



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Understanding Cyber Risk





Mr. Daniel Dobrygowski
Head of Governance and Trust
Centre for Cybersecurity
World Economic Forum, USA

1

Topics Covered

01

What is Cyber Risk?

02

Leadership and Cyber Risk

03

How to Think Strategically about Cyber Risk

04

Resources for Understanding Cyber Risk

2

Take-Aways

>

Cyber risk is a **pervasive and existential** organizational risk

>

Leaders need to account for cyber risk in determining strategy

>

Organizations can set a **risk appetite** for cyber risk just as they do for other risks

e.g.,

• Financial risk

• Reputational risk

3



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Take-Aways

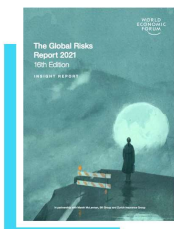
- Cyber risk is a **pervasive and existential** organizational risk
- **Leaders** need to account for cyber risk in determining strategy
- Organizations can set a **risk appetite** for cyber risk just as they do for other risks
- Cyber risk must be understood and communicated in terms that are **relevant to the purpose and strategy** of the organization
 - Economic
 - Human Impact
 - National Security

Risks Reports

Cyber risk has significant
organization and system-wide impacts

4

Risks Reports



Cyber attacks are one of the **top 10 risks** that any organization faces in terms of **likelihood** and **impact**


By 2021, **\$6 trillion** in value will likely be lost to cybercrime

Source:
- World Economic Forum, Global Risks Report, 2021.
- Morgan, Steve, Global Cybercrime Damages Predicted To Reach \$6 Trillion Annually By 2021, Cybercrime Magazine, Cybersecurity Ventures [Link to Report in the Links Tab]



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Organizational or Business Risk




Risk is

THE EFFECT OF UNCERTAINTY ON OBJECTIVES

Source:
NIST Special Publication 800-160 vol. 1, Systems Security Engineering, at page 170, 2016; see also, International Organization for Standardization (ISO) Guide 73:2009, Risk management - Vocabulary, November 2009.

5

Organizational or Business Risk



Risk is

A MEASURE OF THE EXTENT TO WHICH AN ENTITY IS THREATENED BY A POTENTIAL CIRCUMSTANCE OR EVENT, AND TYPICALLY A FUNCTION OF:

The adverse impacts that would arise if the circumstance or event occurs

The likelihood of occurrence

Source:
NIST Special Publication 800-30 rev. 1, Guide for Conducting Risk Assessments: Information Security, at B-9, 2012.

6

Cyber Risk

Cyber risk is a risk arising from an organization's technical infrastructure or the use of technology within an organization

- Threats to the IT infrastructure or digital connectivity are potentially existential threats to the business as a whole



6



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Cyber Risk: Adverse Cybersecurity Outcome

EXPLOITS

CAUSING

Cyber Threat

Vulnerability

Adverse Cybersecurity Outcome

Disgruntled employee (Insider) uses administrator privileges to download customer data without authorization

Confidentiality: releasing customers' personal banking details on the dark web

Outside attacker exploits default passwords on operational technology systems to insert malicious code

Integrity: manipulating sensors causing machinery to malfunction

Cyber criminals install ransomware through phishing attack that locks all systems on network

Availability: preventing access to business data and systems

Source: NIST Special Publication 800-30 rev. 1, Guide for Conducting Risk Assessments: Information Security, at pp. 8-12, 2012.

7

Cyber Risk & Organizational Risk

EXPLOITS

CAUSING

Cyber Threat

Vulnerability

Adverse Cybersecurity Outcome

Disgruntled employee (Insider) uses administrator privileges to download customer data without authorization

Confidentiality: releasing customers' personal banking details on the dark web

Organizational Risk ("Value-at-Risk")

Operational disruption

Regulatory action

Loss of reputation

Loss of revenue

Loss of shareholder value

Direct financial loss (e.g. fraud)

Harm to individuals

National security concerns

Source: NIST Special Publication 800-30 rev. 1, Guide for Conducting Risk Assessments: Information Security, at pp. 8-12, 2012; World Economic Forum, Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, 2015.

8

Leadership and Cyber Risk







Cyber risk is a **strategic issue** that must be addressed at the highest levels of leadership

9



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA


Cyber-Aware Leadership
for Business




Source: World Economic Forum, National Association of Corporate Directors and Internet Security Alliance, Principles of Cyber Risk Governance, 2021.

10


Cyber-Aware Leadership
for Business




Treat cybersecurity as an enterprise-wide strategic issue




Incorporate cybersecurity expertise into board governance




Understand the economic impact of cyber risk



Ensure organizational design supports cybersecurity



Align cyber risk management with business needs



Foster systemic resilience and collaboration

Source: World Economic Forum, National Association of Corporate Directors and Internet Security Alliance, Principles of Cyber Risk Governance, 2021.

Aligning Cyber Risk
to Organizational Goals



Economic



Human Impact



National Security

11



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

How to Think Strategically about Cyber Risk

Categories of Risk	Countermeasures
I. Preventable Risks Example: Ransomware attack causing significant downtime	Compliance/Operational <ul style="list-style-type: none">▪ Creating rules▪ Monitoring processes
II. Strategy Risks Example: AI implementation exposes company to manipulation of underlying data	Governance/Strategy <ul style="list-style-type: none">▪ Setting risk appetite▪ Defining organization strategy▪ Oversight
III. External Risks Example: Nation-state attack on critical network infrastructure	Governance/Strategy <ul style="list-style-type: none">▪ Identifying organization-wide risks▪ Planning for mitigation

Source : Kaplan, Robert S. and Anette Mikes, Managing Risks: A New Framework, Harvard Business Review, 2012.

12

Acting Strategically on Cyber Risk

➤ How do you act strategically about cyber risk?

Source: Dobrygowski, Daniel and Derek Vadala, Does Your Board Really Understand Your Cyber Risks?, Harvard Business Review, 2020.

13

Acting Strategically on Cyber Risk

1. 2. 3.

Source: Dobrygowski, Daniel and Derek Vadala, Does Your Board Really Understand Your Cyber Risks?, Harvard Business Review, 2020.



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Acting Strategically on Cyber Risk

Define Risk Appetite

- Understand your risks
- Check stakeholder expectations
- Look to peer organizations

Establish a Cybersecure Culture

- Encourage responsibility
- Think holistically

Focus on Outcomes

- Relate to organizational goals
- Calibrate expectations

Source: Dobrygowski, Daniel and Derek Vadala, Does Your Board Really Understand Your Cyber Risks?, Harvard Business Review, 2020.

Example: 2020 Coronavirus Pandemic & Cyber Strategy

Business Risk
Strategy Risk:
downtime from lost productivity vs. greater exposure to cyberattacks

Shift to work from home

Threat
No change?

Vulnerability ↑

Adverse Cyber Outcome
Cyberattacks and data fraud

STRATEGY
Determined by enterprise-wide risk appetite and assessment

Business Risk
External Risks: not based on strategic choices, initiated by cyber criminals

Attacks on vaccination research institutions

Threat

Vulnerability ↑

Adverse Cyber Outcome
Breach resulting in data exposure

STRATEGY
Assessment of risk; plan for prevention and mitigation; cooperation with law enforcement

Source:
- World Economic Forum, Cybersecurity Leadership Principles: Lessons learnt during the COVID-19 pandemic, 2020;
- World Economic Forum, COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications, 2020

14

Example: 2020 Coronavirus Pandemic & Cyber Strategy

Business Risk
Strategy Risk:
downtime from lost productivity vs. greater exposure to cyberattacks

Shift to work from home

Threat
No change?

Vulnerability ↑

Adverse Cyber Outcome
Cyberattacks and data fraud

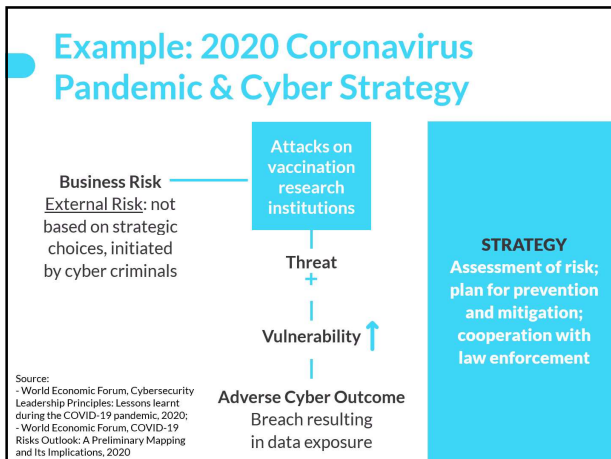
STRATEGY
Determined by enterprise-wide risk appetite and assessment

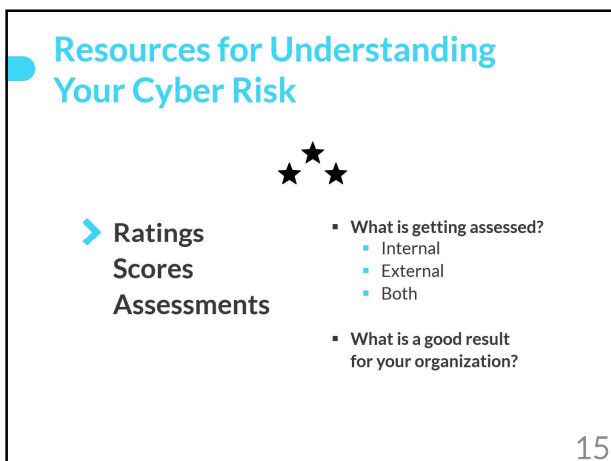
Source:
- World Economic Forum, Cybersecurity Leadership Principles: Lessons learnt during the COVID-19 pandemic, 2020;
- World Economic Forum, COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications, 2020



Mr. Daniel Dobrygowski –

Head of Corporate Governance and Digital Trust, World Economic Forum, USA









Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

Resources for Understanding Your Cyber Risk

> Experts

- Who are the internal experts?
- How do external experts supplement?
- Who do they advise?

Cooperating on Cyber Risk

> Information Sharing and Analysis Centers (ISACs)

Help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.

ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency

> Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)

Source: National Council of ISACs, About ISACs, 2020.

16

Cooperating on Cyber Risk

> Information Sharing and Analysis Centers (ISACs)

> Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)

Expert partnerships between government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks.

Can be regional, industry-based, or both

Source: National Council of ISACs, About ISACs, 2020.



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

To Learn More

[World Economic Forum: Cyber Risk, Leadership, and Corporate Governance Initiative](#)
[Link to the WEF report on the Links Tab]

Report – *Principles for Board Governance of Cyber Risk* (2020)
(with NACD, ISA, and PwC)

Report – *Advancing Cyber Resilience: Principles and Tools for Boards* (2017)

[National Association of Corporate Directors \(USA\): Cyber Risk Oversight Resource Center](#)

[Internet Security Alliance](#)

Report – *Director's Handbook on Cyber-Risk Oversight* (2017, updated 2020)

[Federation of European Risk Management Associations](#)

Report – *At the Junction of Corporate Governance & Cybersecurity* (2018)

17

To Learn More

[National Cyber Security Centre \(UK\): Cyber Essentials](#)

Report – *Cyber Security Toolkit for Boards* (2019)

[Berkeley Center for Long Term Cybersecurity](#)

Report – *Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk* (2020)

[Carnegie Endowment for International Peace: Cyber Policy Initiative](#)

Report – *Board-Level Guide: Cybersecurity Leadership* (2020)

Take-Aways

- Cyber risk is a **pervasive and existential** organizational risk
- **Leaders** need to account for cyber risk in determining strategy
- Organizations can set a **risk appetite** for cyber risk just as they do for other risks
- Cyber risk must be understood and communicated in terms that are **relevant to the purpose and strategy** of the organization
 - Economic
 - Human Impact
 - National Security
- **Understanding cyber risk is important, and there is help if we work together!**

18



Mr. Daniel Dobrygowski –
Head of Corporate Governance and Digital Trust, World Economic Forum, USA

