ADACOM
CYBER SECURITY

The value of visibility:

Optimize your Cyber Risk Strategy

Organizations are living social constructs

- Systems theory says that organizations are social systems that
  - ✓ are influenced by their surrounding environment
  - ✓ influence their environment with their outcomes (i.e. products, services)
- Organizations are influenced by
  - ✓ Opportunities (i.e. technology advancements)
  - ✓ Risks (i.e. climate change, disasters)

Organizations are social systems

Organizations are living social constructs

In order to **survive** in a constantly changing environment, organizations need to:

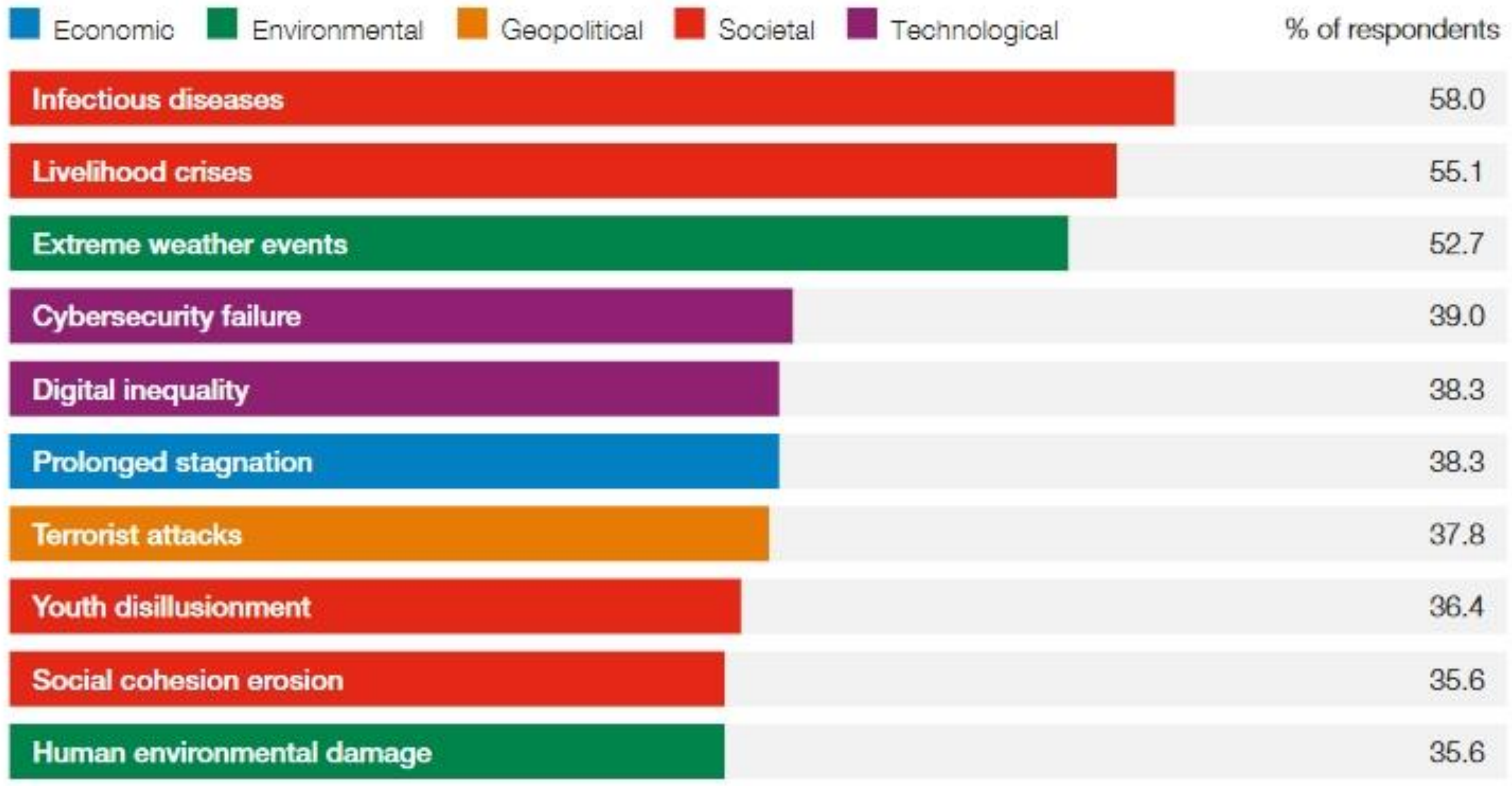
✓ **Adapt** to environmental changes
Reflect on the effectiveness of their internal processes

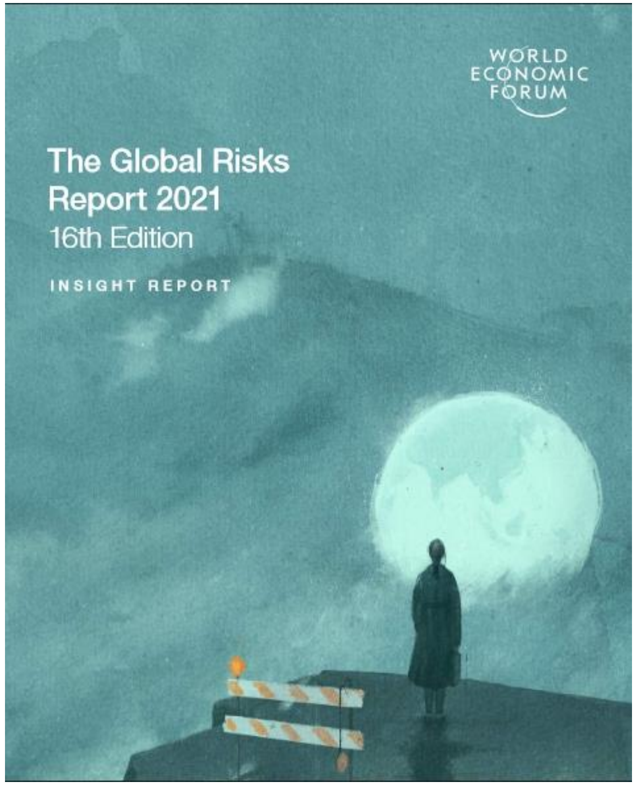
The reaction of most businesses during the disruptive 2020 is a fine example of how organizations **adapt to even violent changes** in their operating environment in order to survive

✓ **Work from home** strategies
Cloud-based services

✗ **Businesses that failed to adapt eventually closed down**

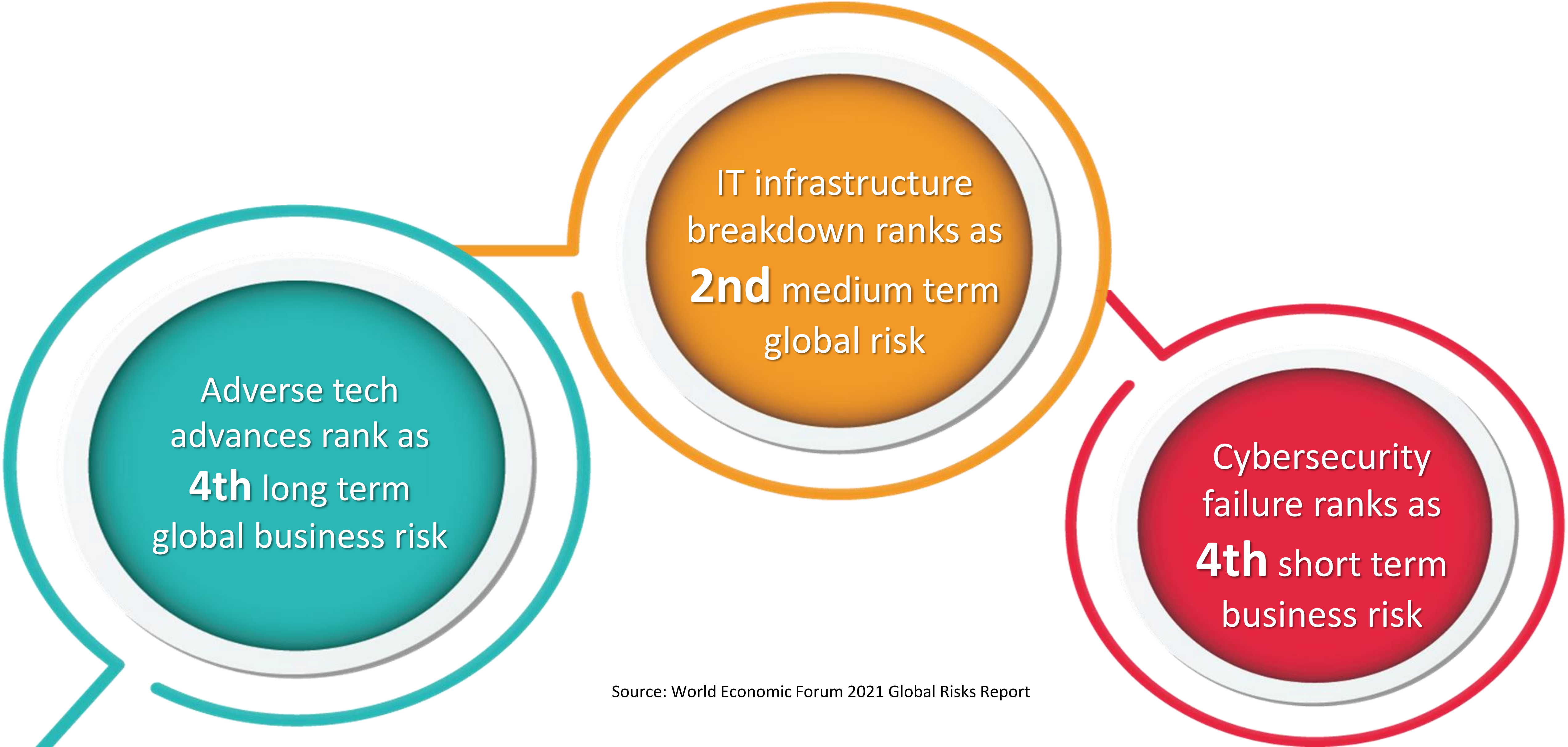
Global risks to doing business





***Executives** and **board members** in organizations of every size and sector recognize that they need to respond to transformational forces that are global and highly complex*

Cyber risks are business risks



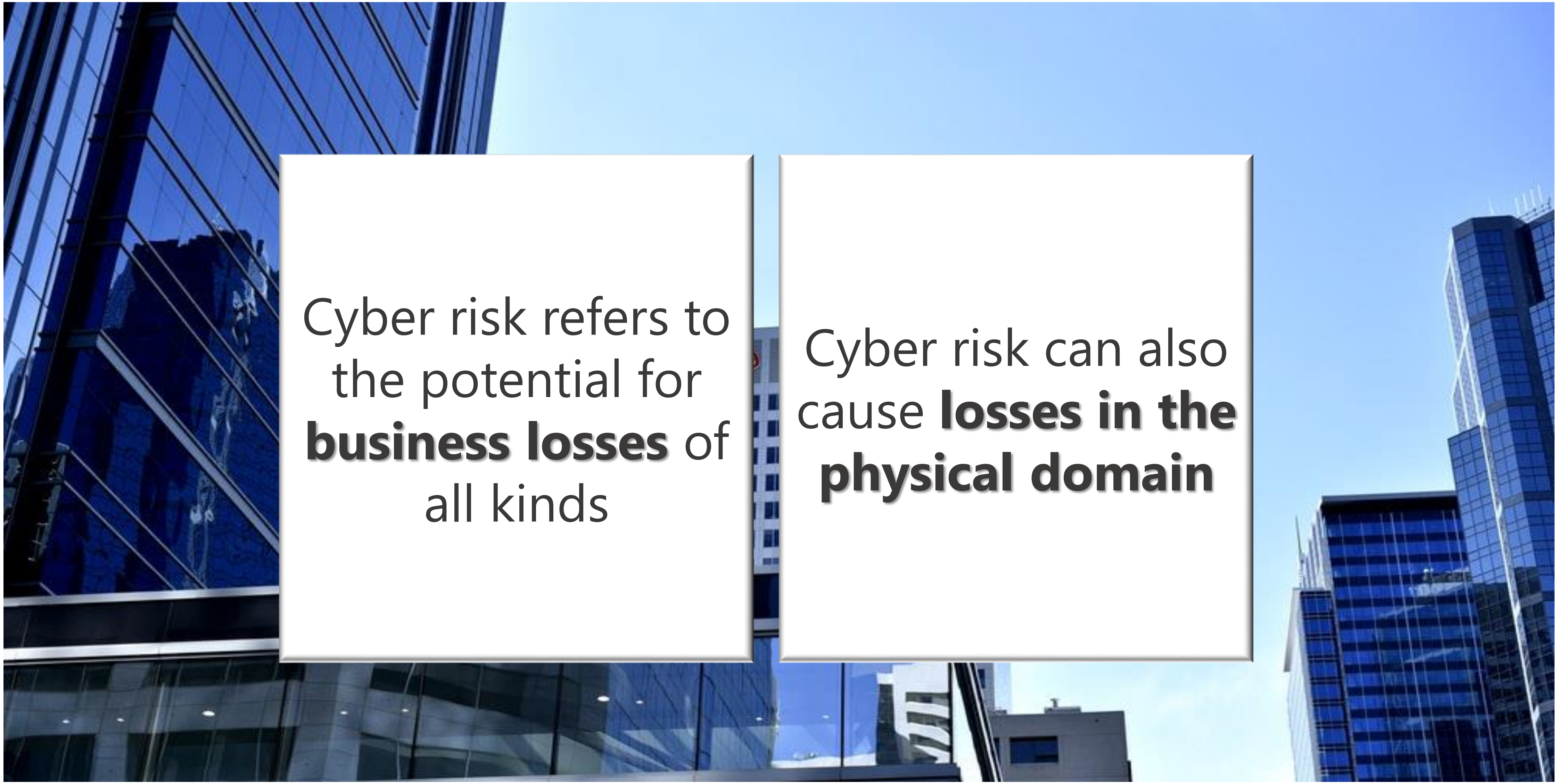
Adverse tech advances rank as **4th** long term global business risk

IT infrastructure breakdown ranks as **2nd** medium term global risk

Cybersecurity failure ranks as **4th** short term business risk

Source: World Economic Forum 2021 Global Risks Report

Cyber risks are business risks – The Damages

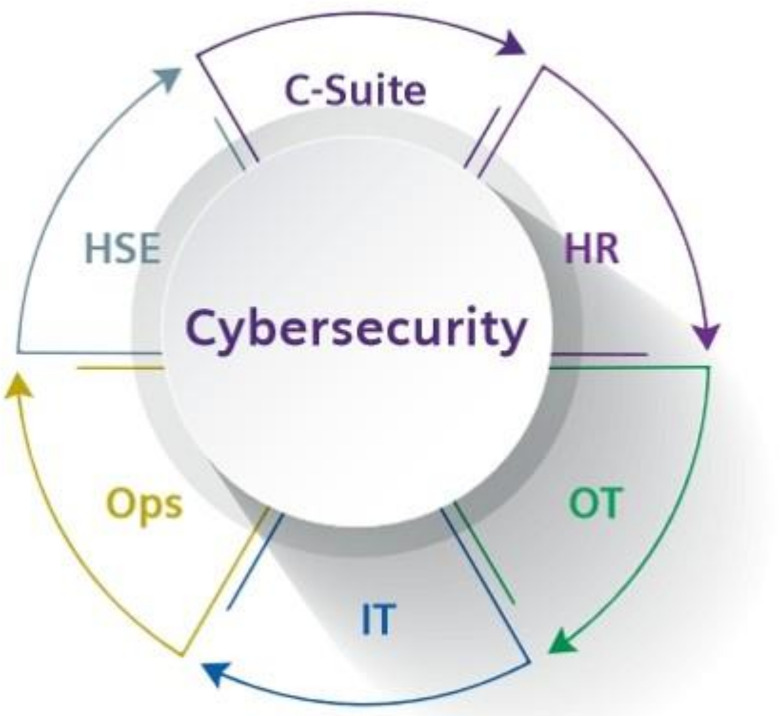


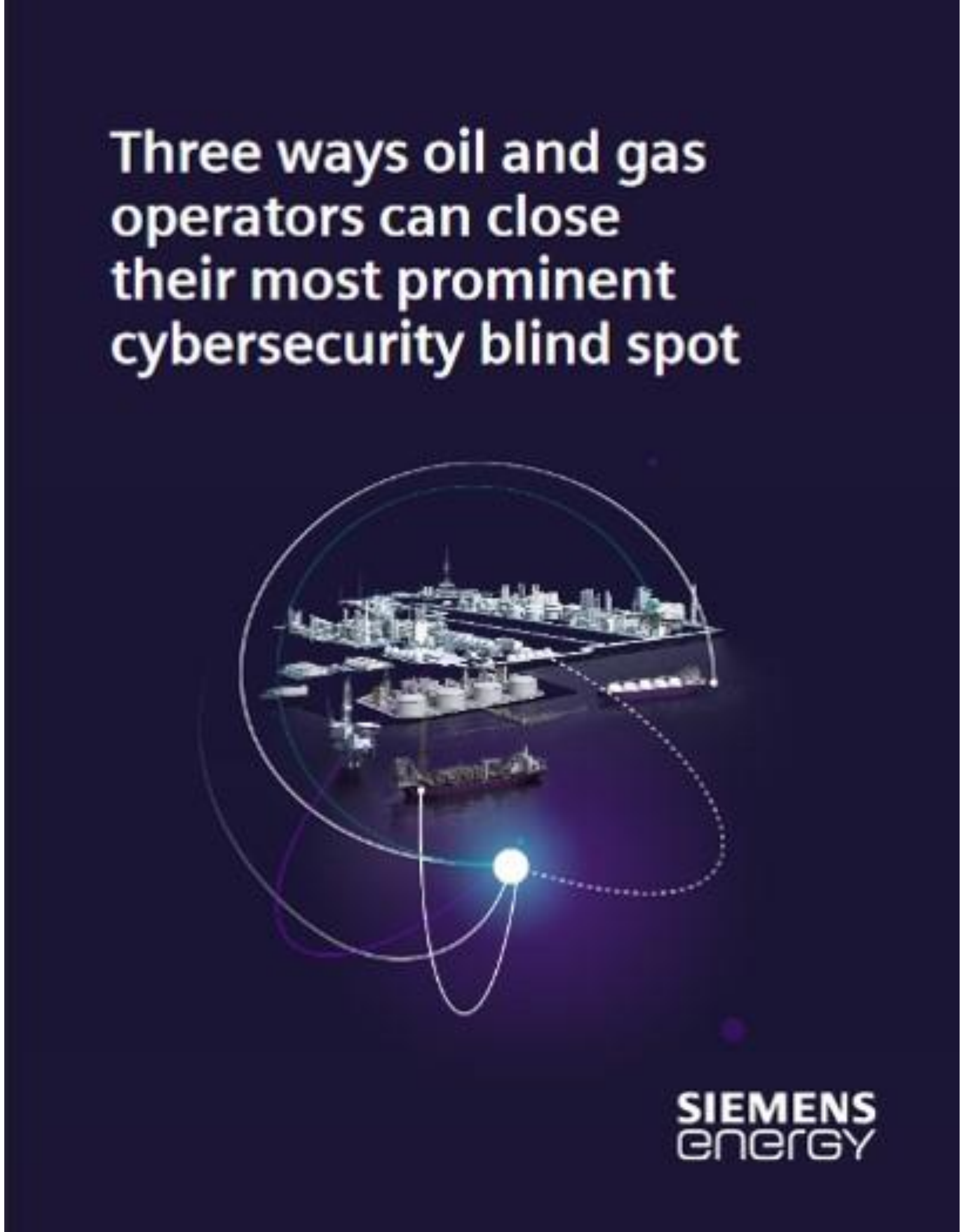
Cyber risk refers to the potential for **business losses** of all kinds

Cyber risk can also cause **losses in the physical domain**

Cyber risks are business risks

> “**Cybersecurity** should be a shared responsibility of all employees in a company, from the executive suite to close collaboration among OT, operations, and enterprise IT ”





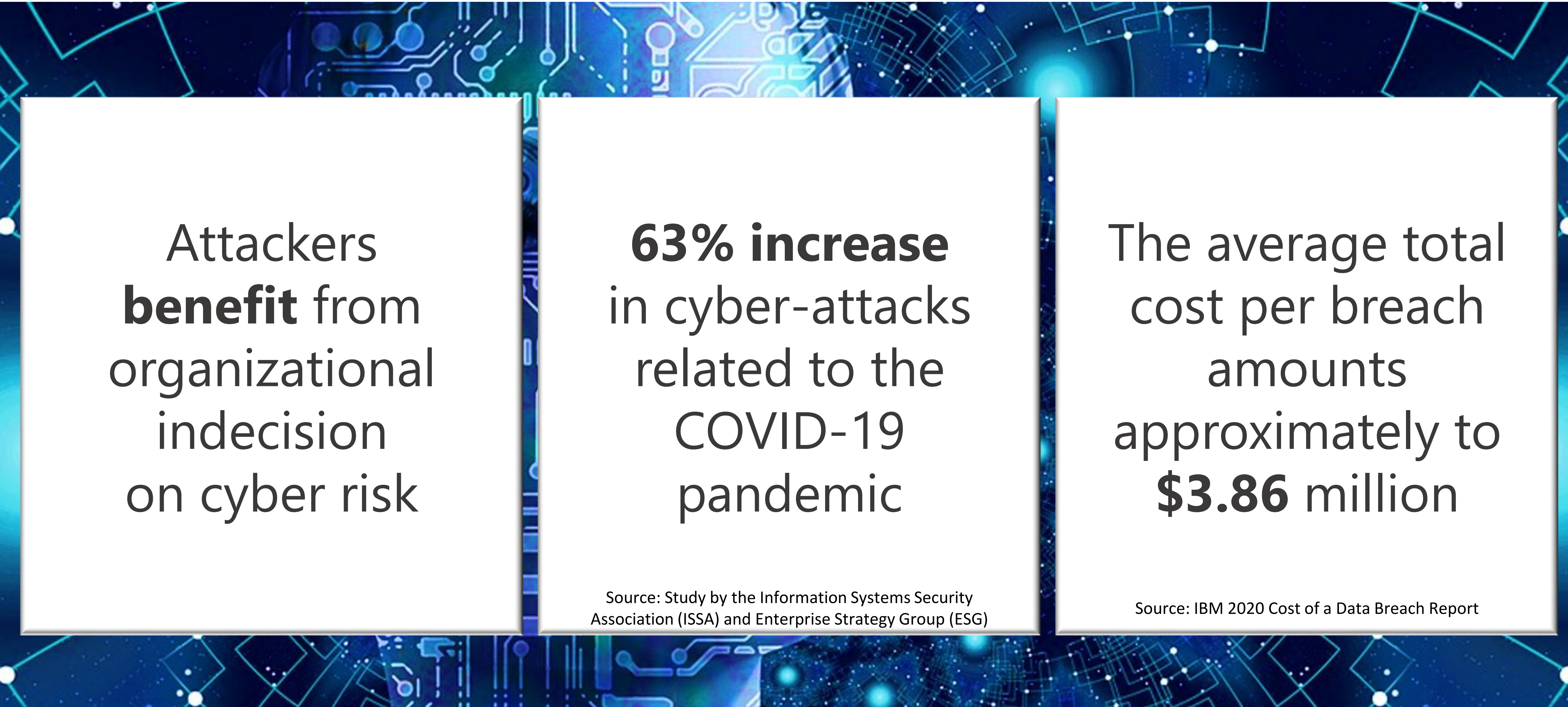
Three ways oil and gas operators can close their most prominent cybersecurity blind spot

SIEMENS energy

Need to understand what cyber risks are

- ✓ Which projects could most **reduce enterprise risk**?
- ✓ What methodology should be used that will make clear to enterprise stakeholders (especially in IT) that those priorities will have **the greatest risk reducing impact** for the enterprise?
- ✓ To decrease enterprise risk, leaders must **identify & focus** on the elements of cyber risk
- ✓ We need to advance a **"risk based" approach** to cybersecurity

The impact of lack of risk visibility



Attackers **benefit** from organizational indecision on cyber risk

63% increase in cyber-attacks related to the COVID-19 pandemic

Source: Study by the Information Systems Security Association (ISSA) and Enterprise Strategy Group (ESG)

The average total cost per breach amounts approximately to **$3.86** million

Source: IBM 2020 Cost of a Data Breach Report

Maturity-based approach is not adequate

- ⊗ *"Build everything and everywhere"*
- ⊗ *"Monitor everything"*
- ⊗ Ineffective spending
- ⊗ Unable to measure how and how much risk is reduced
- ⊗ Overwhelmed teams with little progress

Risk visibility enhances your cyber strategy

There are a variety of factors causing your enterprise's attack surface to expand faster than ever before:

The ongoing migration to the cloud

The widespread shift to remote work

Extensive and complex supply chains and inherited

Data privacy and sovereignty regulations

Risk visibility enhances your cyber strategy

The **risk-based** approach benefits your organization in many ways, including:

✓**Designates risk reduction as the primary goal**. This enables the organization to prioritize investment based on a cyber program's effectiveness in reducing risk.

✓**Transforms the Board's risk-reduction targets** into measurable, realistic implementation programs with clear alignment from the board to the front line.

How to optimize your cyber risk strategy

1. Embed cybersecurity in the enterprise risk management framework.
2. Define the sources of enterprise value.
3. Understand the organization’s enterprise-wide vulnerabilities—among people, processes, and technology—internally and for third parties.
4. Understand the relevant threat actors, their capabilities, and their motive.
5. Link the controls to the vulnerabilities that they address and determine what new efforts are needed to close the gap.
6. Map the enterprise risk ecosystem: the threat actors and their capabilities, the enterprise vulnerabilities they seek to exploit, and the cybersecurity controls.
7. Plot risks against the enterprise-risk appetite and report on how cyber efforts have reduced enterprise risk.
8. Monitor risks and cyber efforts against enterprise risk appetite.

Instead of a conclusion

> “*Imagine a world in which all types of entities could convey the effectiveness of their cybersecurity risk management in a standardized, non-technical way, appropriate to each entity’s size and other business characteristics. Think about the power of such assurance. Boards, shareholders, customers, counterparties, and regulators could gauge the relative effectiveness of organizations’ cybersecurity and resiliency. If done right—with independence, objectivity, appropriate expertise, and professional skepticism—such an assurance process would be a vehicle by which greater cybersecurity and resilience could be achieved.*”

Remarks by Deputy Secretary Sarah Bloom Raskin at the Public Company Accounting Oversight Board International Institute on Audit Regulation, December 14, 2016

Thank You

ADACOM
CYBER SECURITY

United Kingdom
8950 Fitness Lane,
Suite 100 Fishers,
IN 46037
+44(0) 317 588 3131

Greece
Kreontos St. 25,
104 42
Athens
+30 210 5193740

Cyprus
10 Katsoni Str.,
1082,
Nicosia
+357 22 444 071

info@adacom.com