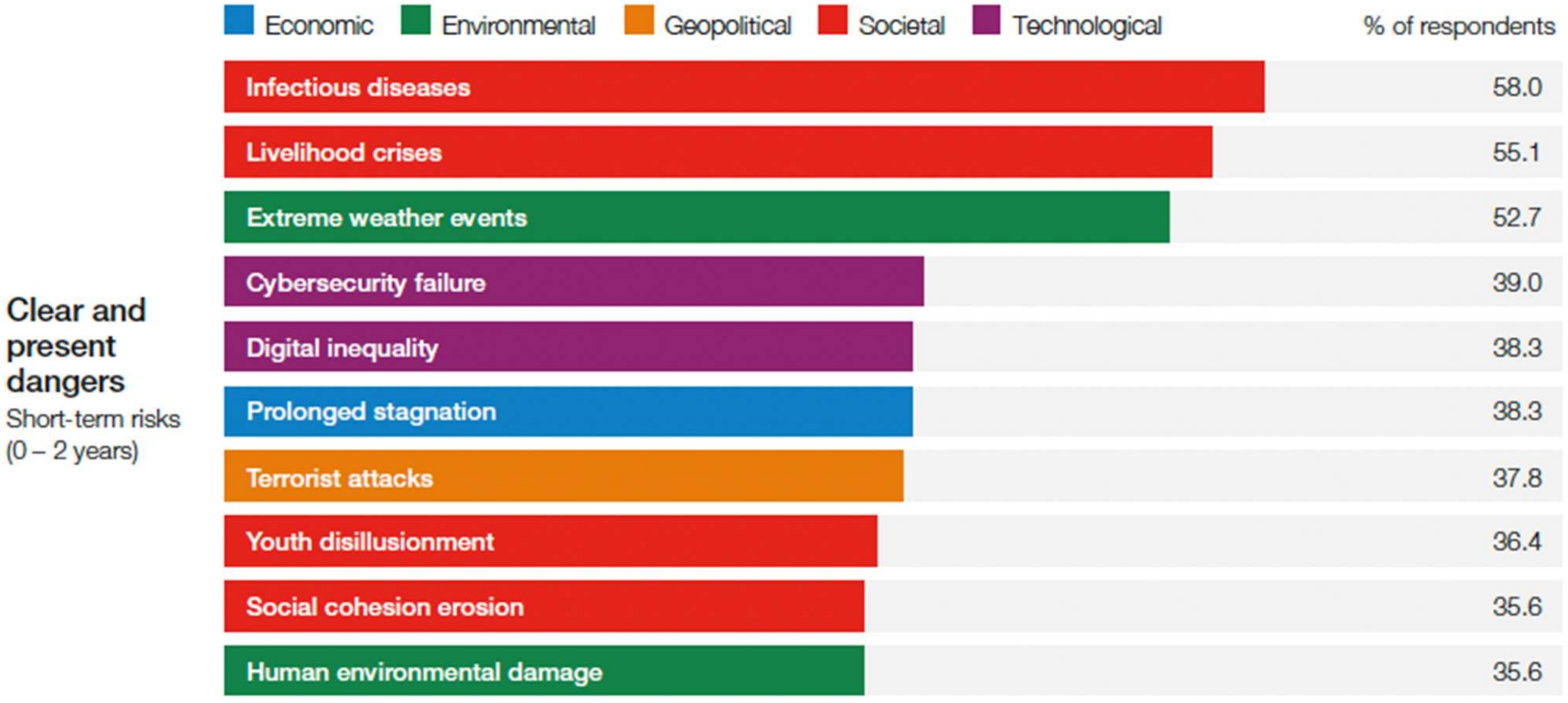
- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and 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?

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?

HIPAA and other compliance requirements

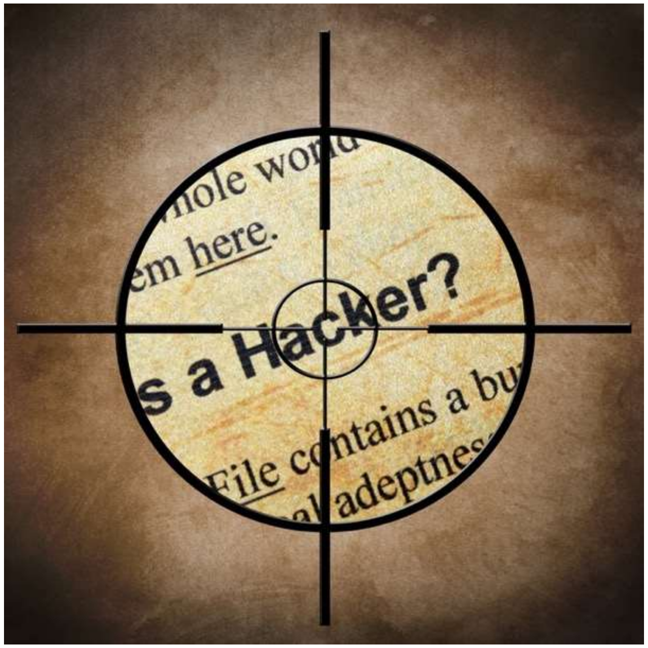
Global Risk Horizon



World Economic Forum 2021 Report

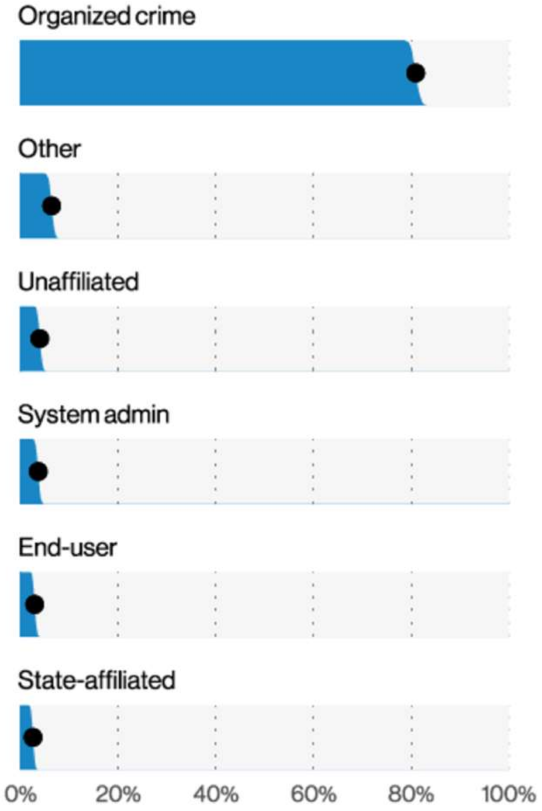
Why is healthcare a target?

- 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



Threat Landscape

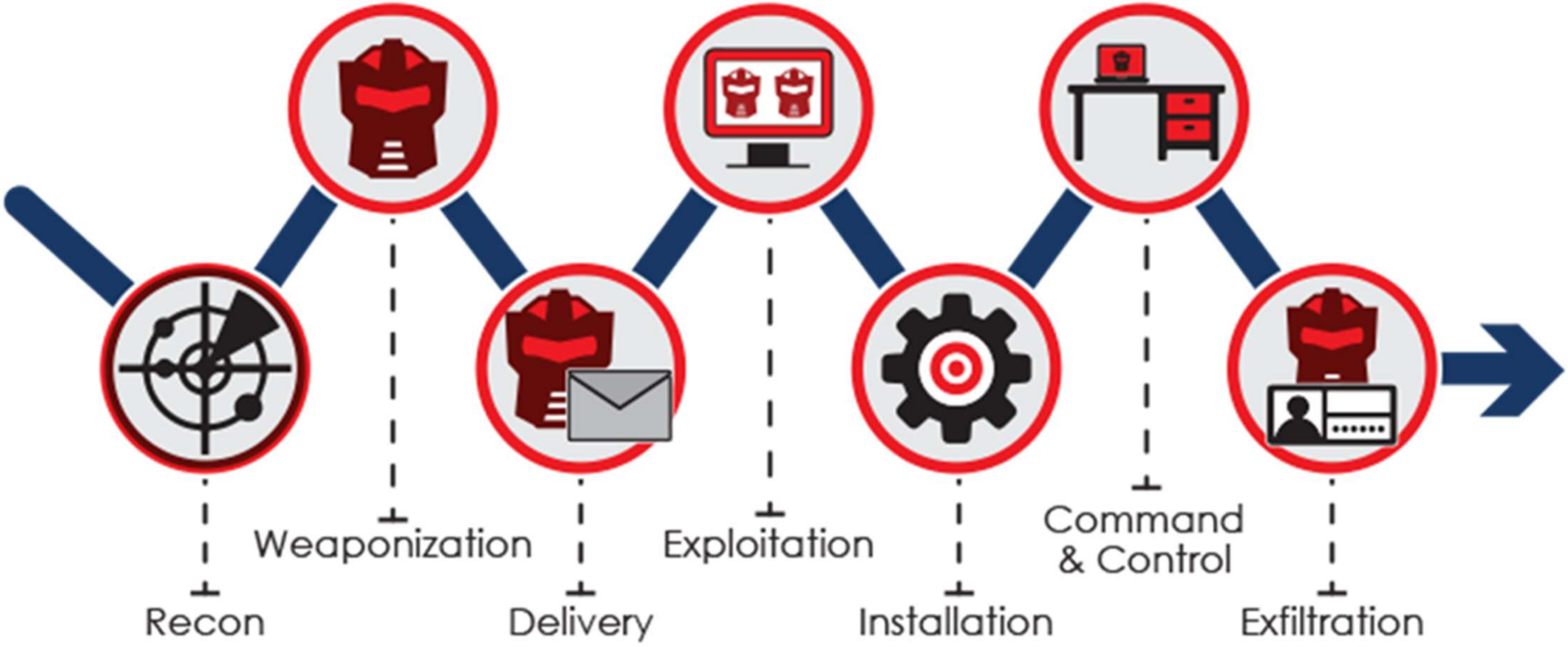
Threat Actors



Verizon 2021 DBIR

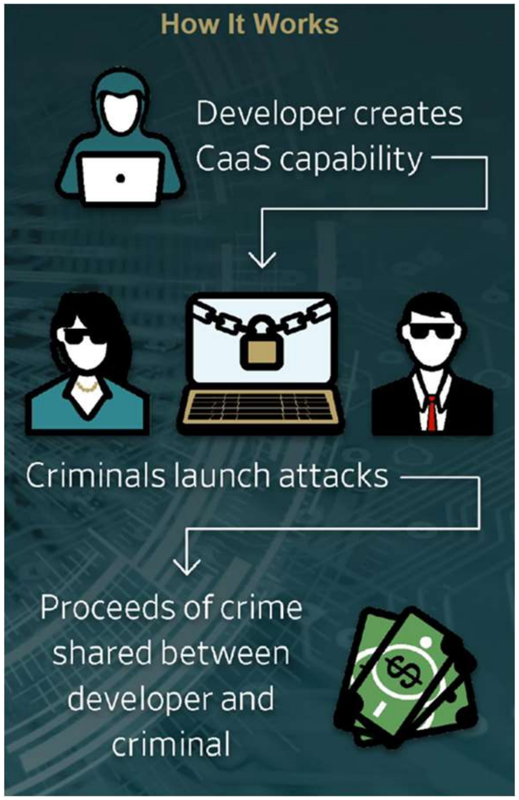
Role	Motivation	Targeted Data
- Organized Crime	- Profit	- Payment card data - Personally Identifiable Information(PII) - Protected Health Information (PHI)
- Insider	- Disgruntled - Personal gain - Espionage	- Intellectual property - Strategic plans - Customer contacts and PHI - Company funds
- Nation State	- Economic growth of their country - Innovation without R&D - Cyber warfare	- Intellectual property - Military secrets / designs - HR and clearance records - Critical infrastructure
- Hacktivist	- Idealism - Influence change - Service disruption	- Sensitive business communications - Executive documents that could case embarrassment

Techniques for Compromising Data



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.



How It Works

Developer creates CaaS capability

Criminals launch attacks

Proceeds of crime shared between developer and criminal

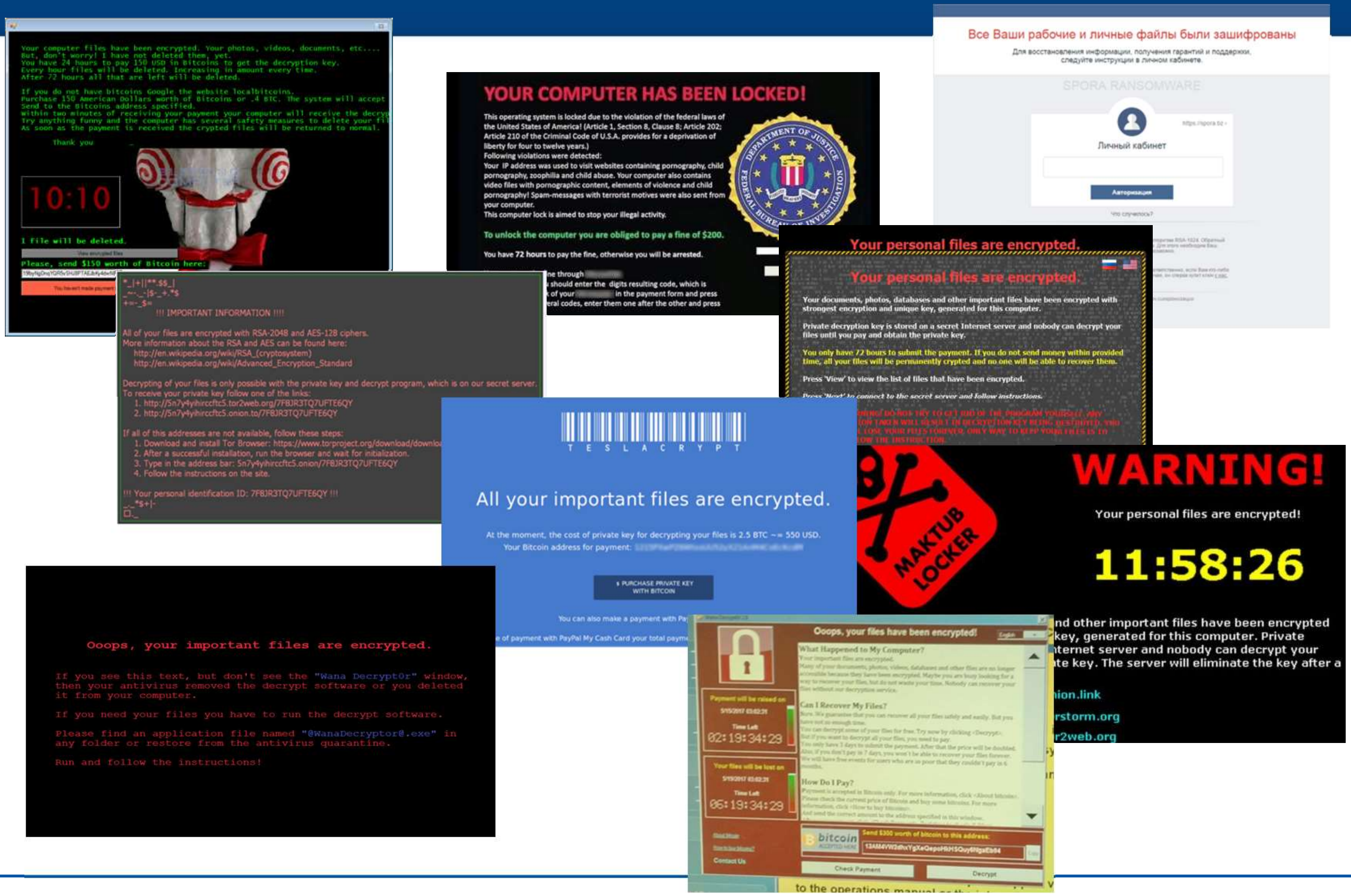
www.wsj.com/pro/cybersecurity/research

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.”

Cyber Attack Examples

Ransomware



Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decry
Try anything funny and the computer has several safety measures to delete your fil
As soon as the payment is received the crypted files will be returned to normal.

Thank you

1 file will be deleted.

Please, send $150 worth of Bitcoin here:

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

...ne through [redacted]
...u should enter the digits resulting code, which is
...k of your [redacted] in the payment form and press
...eral codes, enter them one after the other and press

Все Ваши рабочие и личные файлы были зашифрованы

Для восстановления информации, получения гарантий и поддержки, следуйте инструкции в личном кабинете.

*_|+||**.$$_|
_~-._-|$-_+.*$
+=-_$=
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://5n7y4yihirccftc5.tor2web.org/7FBJR3TQ7UFTE6QY
2. http://5n7y4yihirccftc5.onion.to/7FBJR3TQ7UFTE6QY

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/downlo
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 5n7y4yihirccftc5.onion/7FBJR3TQ7UFTE6QY
4. Follow the instructions on the site.

!!! Your personal identification ID: 7FBJR3TQ7UFTE6QY !!!
_._*$+|-
□._

Your personal files are encrypted.

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

...RNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ...ION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU ...L LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO ...LOW THE INSTRUCTION.

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [redacted]

You can also make a payment with Pa...
...e of payment with PayPal My Cash Card your total paym...

WARNING!

Your personal files are encrypted!

...nd other important files have been encrypted
...key, generated for this computer. Private
...nternet server and nobody can decrypt your
...te key. The server will eliminate the key after a

...ion.link
...rstorm.org
...r2web.org

Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.

Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29

Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

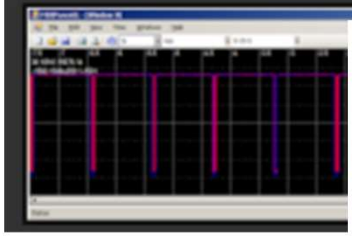
Paging Incident

Saturday, 30 May 2009

Hacking a pager (part 1)

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

I plug my scope on the digi   ced a burst of serial data every 1
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)

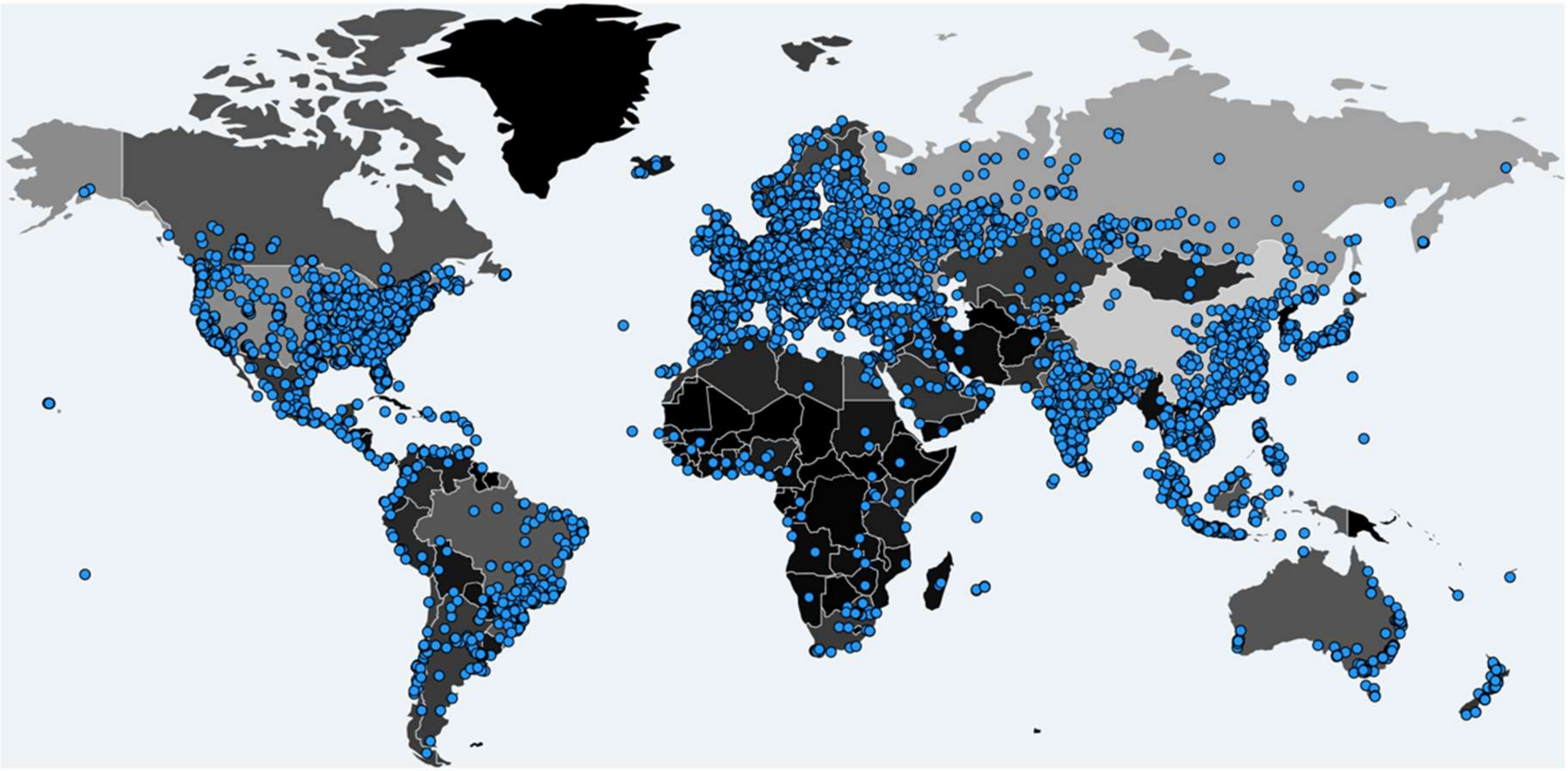
Doctors and pagers are two things that have been closely linked since the introduction of pagers in the 1960s. For decades, the doctor checking his (and later his or her) pager has been a staple in movies and television.

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.

Key facts on WannaCry

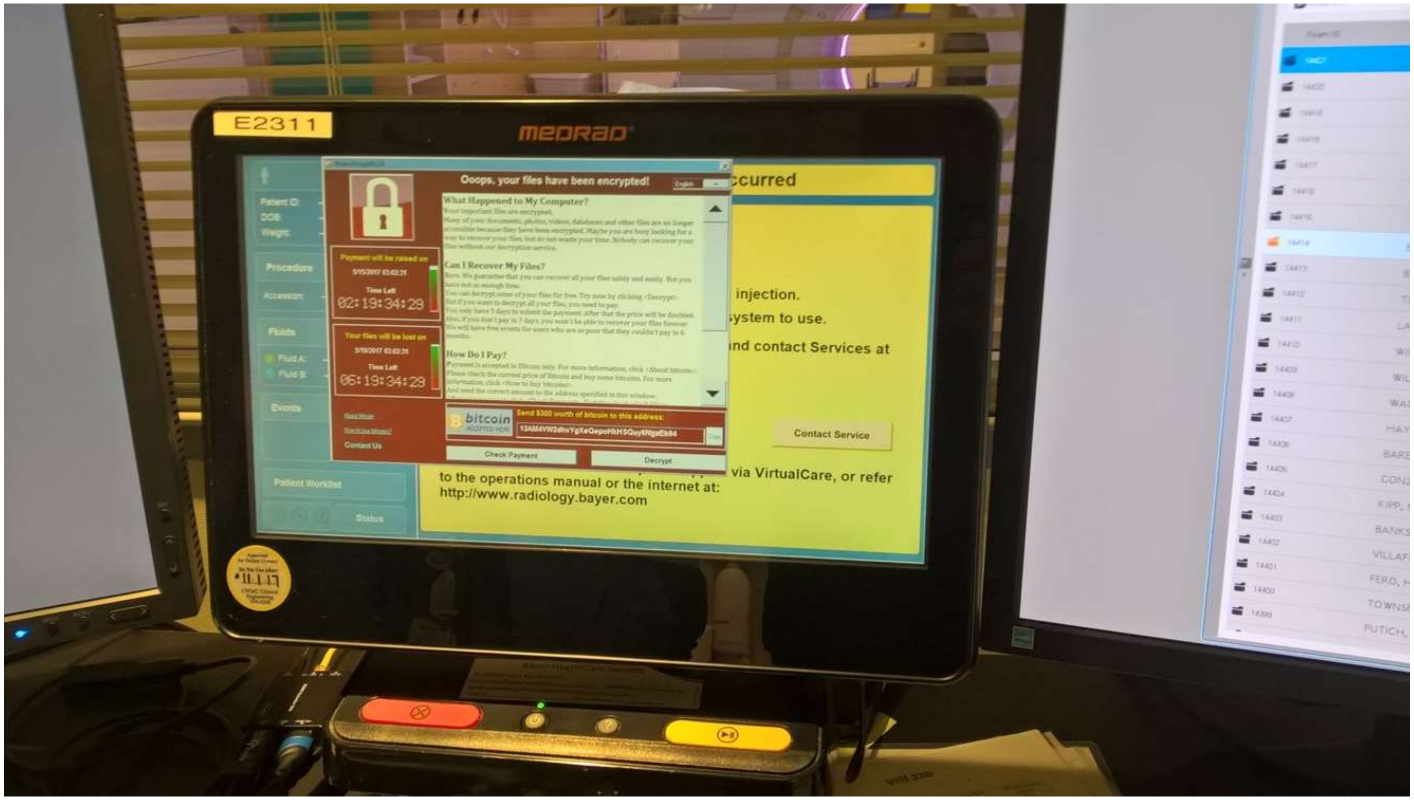
- The malicious program (WannaCry) encrypts files and demands ransom
- Launched on May 12, 2017
- Infected 230,000 hosts in 150 countries
- Distributed using ExternalBlue exploit
- Spreads via SMB (fileshare), RDP (remote desktop) and phishing attacks
- Demands $300-600 in Bitcoins

WannaCry Infections after 24 hours



CT Injector

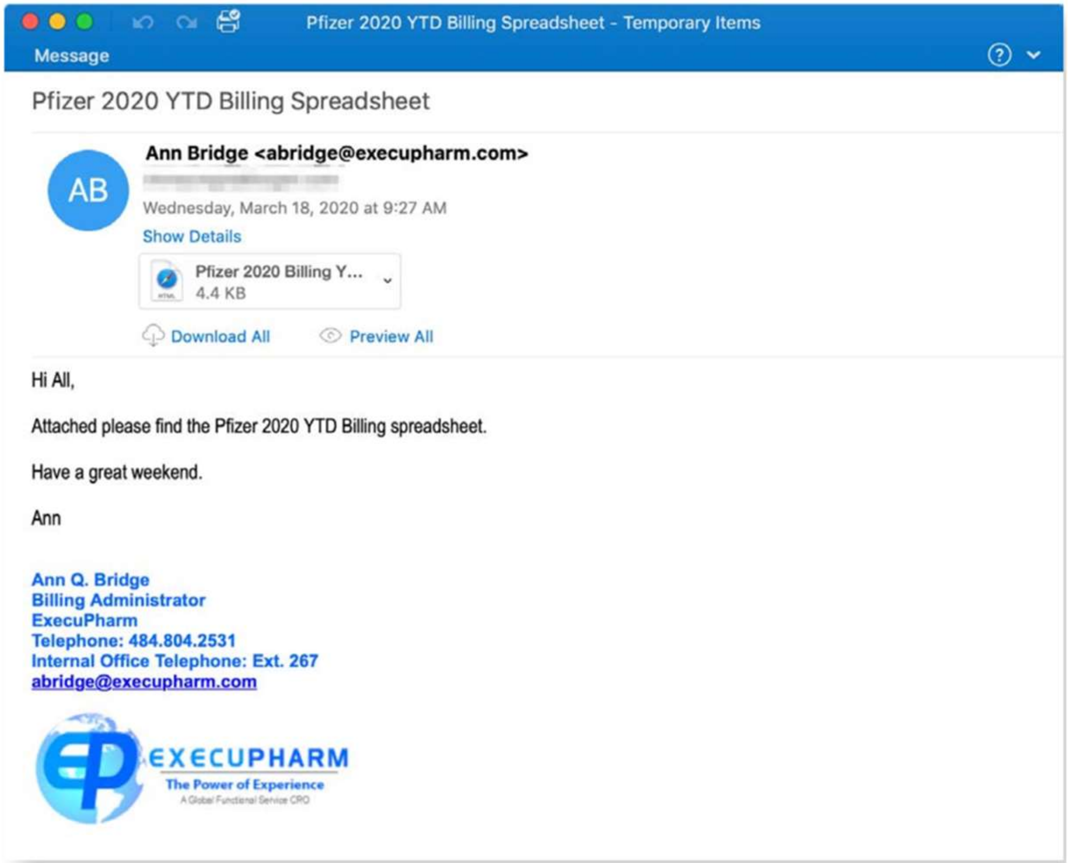
- Attack using WannaCry malware


E2311
MEDRAD
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:19:34:29
Your files will be lost on
Time Left
06:19:34:29
Contact Us
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt
ccurred
injection.
ystem to use.
nd contact Services at
Contact Service
via VirtualCare, or refer
to the operations manual or the internet at:
http://www.radiology.bayer.com
Procedure
Fluids
Fluid A
Fluid B
Events
Patient Worklist
Status

DNA Sequencer

- Attack over RDP from Russian Federation

Pharma: IP, financial data and PII risk



Pfizer 2020 YTD Billing Spreadsheet

AB

Ann Bridge <abridge@execupharm.com>

[redacted]

Wednesday, March 18, 2020 at 9:27 AM

Show Details

Pfizer 2020 Billing Y...
4.4 KB

Download All   Preview All

Hi All,

Attached please find the Pfizer 2020 YTD Billing spreadsheet.

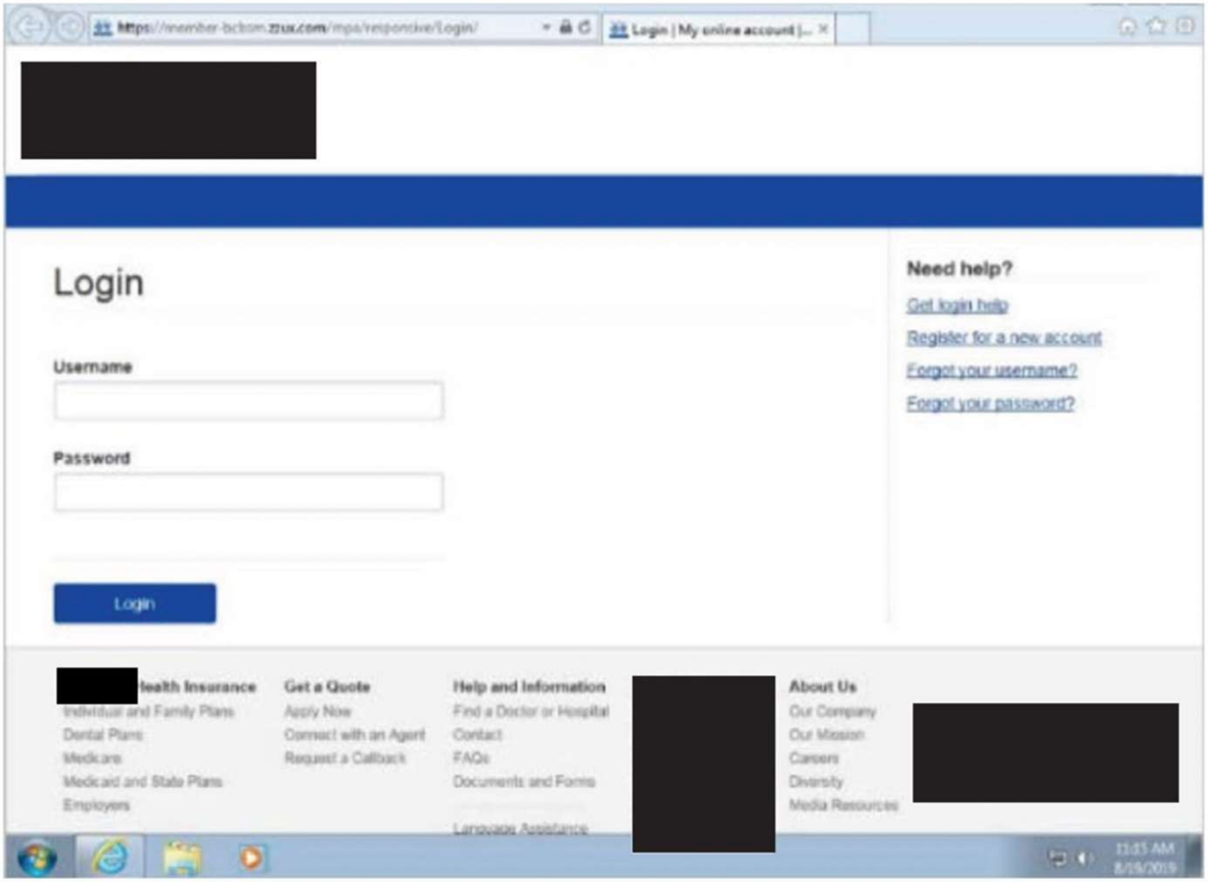
Have a great weekend.

Ann

Ann Q. Bridge
Billing Administrator
ExecuPharm
Telephone: 484.804.2531
Internal Office Telephone: Ext. 267
abridge@execupharm.com

EXECUPHARM
The Power of Experience
A Global Functional Service CRO

Cloned portals



https://member-bcbsm.zzux.com/mpa/responsive/Login/

[redacted]

Login

Username

Password

Need help?

Get login help

Register for a new account

Forgot your username?

Forgot your password?

[redacted]ealth Insurance
Individual and Family Plans
Dental Plans
Medicare
Medicaid and State Plans
Employers

Get a Quote
Apply Now
Connect with an Agent
Request a Callback

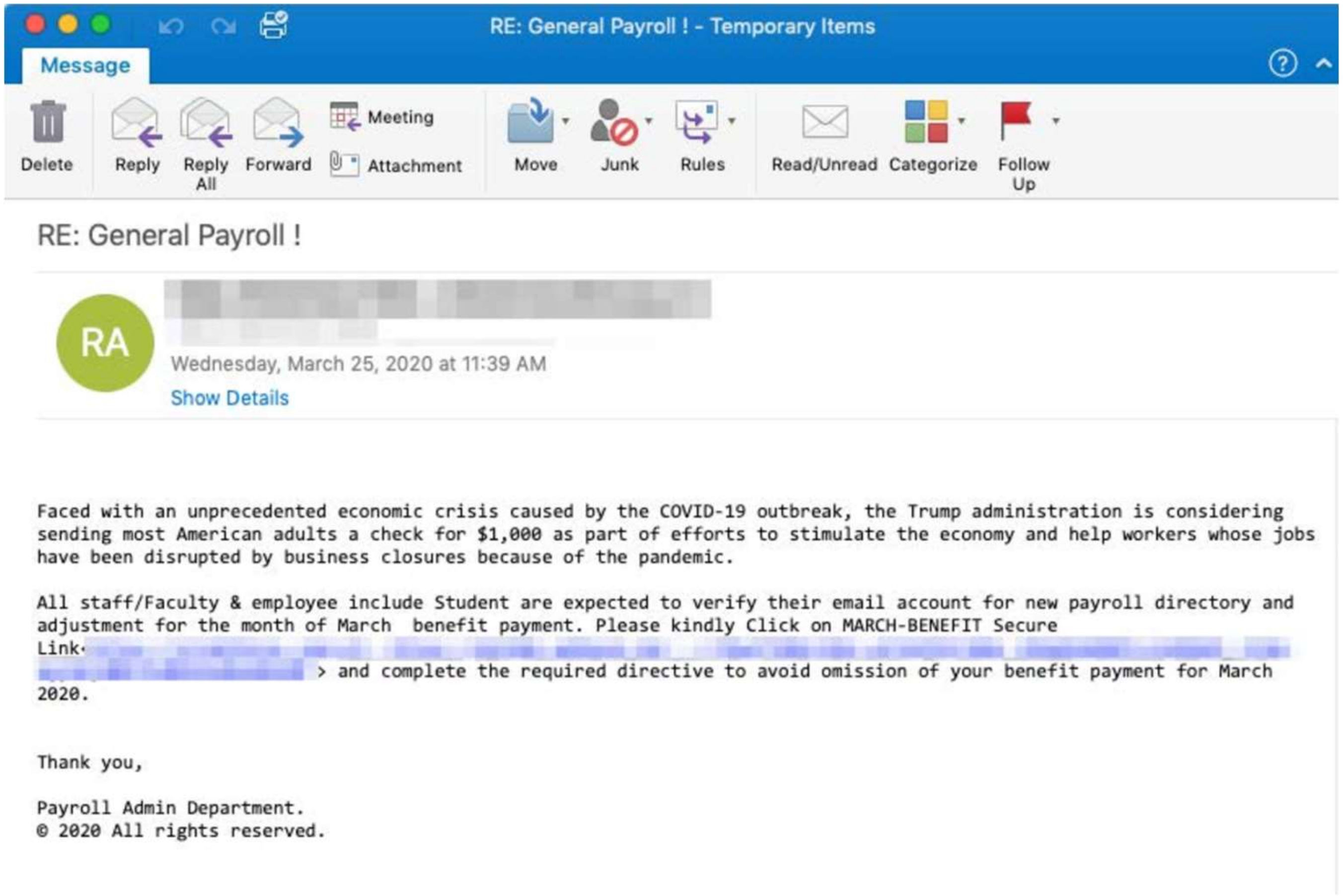
Help and Information
Find a Doctor or Hospital
Contact
FAQs
Documents and Forms
Language Assistance

[redacted]

About Us
Our Company
Our Mission
Careers
Diversity
Media Resources

[redacted]

Hospital



RE: General Payroll !

[redacted]

Wednesday, March 25, 2020 at 11:39 AM

Show Details

```
Faced with an unprecedented economic crisis caused by the COVID-19 outbreak, the Trump administration is considering
sending most American adults a check for $1,000 as part of efforts to stimulate the economy and help workers whose jobs
have been disrupted by business closures because of the pandemic.

All staff/Faculty & employee include Student are expected to verify their email account for new payroll directory and
adjustment for the month of March  benefit payment. Please kindly Click on MARCH-BENEFIT Secure
Link<[redacted]> and complete the required directive to avoid omission of your benefit payment for March
2020.


Thank you,

Payroll Admin Department.
© 2020 All rights reserved.
```

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?

Information security is a strategic business enabler

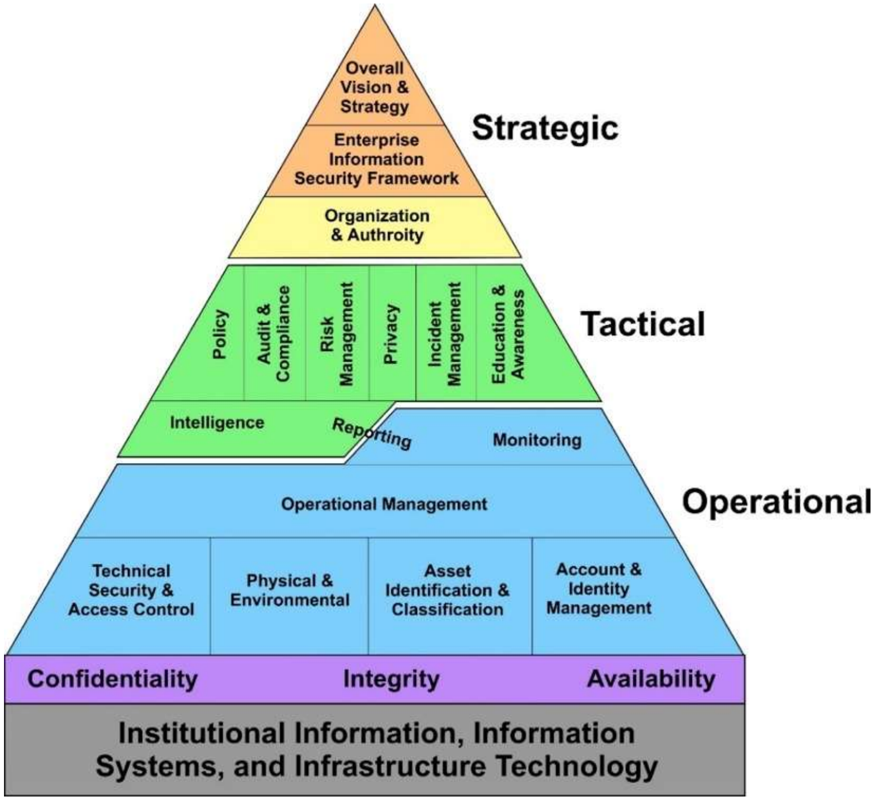
- Determine which board committee should have primary oversight of information security risk issues
- Hardwire information security risk considerations into key operational and strategic decision-making process
- Analyze information security issues with respect to their strategic implications and as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

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?

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



Overall Vision & Strategy

Enterprise Information Security Framework

Organization & Authroity

Strategic

Policy | Audit & Compliance | Risk Management | Privacy | Incident Management | Education & Awareness

Tactical

Intelligence

Reporting

Monitoring

Operational Management

Operational

Technical Security & Access Control | Physical & Environmental | Asset Identification & Classification | Account & Identity Management

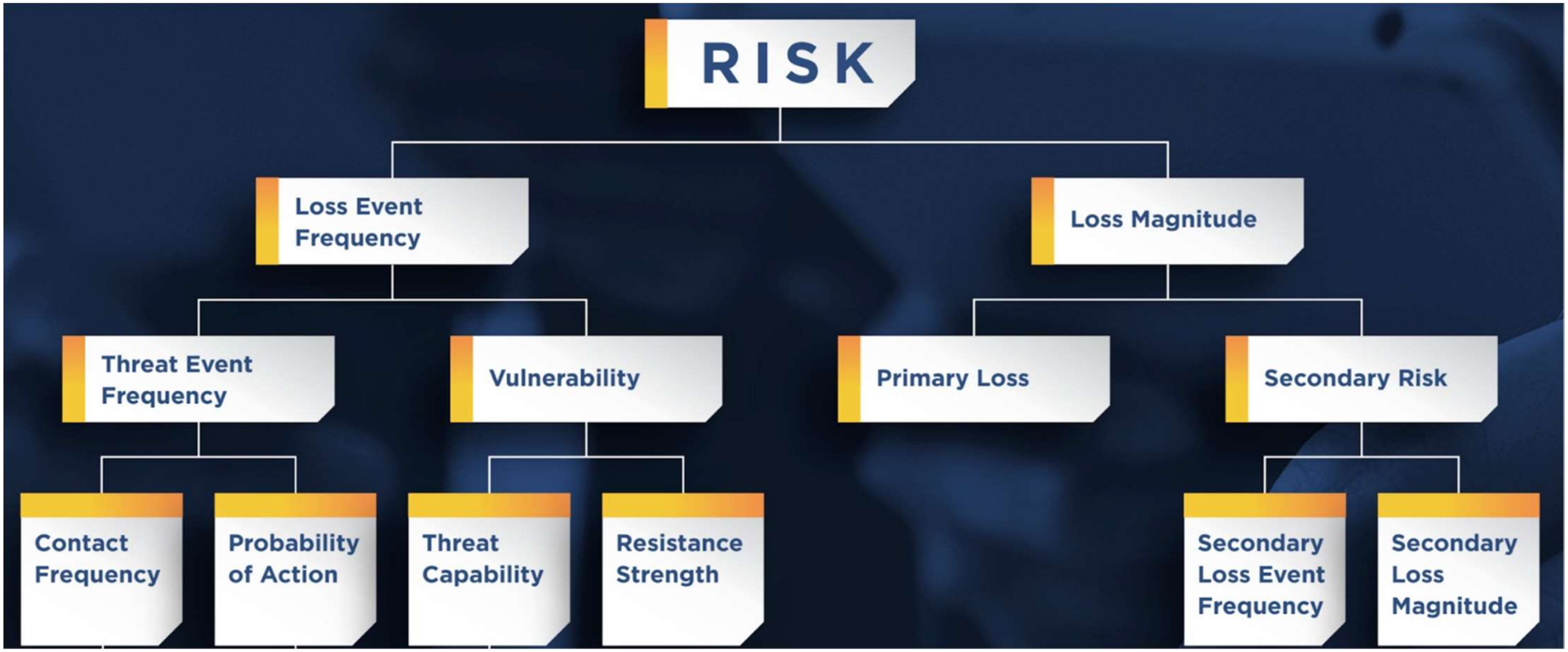
Confidentiality | Integrity | Availability

Institutional Information, Information Systems, and Infrastructure Technology

NIST CSF Core Functions

Identify	Protect	Detect	Respond	Recover
Asset Management	Identity Management & Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Proactive Technology			

Factor Analysis of Information Risk (FAIR)



What should a board know about their security program?

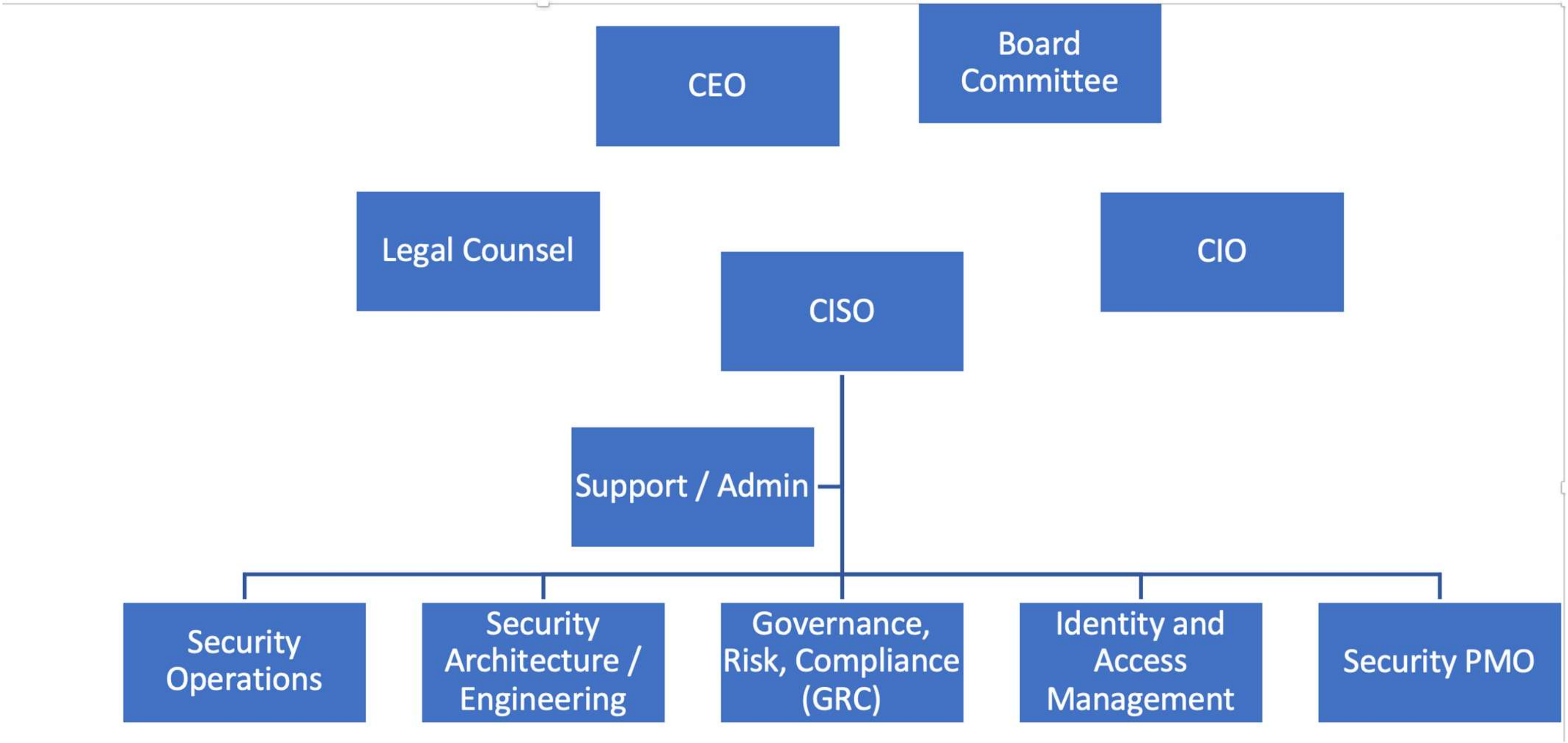
- Is our cybersecurity strategy based on a recognized risk management framework, adapted to our specific needs and aligned to our business strategy?
- Do we have appropriate internal and external expertise to lead and deliver the strategic and tactical duties of defending our organization's network and 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?

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

Establish a culture of cybersecurity and resilience

Example security Org chart


CEO
Board Committee
Legal Counsel
CIO
CISO
Support / Admin
Security Operations
Security Architecture / Engineering
Governance, Risk, Compliance (GRC)
Identity and Access Management
Security PMO

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

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?

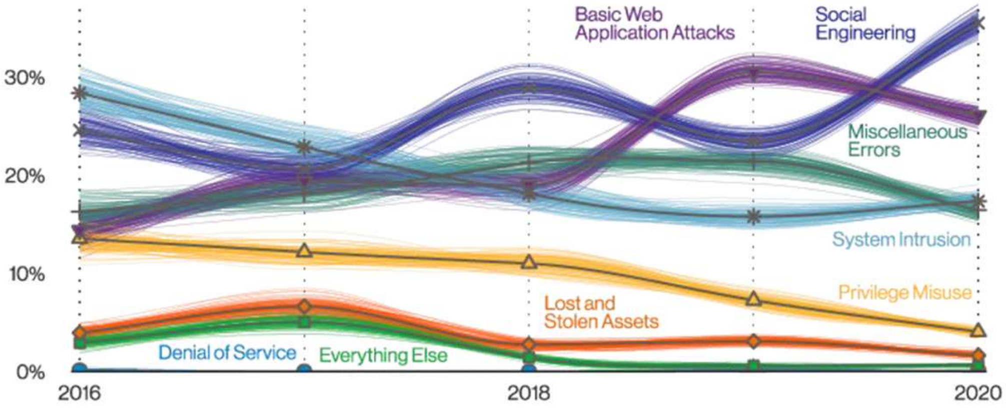
Understand the economic drivers and impact of cyber risk

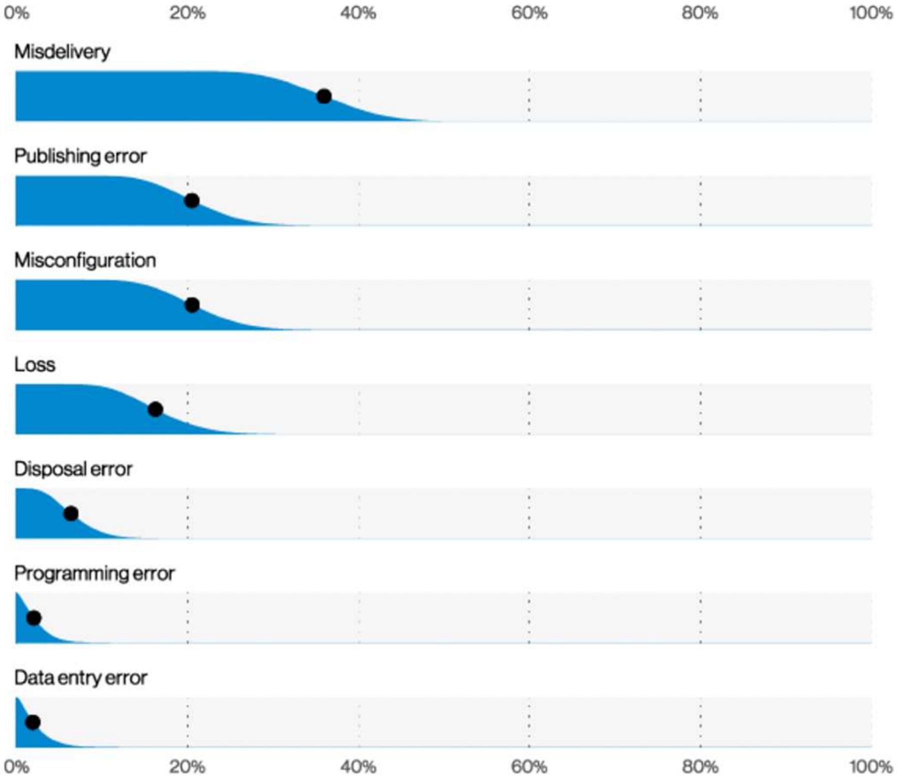
- Review and approve the organization’s cyber-risk appetite, or tolerance
- Instruct management to establish a consistent framework, using industry-accepted risk quantification models
- Require continuous examination of comparative measurements and metrics
- Base information security risk management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

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

Incident information





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?

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

Risk Management

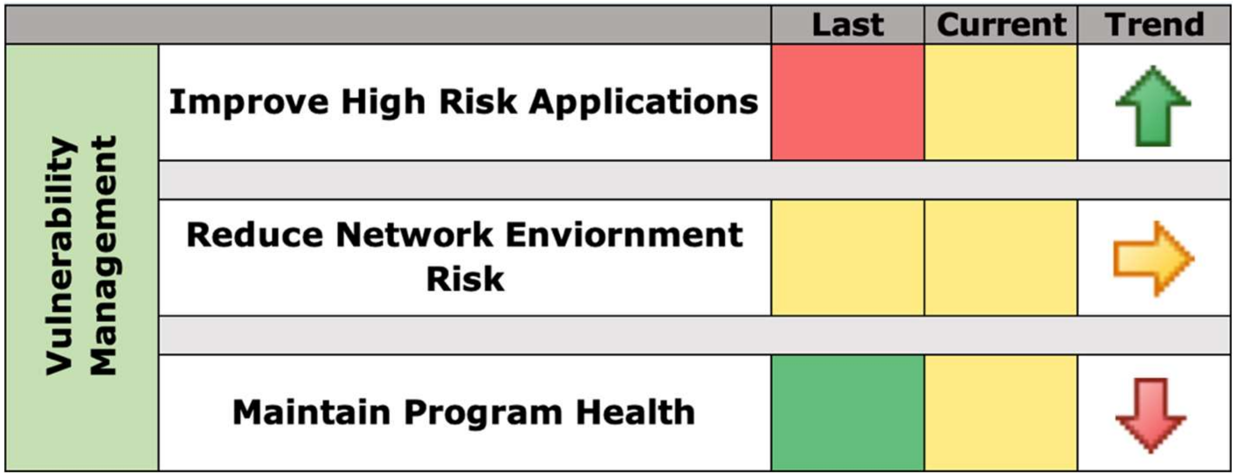
resources
security challenge challenge
financial manage finance
monitor concept investment
danger concept concept probability
idea probability
analysis
monitor idea
mitigation
security Risk Management monitor danger
measures monitor
assess resources security
business market identification resources
business assess hazard
finance
plan resources identification reduce
bank investment idea
financial investment
hazard control resources Risk Management identification market
Risk Management
financial measures strategy assess
monitor danger
plan risk identification risk assess control bank
risk economy
idea finance finance economy investment
danger security mitigation concept strategy
concept challenge financial analysis strategy
analysis manage bank control analysis
challenge analysis bank
business identification financial probability plan market
control strategy hazard economy
reduce
business Risk Management
mitigation financial
manage market manage measures
concept investment reduce

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

Security Performance (Example)

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

Vulnerability Management KPI

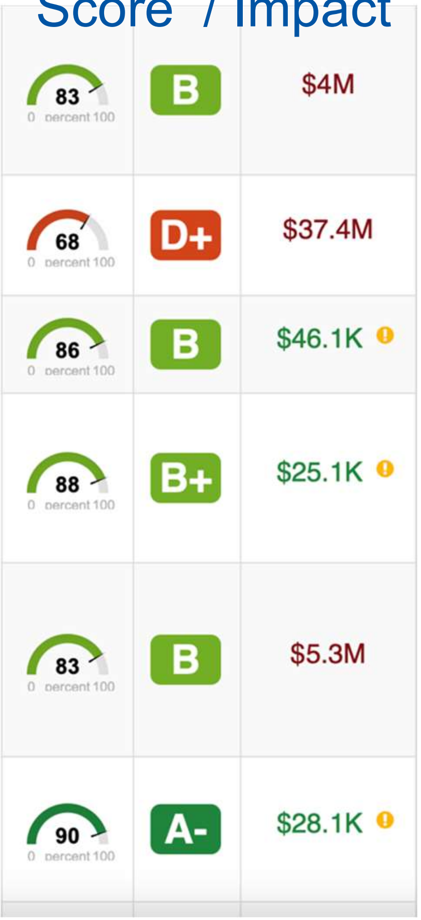


		Last	Current	Trend
Vulnerability Management	Improve High Risk Applications	🟥	🟨	⬆
	Reduce Network Enviornment Risk	🟨	🟨	➡
	Maintain Program Health	🟩	🟨	⬇

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 ❗

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

NIST CSF Risk Management Sample Measurement

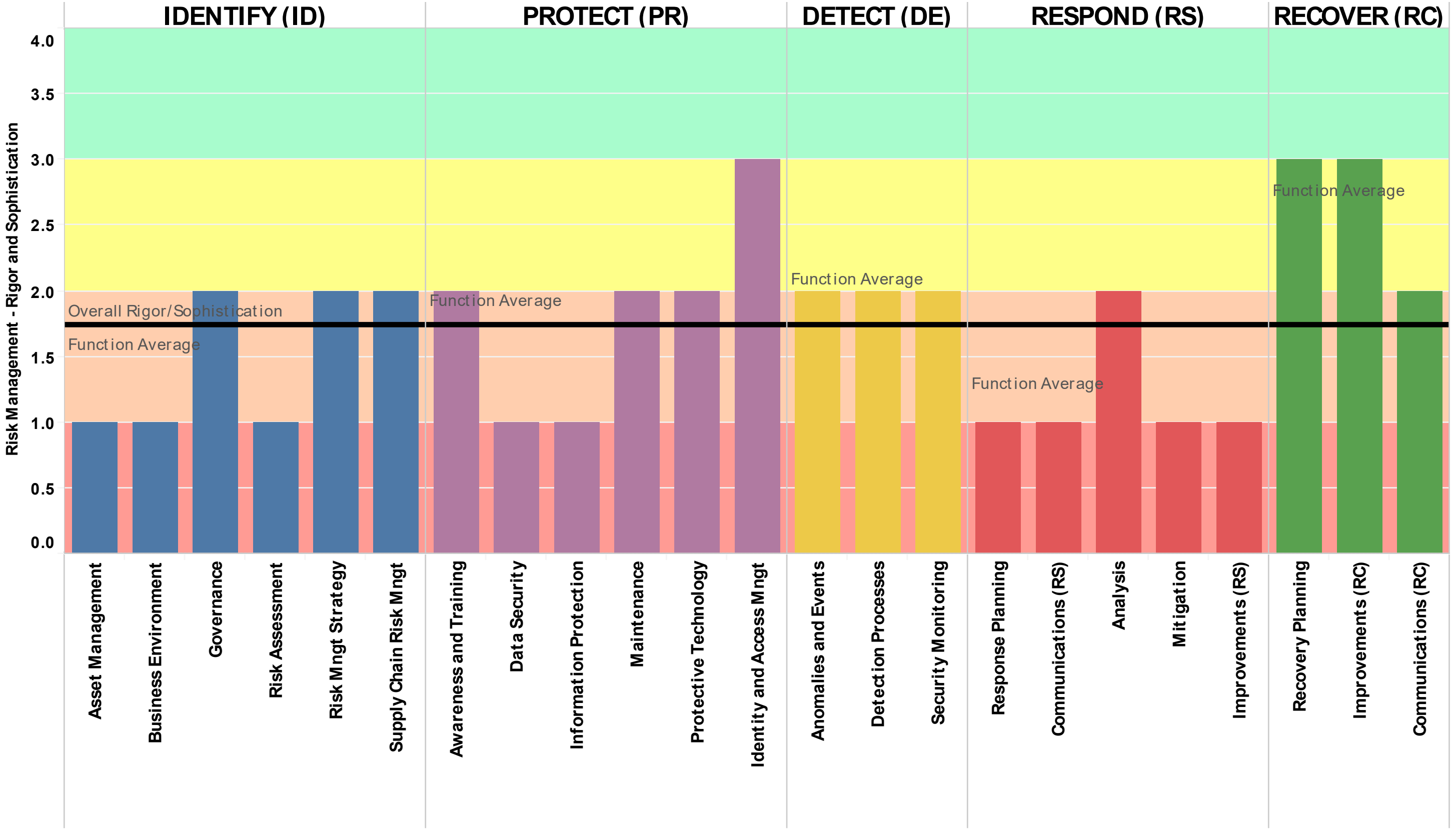
Rigor and sophistication of risk management

1 - Partial

2 - Risk Informed

3 - Repeatable

4 - Adaptive



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?

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

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

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?

Questions

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