Cybersecurity in the sustainable investment process

- **WHY INTEGRATE CYBER RISK INTO THE INVESTMENT PROCESS**
- **MEASURING AND VALUATION OF THE CYBER RISK**
- **ENGAGING ON THE CYBER RISK SCORE**

White paper for cyber security experts and professional investors

April 2021

Vincent Toms
https://www.linkedin.com/in/vincenttoms/

Three things are clear:

- Cybercrime is rising
- The world is becoming more digitalized
- And… everything can be hacked

Cybersecurity and (non) compliance has never been so important a topic for investors to consider as it is today.

Contents

Introduction

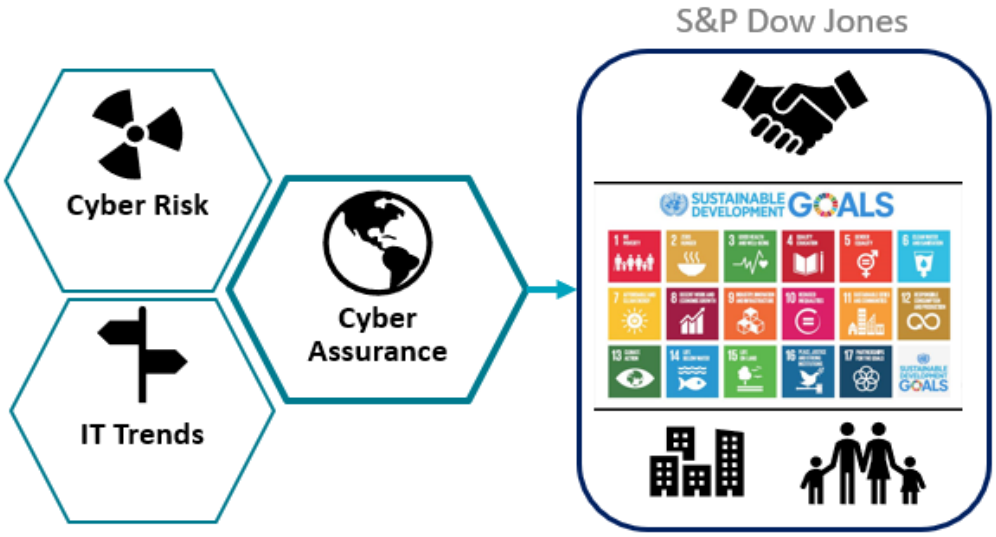
According to the World Economic Forum's report on global risks, cybersecurity is ranked as one of the top five risks to businesses, reaffirming the need for company boards to prioritize this issue.

Although companies are increasingly recognizing cyber risks and their impacts, corporate information in the public domain does not reassure others that companies have adequate governance structures and measures in place to deal with cyber security challenges.

The current lack of public disclosure still makes it difficult for investors and buyers of a service/ product to differentiate between those companies that are proactively developing, monitoring and managing cyber security risks versus those failing to prioritize these risks.

The United Nations has also set forth a set of SDG's to raise awareness to the need to be sustainable and resilient. One of the topics in the globally agreed on sustainability framework, is Cyber Security. As the IT covers multiple sectors and provides solutions to achieve the SDG's, cyber security has a direct impact on all of the SDG's.

With this paper we provide investors and cyber security experts insight in why to integrate cyber risk in the investment process, how to measure the cyber risk and the importance of engagement to create a safer and better world.



Integrating cyber risk into the investment process

Cybersecurity – or rather cyber-insecurity – is becoming a more important topic in analyzing a company. This element needs to be taken into account in addition to the financial attractiveness and the general ESG analysis.

Although cybersecurity should be an important consideration everyone, it is obvious that the impact is even larger for digitally oriented companies. The number of companies that rely on digital business models or are placing more of their business online, is growing fast. Therefore, cybersecurity analysis must also keep pace with this growing trend. The only problem is that there is no clear framework for testing it, nor is there an auditable standard for reporting on it. In order to tackle the analysis question, it is therefore important to develop such a framework, and use that to define a blueprint for company's reporting standards, as has been done for many years on ESG.

The challenge of an international Cyber Security disclosure

While there are disclosure problems, things do move on, as sustainable investing and ESG adoption increasingly moved into the mainstream. A decade ago, there were not many companies reporting on their gender diversity policy, water usage, CO2 emissions and many more ESG-related topics. Today, that information is becoming more widely available, and reporting is becoming more standardized.

While we are a long way from standardized cybersecurity reporting, there are many widely available policies and best practices that companies can use to report on their digital environment and security. IMF's report 'Central Bank Risk Management, Fintech and Cybersecurity' confirms this situation. Of the 1,095 AIV technology search hits, only 3 AIVs could be found with explicit references to cybersecurity.[i]

Although there is no proven correlation yet between the execution of best practices and the risk of actually being hacked, or enduring a substantial financial impact from cyber incidents, it makes sense from a risk perspective to demand for more cyber security assurance in the public disclosure.

Establishing a Cyber Risk baseline

The differences that emerge between companies in terms of their cyber governance serve as a discussion point and will eventually have an impact on the portfolio weighting process. Not adhering to best practices can lead to higher risk of cyber incidents and other governance-related issues, and should therefore be taken into account in the positioning decision. Although we have discussed cybersecurity from a risk perspective, it also serves as a means of screening for opportunities. The likelihood of severe business disruption with a strong cyber risk approach could be translated into a higher cybersecurity rating.

‘The number of companies that rely on digital business models, or are placing more of their business online, is growing fast. Therefore, cybersecurity analysis in the investment process must also keep pace with this growing trend’

The importance of a international evidence based Cyber Risk baseline

One of the attractive elements of when analyzing cybersecurity risks is that the approach is partly evidence based. If a company states that it has a cybersecurity policy on e-mail routing, for example, this should be verifiable by using tools that test those claims. The feedback from those tools serves as evidence of the execution of best practices and guidelines in reality, rather than on paper. This also makes it possible to communicate the issues with management and test progress over time. This can then serve as another input in the decision-making process.

Summing it up: cybersecurity will become much more important in the research process, as well as in portfolio construction. Having the right tools to analyze cyber risks is essential. and companies that report on cyber-related topics in an auditable way will have a great competitive advantage.

The impact of Cybersecurity on the stock price

Cyber attacks can affect the interests of all stakeholders, disrupting a company’s operations, affecting how its employees work and inflicting brand damage that can severely jeopardize customer loyalty and trust. A breach can also impact sensitive information related to clients, contractors and suppliers. However during the last couple of years we haven’t seen much impact of a data breach, GDPR penalty or for instance ransomware for the stock price. But the impact of cybersecurity on the SDG’s and our environment is enormous. While the digital transformation fuels innovation and creates whole new ways of doing business, there are new risks, led by increasingly sophisticated cyberattacks, and affects almost everyone.

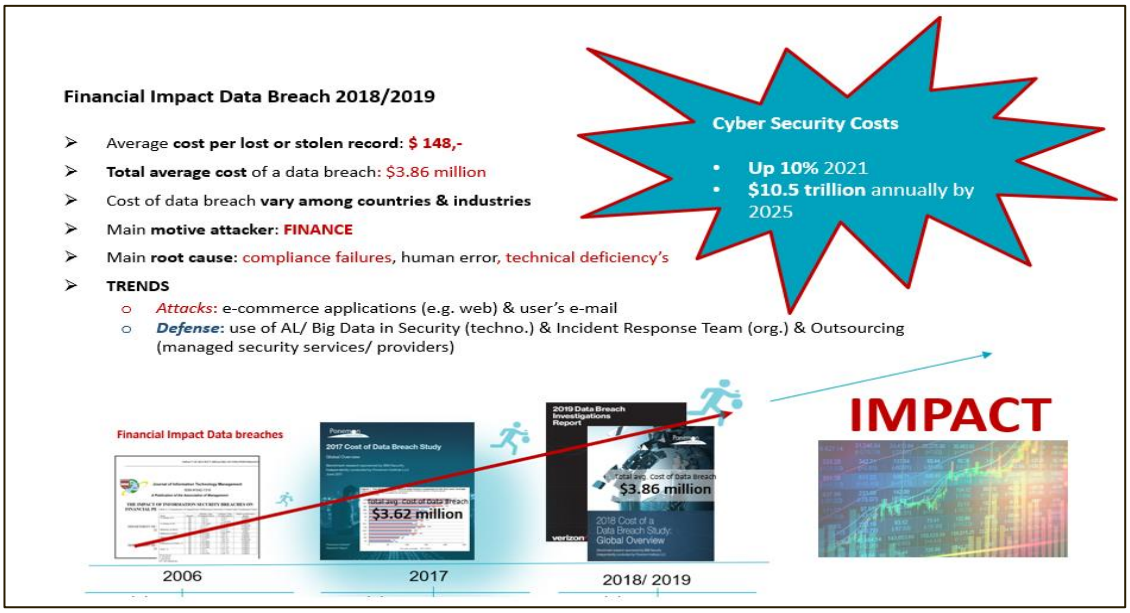


Figure 1 | Impact of Cyber Risk

The investigation showed that the cost of a lost or stolen record has gone up but didn’t have any effect on the stock price of the entity that was hit by an data breach. The same was seen if a entity gets hit by

ransomware. Although cybercrime will cost the world $10.5 trillion annually by 2025. But also the necessary extra investment in cyber security seems to have none effect on the stock price. The worldwide cybersecurity spending's are to increase 10% in 2025[ii] and the total costs on Cyber security spending's is heading up for $200 billion a year by 2024.[iii]

The impact of SDG's and Cybersecurity

Sustainability and social involvement play an increasingly important role in the portfolios of institutional investors. The SDG score also narrows down the possibilities in the investment process as entity's need to score a certain level. **According to Bloomberg[iv] the Global ESG assets are on track to exceed $53 trillion by 2025, representing more than a third of the $140.5 trillion in projected total assets under management**. In the 2019 RBC Global Asset Management Responsible Investment Survey it states that of the nearly 800 investors surveyed in the United States, Canada, Europe and Asia, 67% reported concerns about cyber security[v].

With this in mind the impact of having a good score for cyber security will be a factor to take into consideration during the investment process. In appendix A you will find a table that shows the SDG goal and the relationship with cybersecurity.

The GOV.UK, other National CERTS and IETF (Internet Standards) publish their advice on how to prevent and protect yourself against cyber-attacks (e.g. e-mail attacks). Being compliant to these "minimal Cyber Security Standards" does help.

The next stage: cyber certificate and market entry

As well as in Europe as in the United States there are developments to create a cyber certificate. The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to establish and maintain the trust and security on cybersecurity products, services and processes. From an economic perspective, they could address imbalances in the market that lead to suboptimal outcomes and could also touch upon socio-economic aspects such as user trust, the duty of care of a manufacturer or provider and prevention of cybersecurity failure to protect market reputation.

'Organizations that are more cyber secure are the financial out-performers in the future'

In due time the cyber certificate will have a big impact on which IT product / service are led into the market and which product or service are aloud to be used and connected with other IT solutions. An example of what can happen is the case of **Huawei** that no longer can enter the US market or have a major role in enrolling 5G. But also **Tesla** that seems to have a hard time to enter the Chinese market due to the discussion that the car is used to spy. The entities that are already levelled up with security and privacy controls are better prepared for the future.

Measuring and Valuation of the Cyber Risk

Measuring the Digital Hygiene

International (cyber)governance and public disclosure

While much in-depth research and data exists on financial & some ESG related topics, an organization's approach to cybersecurity remains somewhat of a black box for investors and other stakeholders. This presents a problem in that investors are faced with assessing company performance on what is a highly financially material topic without having sufficient access to the wealth of data which would usually be accessible for other ESG issues.

Typically, organizations will go no further than providing a high-level outline and policy framework for their cybersecurity strength, with little information on what investors really need to know. The stark reality of this misalignment between materiality and disclosure was shown in a 2018 study by consultants EY. While 100% of companies included cybersecurity as a risk factor in their annual report, with 92% o prominently mentioning the topic, only 14% highlighted it as a strategic focus. The knock-on effect is that very little appropriate and comparable information was disclosed by companies as to their spending, management reporting and oversight of cybersecurity.

So, how can investors gain more insight into an individual organization's cyber resilience? And how can this be factored into the investment process both pre- and post-investment? The starting point is to build an understanding of each organization's cyber approach which is understandable, consistent and comparable.

An integrated approach: cyber risk and level of control

In order to effectively understand cyber risk and each organization's exposure to, and performance on, cybersecurity, we must understand its sense of security awareness and the interdependency between different IT systems, controls and risk frameworks used within the organization. This includes an assessment of the organization's use of appropriate controls, how assurance is delivered, the security level of service(s) provided, and the resulting level of cyber resilience. This is also stated by Bouveret[vi] about Fintech who points out that fintech is "particularly exposed to cyber-attacks given [its] reliance on technology," as well as expanding "the range and numbers of entry points into the financial system, which hackers could target." Additionally, fintech could "increase third-party reliance, where firms outsource activities to a few concentrated providers." He stresses that "cyber-risk is an emerging threat for all types of financial institutions, including central banks as well as fintech firms".

However, mitigating cyber risks effectively does not solely depend on the technical environment – it also relies on the organization's risk attitude and control environment. Then there is the inherent attractiveness of the business and/or sector to cyber criminals, with some offering more profitable pickings than others.

Calculating the 'Cyber Risk'

The Cyber Risk formula measures and quantifies the level of cyber security compliance and risk within a firm, portfolio or position over a specific timeframe, based on *public information*[1]. The formula takes an integrated approach across several cyber risk domains, producing a rating on how each organization manage this across each domain, both individually and in aggregate. It is based on several internationally accepted controls and risk frameworks to gain insight into the cyber resilience of an organization. Every domain has several key indicators that when combined together result in a final score.

CR = IR x ICR x DCR x OR

The risk formula is used to produce an overall score for each company. A baseline can then be established, allowing companies to be assessed both in an absolute sense, as well as relative to a benchmark for their sector and peers. This score can be a factor when deciding whether to invest in a company.

IR: The inherent risk (IR) is the likelihood that you will be attacked by cyber criminals assuming that there are no related controls
ICR: The internal control risk (ICR) is that risk that a vulnerability, either individually or when aggregated with other vulnerabilities, will not be prevented, detected and corrected by the entity
DCR: The detection risk is the risk that the entity will not detect a criminal activity and/or exploit on a network or system
OR: The opportunity risk (OR) is about the ability of anyone who has an internet connection to hack a system

Risk domains and key controls

The indicators when measuring the cyber risk and controls of a company are based on several international cybersecurity frameworks and research consisting of more than 150 indicators. These indicators are grouped into six key domains:

1. Business risk & cyber dependency
2. Cyber governance and culture
3. Internal controls
4. Detection controls
5. Technical compliancy
6. Trends and oppportunity attackers

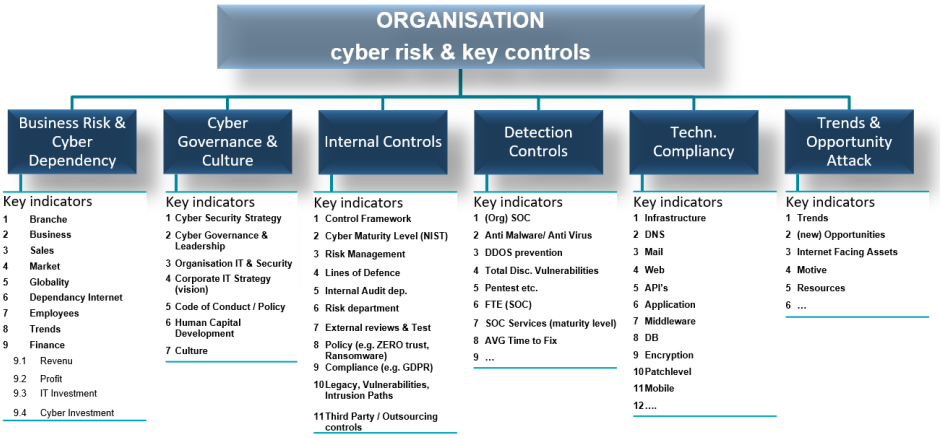


Figure 2 | Measuring the Cyber Risk

[1] E.g. OSINT, financial disclosure, website, white papers, vacancies, marketing & product info.

The category 'business risk and cyber dependency' gives insight into issues such as how reliant the company is on online manufacturing processes and sales, and the total investment made in securing these operations. The testing in categories two, three and four gives insight into the cyber risk attitude and control environment of a company. The level of compliance of the technical environment with international internet and security standards is tested in category five. The final category is based on recent attack trends and any new vulnerabilities that have emerged.

The added value of the Cyber Risk score for the investment

IT security has become an impactful risk factor in a company's suitability for investment. The approach aims to gather and structure publicly available cybersecurity information so that it can be integrated into investment decisions and engagement process.

We believe that organizations which are more cyber secure and compliant with international security standards are better placed to offer digital services or products to a wider international market, as well as being ready for future 'cybersecurity certificates' that may be issued. Complying with basic internet and security standards, and to be able to give a digital assurance will make all the difference.

"In our view Cyber Security is one of the most overlooked risk for the Fintech sector (Swiss Private Bank - Lombard Odier)"

Although there is no precise measure of Cyber Risk and each measure comes with its own limitations, the framework gives a better insight into whether an organization is underperforming or outperforming relative to its peers, and provides insight into an organization's cyber resilience and readiness for the future.

The cyber research and rating provides more insight on the IT security of a company and the potential risks associated with it. This includes an assessment of cyber risk domains at a country, industry and individual organizational level. Using publicly available data it is able to break open the black box, giving the investors greater insight into the cyber risk and resilience of each analyzed company.

The Cyber Risk score creates the opportunity to:

- **Identify and manage cyber risks in the investment portfolios**
  - Relative ranking shows which companies are mostly impacted by cyber related threats
  - Portfolio construction can take this into account as input in the weighing process, just like ESG and regular financial data
  - If we know the relative attractiveness of a company's cyber risks, it can also serve as a buying opportunity when the stock falls on headlines
- **Engage with companies to increase cyber readiness**
  - Help to improve the cyber security and resilience in portfolio holdings to ultimately decrease risks
- **Create societal awareness around the subject and work towards an audited reporting standard**
  - Reporting standards around cyber security are not yet in place, but we need to develop these standards because of our ever-increasing digital dependency.
- **Improve visibility of cyber risks for society**
  - Ultimately people need to know if the products and services they consume are protected and prevent surprises resulting from breaches corporate choice of speed-to-market over safety.

Integrating Cyber Risk in the investment process

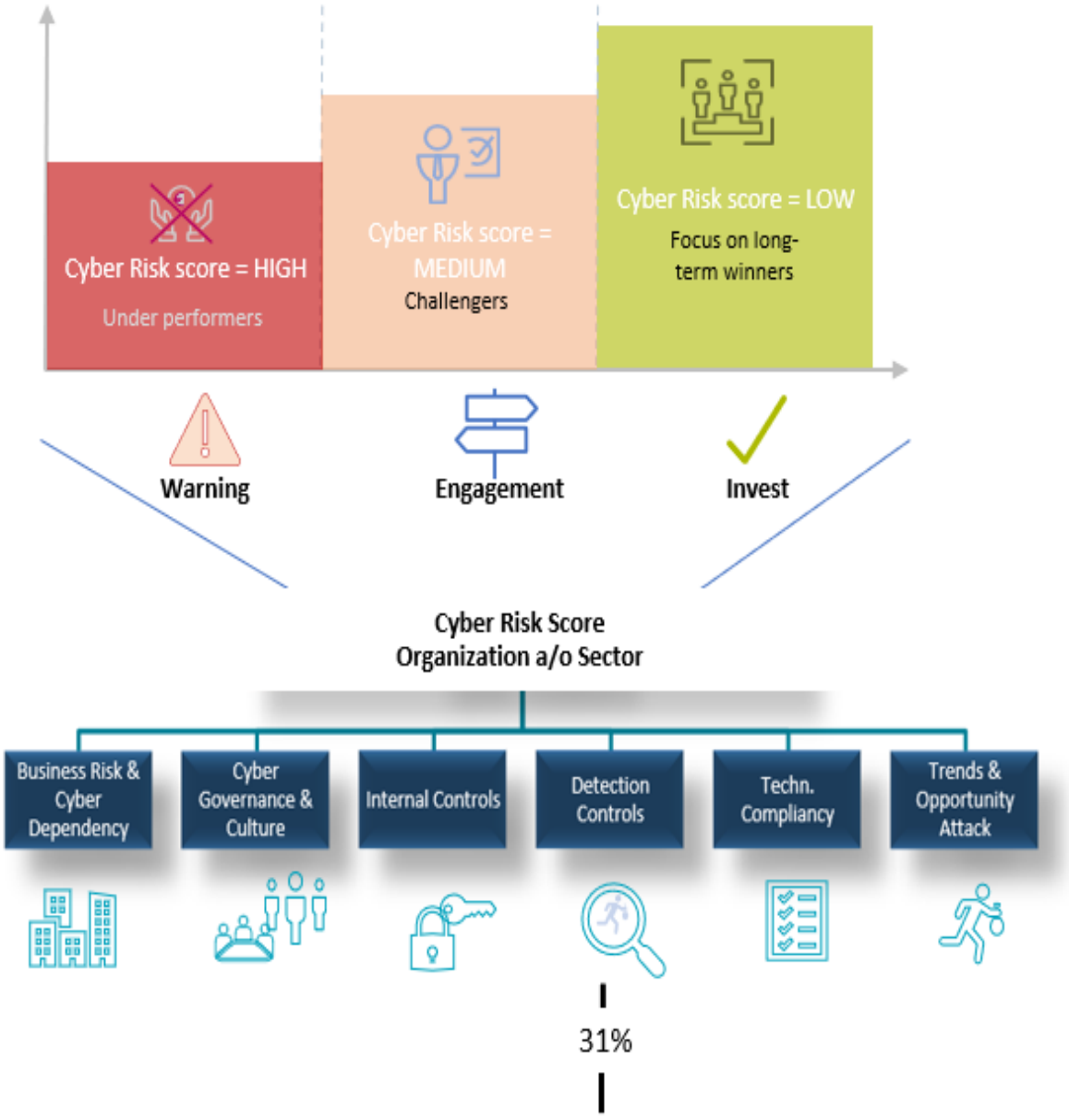


Figure 3 | Integrating the Cyber Risk Score in the investment process

.

Engaging on the Cyber Risk Score

During the last couple of years we haven't seen much impact of a data breach, GDPR penalty or for instance ransomware for the stock price. But the impact of cybersecurity on the SDG's and our environment is enormous and engaging with companies on this issue is more than important. While the digital transformation fuels innovation and creates whole new ways of doing business, there are new risks, led by increasingly sophisticated cyberattacks, and affects almost everyone.

The believe is that engagement and voting are critical elements of a successful sustainable investing strategy and can improve a portfolio's risk/return profile. By taking a proactive approach to engagement, focusing on long-term financially material sustainability themes like cyber security it will have the most potential to create value for shareholders and society.

The development of a cyber risk rating allows the Active Ownership team to take an objective and pre-defined set of metrics and indicators into engagement discussions. Conversations about cybersecurity can more effectively go beyond disclosure-related topics if companies can be compared to each other, based on this rating. The intention is not to address specific technical vulnerabilities in conversations with cybersecurity officers or other personnel. Instead, the rating and its indicators enable us to gauge whether governance systems function properly in implementing strong cyber controls and fostering a 'cyber mature' culture.

The Cyber Risk score – "A basis for successful (cyber) engagement"

Engaging with corporates on cybersecurity will help bring the issue nearer to the top of executives' and boards' priority lists. The Cyber Risk score helps to identify cybersecurity laggards in portfolios, allowing the Active Ownership team to target engagement at the companies with the most room for improvement. In this way, engagement supports the investment process by improving portfolios' risk-return profiles.

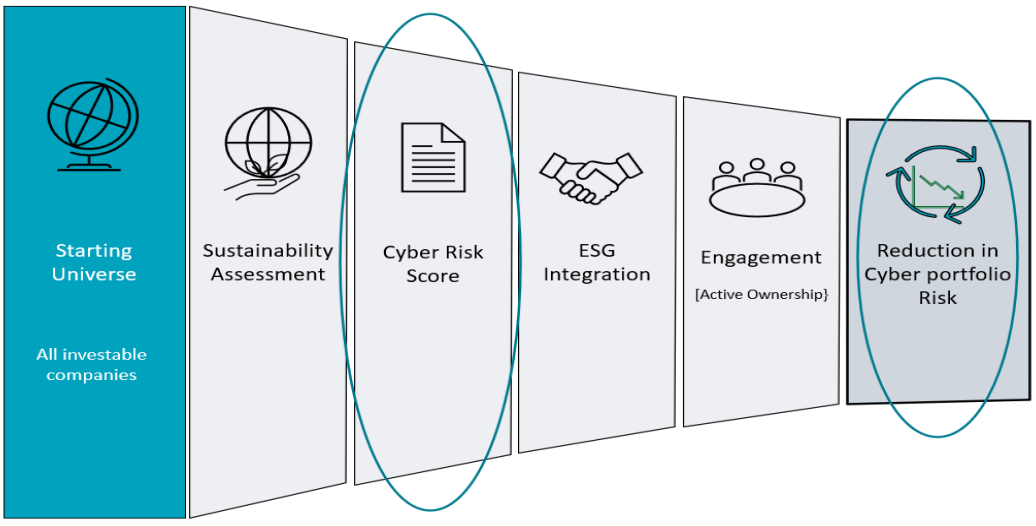


Figure 4 | Engagement on Cyber Risk

The human element

It is important to note that an increasingly digitalized and connected world is not, per se, a bad thing. Advances in technology also helps to raise global living standards, while 'smarter' cars could become one weapon in the fight against climate change. The issue is therefore not necessarily with the technologies themselves, but rather with the impact that comes with lax security standards, poor risk management or a lack of appropriate governance. For example, a survey of companies by consultant PwC found that 48% of respondents did not have an employee security awareness training program on cybersecurity, while 54% did not have an incident-response process. Given the recent trends in cybercrime and possibilities, cybersecurity must be addressed.

'Who wants to invest in organizations who are not willing to comply with the minimal Cyber Security Standards?'

Building momentum

Demonstrating to companies that investors are increasingly taking cyber risk more seriously also assists in putting cyber risk at the top of executives' agendas. Of key importance is clearly communicating to companies what investors expect from them, and when gaps are identified, how and when this will be rectified.

The cyber risk score and analyses gives investors the opportunity to enter into a debate with the board and gives organisations insight in what investors expect from them, with the ultimate goal to improve cyber security and reduce cyber risk for everybody.

Appendix A: How cybersecurity contributes to the SDG goals

SDG	Notable targets	How good cybersecurity contributes to the goal
Goal #1: End Poverty	▪ reduce by half the number of humans living in poverty by 2030 ▪ Give the poor and vulnerable equal rights to economic resources. ▪ Reduce the vulnerability of the poor and other vulnerable populations to economic, social and environmental shocks and disasters.	▪ Supports economic growth by preserving the benefits digitization and increasing trust in it. ▪ Ending poverty depends on individuals being able to access information over the Internet. Thus, it can be disrupted by weaknesses in, and attacks on, the availability of information services and the networks that individuals use in connecting to them.
Goal #2: Zero Hunger	▪ Correct and prevent distortions in the world agricultural markets ▪ Adopt measures to ensure the proper functioning of food commodity markets and their derivatives and facilitate timely access to market information.	▪ While famine has more significant underlying causes, a stable food supply relies on distribution mechanisms, which relies on dependable ICT
Goal #3: Good Health and Well Being	▪ By 2030, reduce the global maternal mortality ratio to less than 70 per 100,000 live births. By 2030, reduce by one third premature mortality from non-communicable diseases through prevention and treatment and promote mental health and well-being. ▪ Achieve universal health coverage, including financial risk protection, access to quality essential health-care services and access to safe, effective, quality and affordable essential medicines and vaccines for all.	▪ Increased digitization of the healthcare sector yields immediate dividends, but also exposes patient data to new risks and opens hospitals and other service providers up to new risk for disruption.
Goal #4: Quality Education	• Substantially increase the number of youths and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship • Build and upgrade education facilities that are child, disability, and gender sensitive and provide safe, nonviolent, inclusive and	• ICT allows for more distributed and scalable delivery of educational products. However, these products and the systems must be trusted and secure to safeguard the privacy of students ▪ Additionally, good practices when using computers and digital technologies will be increasingly important skills,

SDG	Notable targets	How good cybersecurity contributes to the goal
	effective learning environments for all	and educating populations on good cyber hygiene is an integral part of that
Goal #5: Gender Equality	• End all forms of discrimination against all women and girls everywhere • Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation • Undertake reforms to give women equal rights to economic resources, as well as access to ownership and control over land and other forms of property, financial services, inheritance and natural resources, in accordance with national laws	▪ Although literature is still nascent on the topic, some studies have suggested that cybersecurity inequalities exacerbate existing societal inequalities, including along gender lines. In addition, online resources for reporting discrimination and violence against women require strict privacy controls or they risk putting women at further risk
Goal #6: Clean Water and Sanitation	▪ Expand international cooperation and capacity-building support to developing countries in water- and sanitation-related activities and programmes, including water harvesting, desalination, water efficiency, wastewater treatment, recycling and reuse technologies ▪ Support and strengthen the participation of local communities in improving water and sanitation management	▪ Cybersecurity is important for protecting critical systems that use IT. As evidenced by various hacks on critical infrastructure, water and sanitation systems, as well as energy grids, are not out of bounds
Goal #7: Affordable and Clean Energy	▪ Expand infrastructure and upgrade technology for supplying modern and sustainable energy services for all in developing countries, in particular least developed countries, small island developing States, and landlocked developing countries, in accordance with their respective programmes of support	▪ Affordable and clean energy increasingly relies on automation and automated systems. As portrayed by power disruptions in Ukraine, these systems are vulnerable and can present new avenues for disruption is not properly secured
Goal #8: Decent Work and Economic Growth	▪ Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized	▪ Refer to Goal 1. Economic growth depends on things like your money staying in the bank when you put it there, ensuring you control your intellectual property, and that the systems you use for your business are available.

SDG	Notable targets	How good cybersecurity contributes to the goal
	enterprises, including through access to financial services ▪ Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors ▪ Strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance and financial services for all	▪ Mobile payment systems are increasingly important for distributed access to financial flows. Insecure payment systems will undermine trust and potentially stunt economic growth
Goal #9: Industry, Innovation, and Infrastructure	▪ Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all ▪ Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services, including affordable credit, and their integration into value chains and markets ▪ Upgrade infrastructure and retrofit industries to make them sustainable, with increased resource-use efficiency and greater adoption of clean and environmentally sound technologies and industrial processes, with all countries taking action in accordance with their respective capabilities ▪ Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States ▪ Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification	▪ Increased access to ICT and novel internet-connected technologies without managing the technologies' security risks making them inconvenient and may hinder uptake. ▪ Ports and modern transportation infrastructure have proven vulnerable to disruption from cyberattacks.

SDG	Notable targets	How good cybersecurity contributes to the goal
	and value addition to commodities ▪ Significantly increase access to information and communications technology and strive to provide universal and affordable access to the internet in least developed countries by 2020	
Goal #10: Reduced Inequalities	▪ Empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status ▪ Ensure equal opportunity and reduce inequalities of outcome, including by eliminating discriminatory laws, policies and practices and promoting appropriate legislation, policies and action in this regard.	▪ Protecting the integrity of people's information should be a priority no matter if it is the poor or the rich and powerful. Uneven access to cyber tools disadvantages the poor and exacerbates inequalities
Goal #11: Sustainable Cities and Communities	▪ By 2030, provide access to safe, affordable, accessible and sustainable transport systems for all, improving road safety, notably by expanding public transport, with special attention to the needs of those in vulnerable situations, women, children, persons with disabilities and older persons ▪ By 2030, significantly reduce the number of deaths and the number of people affected and substantially decrease the direct economic losses relative to global gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations ▪ By 2020, substantially increase the number of cities and human settlements adopting and implementing integrated policies and plans towards inclusion, resource efficiency, mitigation and adaptation to climate change, resilience to disasters, and develop and implement, in line with the Sendai Framework for Disaster Risk Reduction 2015-	▪ Smart cities with intelligent physical, social, institutional, and economic architecture help deliver greater sustainability to cities and communities and contribute to the targets outlined here. However, as EY notes, insecure hardware, a larger cyber attack surface, issues around internet bandwidth, and increased reliance on apps are all cybersecurity challenges faced by increasingly digitalized cities and communities.

SDG	Notable targets	How good cybersecurity contributes to the goal
	2030, holistic disaster risk management at all levels ▪ Support least developed countries, including through financial and technical assistance, in building sustainable and resilient buildings utilizing local materials	
Goal #16: Peace, Justice, and Strong Institutions	▪ Significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime ▪ Substantially reduce corruption and bribery in all their forms ▪ Develop effective, accountable and transparent institutions at all levels ▪ Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements ▪ Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime	▪ Information systems can be a boon for transparency and increase the strength of peace and justice institutions. However, just as these systems can improve the delivery of justice, malicious manipulation of information and data threatens to weaken core democratic institutions. ▪ Due to low barriers to entry and high yields, organized criminal groups are increasingly engaging in cybercrime. Equipping lower- and middle-income countries with the expertise to combat this new form of crime will help safeguard populations from this activity and give police the capacity to identify and prosecute cybercrime.

Source | https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/appendix-the-sdgs-and-cybersecurity/

Sources & other papers you may like

[i] https://www.imf.org/en/Publications/WP/Issues/2021/04/23/Central-Bank-Risk-Management-Fintech-and-Cybersecurity-50278
[ii] https://securitybrief.com.au/story/worldwide-cybersecurity-spending-to-increase-10-in-2021-canalys
[iii] https://www.information-age.com/cyber-security-spending-heading-for-200-billion-year-bloomberg-123494864/
[iv] https://www.bloomberg.com/professional/blog/esg-assets-may-hit-53-trillion-by-2025-a-third-of-global-aum/
[v] https://global.rbcgam.com/sitefiles/live/documents/cgri/cyber-security-is-the-top-esg-concern-for-institutional-investors.PDF & http://go.pardot.com/l/441592/2019-10-14/qbhs24
[vi] Bouveret, 2018, Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper, 18/143. Washington, D.C.: International Monetary Fund.

OTHER PAPERS THAT YOU MAY FIND INTERESTING

- Cyber Hygiene in the Netherlands (NCSC NL)
  https://english.ncsc.nl/research/research-results/cyber-hygiene-in-the-netherlands

- Incentiving responsible and secure innovation: Principles and guidance for investors
  https://www.weforum.org/reports/incentivizing-responsible-and-secure-innovation-principles-and-guidance-for-investors