New SEC Cyber Rules and Advancing Cyber Risk Governance
H-ISAC

Christopher Hetner
chetner10@gmail.com

1

Brief Introduction: Christopher Hetner

Business Strategy - Cybersecurity - Risk Management - Regulatory Compliance
25 years experience leading Cybersecurity & Operational Resilience in Public/Private Sectors

Chair Cybersecurity and Privacy, **NASDAQ Insights Council**
Cyber Risk Advisor, **NACD** (National Association of Corporate Directors)
Senior Advisor, **The Chertoff Group**
National Board Member, **Society of Hispanic Professional Engineers**

Former Affiliations:
Senior Cybersecurity Advisor, Chair of the **US Securities and Exchange Commission (SEC)**
Senior Member, **US Department of Treasury** Financial Banking Information Infrastructure Committee
United States Department of Homeland Security
Managing Director, **Marsh**
Cybersecurity Practice Leader, **EY Wealth and Asset Management and Private Equity**
Global Chief Information Security Officer, **GE Capital**
Senior Vice President Information Security, **Citi**

2

AGENDA

- Landscape
- Heightened Expectations
- Industry Trends
- Evolving Cyber Risk Reporting
- Key Takeaways

3

Landscape

Cybercrime to cost the global economy $10.5 Trillion annually by 2025 Cyber Ventures Report.

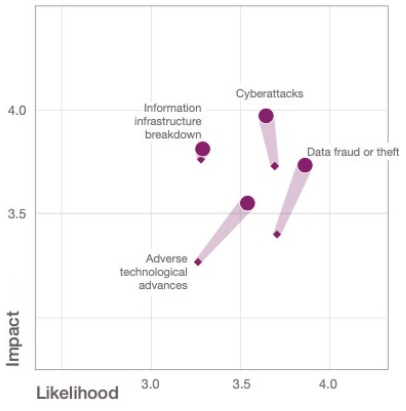
DHS continues to expand cybersecurity regulations to new sectors. Directives require critical sectors to respond and report incidents expands across the 16 critical sectors.

The current lack of cyber governance and the presence of cybersecurity blind spots increase the risk of a fragmented cyberspace and competing technology regulations creates complexity.

Heightened regulatory (SEC) expectations placed on the executive management and the board of directors (e.g., Sen. Reed's bill on disclosing cyber expertise on the board).

Increased focus on transparency (Twitter, Uber, etc…)

Material business interruptions causing write downs (Haynes Brands.. $100MM)



Source: World Economic Forum

4

Cyber Risk Governance Expectations

As cyber risk continues to become an empirical threat to the global economy and organizations, academia, business leaders, shareholders and regulators expect transparent and quantitative means for evaluating and understanding an organization's cyber risk exposure.

To address these heightened expectations, organizations need to understand the financial and business impact associated with cyber event risk.

Boards of directors and management are also expected to demonstrate to investors due care in the governance and oversight of cyber risk.

Moreover, global regulators continue to roll out privacy rules that are underpinned by the need for strong cyber hygiene with severe consequences for failure.

This represents a rising tide in the need for strong cyber risk oversight and will impact the decision-making and expectations from investors during the next decade.

5

5

Are We Prepared for Heightened Disclosure Requirements?

SEC 2018 Cybersecurity Disclosure Requirements: Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate time frame are disclosure controls and procedures that….

- ✓ *Establish an appropriate method of discerning the impact of cyber risks and incidents*
- ✓ *Protocols to determine materiality of cyber risks and incidents*
- ✓ *Alignment of cyber risks and incidents to the company and its business, financial condition, and results of operations*

In a September 2021 meeting with the U.S. Senate Committee on Banking, Housing and Urban Affairs, SEC Chair Gensler issued remarks on its cyber agenda: "Staff are developing a proposal for the Commission's consideration on cybersecurity risk governance, which could address issues such as cyber hygiene and incident reporting." Continued enforcement action from the SEC will encourage organizations to develop policies and procedures to manage and minimize their cyber-risk exposure, implement written internal guidelines, and proactively plan and adjust defenses as time progresses and technology improves.

Cause a knock-on effect in litigation and shareholder class actions…..

6

Proposed rule Public Company…

SEC Chair Gary Gensler Statement issued March 9, 2022

Today's release would enhance issuers' cybersecurity disclosures in two keyways:

First, it would require mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks. This would allow investors to assess these risks more effectively. For example, under the proposed rules, companies would disclose information such as:

- managements and the board's role and oversight of cybersecurity risks;
- whether companies have cybersecurity policies and procedures; and
- how cybersecurity risks and incidents are likely to impact the company's financials.

Second, it would require mandatory, material cybersecurity incident reporting. This is critical because such material cybersecurity incidents could affect investors' decision-making.

7

Statistics

Top 5 Threats

Healthcare
- Web Application Attacks
- Everything Else
- Error
- Crimeware
- PoS Intrusion

Insurance
- Web Application Attack
- DoS Attack
- Everything Else
- Error
- Crimeware

Manufacturing (Pharma)
- Crimeware
- DoS Attack
- Web Application Attack
- Everything Else
- Espionage

Retail (Pharmacies)
- Crimeware
- Web Application Attack
- Point of Sale Intrusion
- DoS Attack
- Everything Else

Losses/Mitigation/Assets

Loss Categories
- Misappropriation of Services (the ISAC needs to focus on integrity-based incidents)
- Misappropriation of Intellectual Property
- Misappropriation of Funds
- Ransomware
- Interruption
- Data Breach

Mitigation
- Network Monitoring and Defense
- Security Awareness Training
- Penetration Testing
- Data Protection (includes intellectual property)
- Audit Log Management

Asset Groups
- ICS, SCADA, OT protections related to crimeware, web application attacks, error, etc.
- Server protections related to web application attacks, crimeware, and everything else
- Critical IoT related to crimeware, everything else, and error (IoT is rapidly growing in this sector)

Average Loss Ratio = 3.5% of revenue
GDP at Risk in Healthcare = $250 billion in the USA

Source: X-Analytics and Cyber Insurance Losses

8

Loss Insights

From IRIS Report (Advisen Data)
•Healthcare makes up 16% of total reported volume
•The average loss is only $211k

HHS OCR Portal (data breached, >= 500 records)
•78.5% = hacking
•16.9% = unauthorized access and disclosure
•3.8% = theft and loss
•0.6% = improper disposal

DBIR Data
•95% of all incidents were due to financial motivation
•58% of all breaches included personal records, and only 46% included health records

BakerHostetler Data
•$875k was the average ransom paid in healthcare
•6.1 days was the average duration of ransomware incident

Sophos Data
•66% of healthcare hit with at least one ransomware incident
•72% of healthcare (inflicted with ransomware) used backup as the primary recovery tool

Large Ransomware Incident
•Tenet Healthcare = roughly $100 million in impact
•Scripps Health = $113 in impact

9

Cybersecurity is a business risk

Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims

The FBI assesses ransomware **actors are very likely using significant financial events, such as mergers and acquisitions,** to target and leverage victim companies for ransomware infections. Prior to an attack, ransomware actors **research publicly available information**, such as a victim's stock valuation, as well as material nonpublic information. If victims do not pay a ransom quickly, ransomware actors will **threaten to disclose this information publicly, causing potential investor backlash.**

Cybersecurity is not a technical risk.. It's a business risk. There is too much dialogue around the technological nuances around cybersecurity. Now is the time for the cybersecurity, investor, risk management and boardroom community to start **applying financial analytics** to the treatment of cyber risk.

As stated in the SEC 2018 Guidance… there's an expectation around the "Alignment of cyber risks and incidents to the company and its business, financial condition, and results of operations." Not sure what else needs to happen to incentivize companies. **The bad guys have them figured out!!**

[10] https://www.ic3.gov/Media/News/2021/211101.pdf

10

Boardroom Implications- NACD Principles

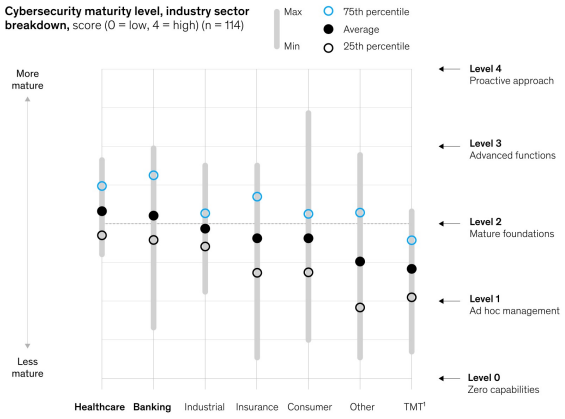
As cyber **capabilities continue to grow** and companies push the boundaries of digital transformation, it is imperative for **boards to oversee the development of effective strategies** to manage enterprise cyber risk. Boards should ask management the following questions:

- What is our financial exposure to cyber threats?
- What kinds of cyberattacks—and targeting what data and systems—could have the largest financial impact to our business?
- How much financial exposure are we accepting within the enterprise and through our digital supplier ecosystem?
- Are our digital initiatives being pursued in a cyber-resilient manner?
- What's our organization's unique risk profile and what's an acceptable level of risk?
- Are we making the right investments that materially reduce our cyber risk exposure?

https://blog.nacdonline.org/posts/financial-exposure-cyber-risk#comments

Why Are Organizations Experiencing Cyber Incidents?

Cybersecurity maturity varies within sectors more than it varies from sector to sector.



The fact:
Despite best efforts, most organizations still have not achieved a mature implementation of cybersecurity controls.

The reason:
Part of this is due to complexity, finite resources and lack of priority. But this is mostly due to the traditional use of cybersecurity metrics that don't resonate at the executive and corporate director level.

The resolution:
With the conversion of traditional cybersecurity metrics to financial details, executives and corporate directors will have the ability to determine if they can accept their financial impact due to cyber risk. If not, then they can prioritize risk remediation and transfer options.

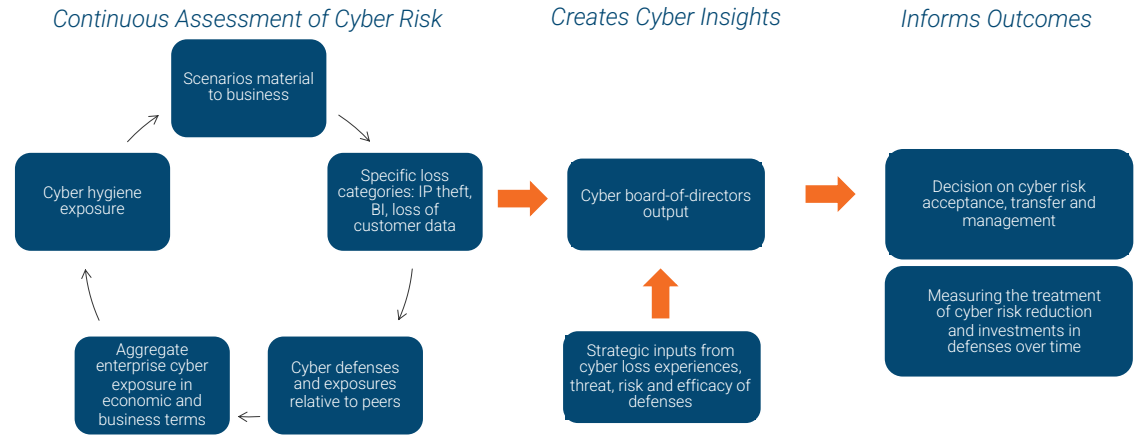
†Technology, media, and telecommunications.
Source: Crunchbase; McKinsey analysis

McKinsey & Company

Evolving Cyber Risk Governance Oversight and Reporting

What's Needed?

An approach that leverages a 360-degree enterprise view that aligns to cyber exposure/scenarios and economic exposure



13

Prepare for Heightened C-Suite and Board Engagement

Be prepared to address the following questions surrounding cyber risk:

- Which risks do we need to remediate?
- Which risks do we need to accept? (This answer could vary by business unit and stakeholder)
- Which risks do we need to transfer? (This includes options beyond cyber insurance.)
- How do we best prioritize our finite resources for our risk resilience journey?
- Is our current program effective, and if so, how do we know?
- How do we align cyber risks with all other enterprise-wide risks within the Corporate Risk Register?

14

Evolving Cyber Risk Reporting Requirements

As per the SEC Cyber Risk Governance Rule "materiality" determination is influenced by the incident and risk impact to the company's business, operations and financial condition. Below is an enumeration of the types of business and financial factors that should be contemplated when determining materiality:

The types of costs and adverse consequences that companies may incur or experience as a result of a cybersecurity incident include the following:

- Costs due to business interruption, decreases in production, and delays in product launches;
- Payments to meet ransom and other extortion demands;
- Remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;
- Increased cybersecurity protection costs, which may include increased insurance premiums and the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third-party experts and consultants;
- Lost revenues resulting from intellectual property theft and the unauthorized use of proprietary information or the failure to retain or attract customers following an attack; Litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;
- Harm to employees and customers, violation of privacy laws, and reputational damage that adversely affects customer or investor confidence; and
- Damage to the company's competitiveness, stock price, and long-term shareholder value.

15

Cyber Risk Reporting Deployed across the Boardroom Community

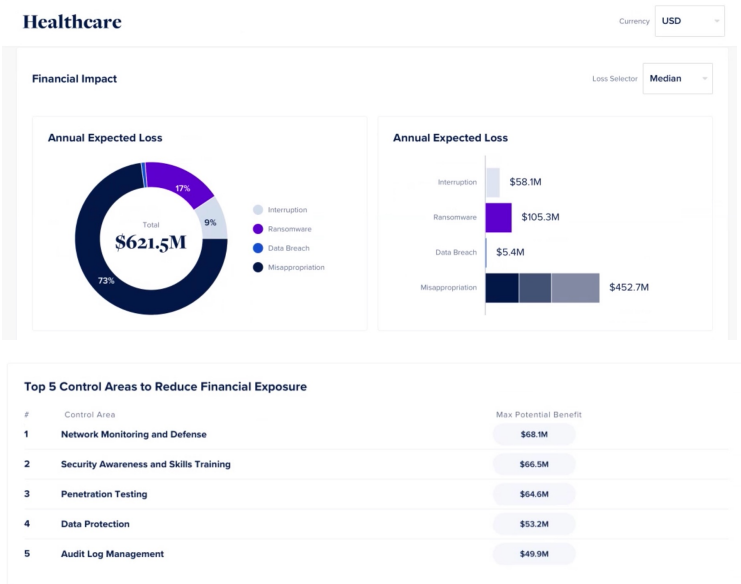
Building a bridge between business leadership and technologists using cyber economics as a shared vocabulary.

Maximizing cyber investments on technologies most likely to **reduce cyber risk**.

Focusing cyber efforts on threat scenarios most likely to impact the organization.

Aligning cyber budgets with overall business and enterprise risk management **priorities**.

Empowering business leaders to **improve cyber outcomes** through fiscal strategies.



16

17

Definitions

Data breach - A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. The expected loss value includes ID protection services, forensics, regulatory fines, brand damage, and many other cost elements.

Interruption (DoS) - A service interruption (denial-of-service attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The expected loss value includes revenue loss, forensics, recovery, brand damage, and many other cost elements.

Interruption (Non-DoS) - A service interruption (Non-DoS) is any cyber incident (via malice or error) that makes a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services. The expected loss value includes revenue loss, forensics, recovery, brand damage, and many other cost elements.

Misappropriation of Intellectual Property – Misappropriation is the intentional, illegal use of the property, or ideas of another organization for one's own use or other unauthorized purpose via a cyber event. The expected loss values includes value of trade secrets, loss profits, legal fees, and many other cost elements.

Misappropriation of Funds – Misappropriation is the intentional, illegal use of the funds of another organization for one's own use or other unauthorized purpose via a cyber event. The expected loss values includes value of stolen funds, loss profits, legal fees, and many other cost elements.

Misappropriation of Services – Misappropriation is the intentional, illegal use of IT services of another organization for one's own use or other unauthorized purpose via a cyber event. The expected loss values includes liability and revenue loss, legal fees, brand damage, and many other cost elements.

Ransomware - Ransomware is a subset of malware in which the data or system instructions on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data or system instructions are decrypted and access returned to the victim. The expected loss value includes extortion, revenue loss, equipment and data replacement, brand damage, and many other cost elements.

18