CYBERSECURITY AND SUSTAINABILITY

Estimated read time: 3 min

ON THE GREEN AGENDA

KEY TAKEAWAYS

Cyber-risk is one of the top threats facing organisations and their stakeholders today.

Companies managing energy systems, such as gas utilities and power producers, have a greater responsibility to plan for and mitigate cybersecurity risks.

Companies should prepare for the day when cybersecurity risk and resilience form part of ESG regulatory requirements.

In 2020, the COVID-19 pandemic coincided with an increase in cyber-incidents, including ransomware.[1]

In December of the same year, the Solarwinds Supply Chain attack was discovered. The attack had started since March 2020, when Solarwinds (the company) was infiltrated by hackers who injected trojan malware into the Solarwinds software update, that subsequently went out to at least 200 major customers worldwide.[2] Some of Solarwinds' customers include the US military, the National Security Agency and Fortune 500 companies.

In 2021, the Colonial Pipeline cyber-attack in the US demonstrated the vulnerability of critical infrastructure and the negative impact on physical environment and social stability. In 2022, the Russian invasion of Ukraine saw an increase in cyber-warfare against Ukraine.[3]

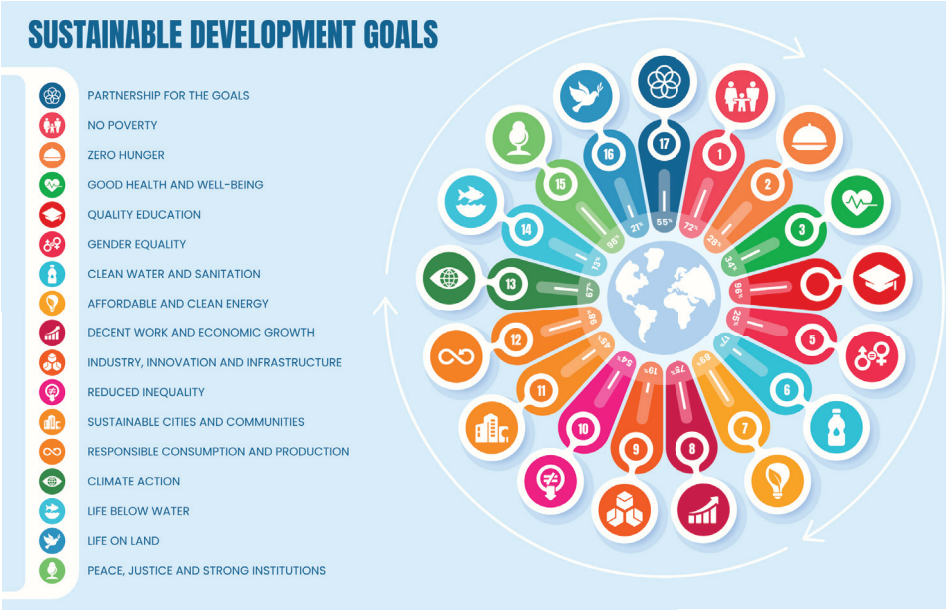
Every one of those major cyber-incidents impacted the social stability of people, businesses and countries. Were any of those impacted entities practising good governance to ensure resilience in the event of cyber-attacks? Would investments depreciate in light of entities being victims of cyber-attacks? The short answer is that it depends on whether those businesses reported their cybersecurity efforts. This is one reason why businesses should include cybersecurity risk measures in their sustainability reporting.

[1]"Cyber Threats Have Increases 81% Since Global Pandemic," [Online]. Available: https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic.
[2]"The SolarWinds hack timeline: Who knew what, and when?," CSO Online, [Online]. Available: https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.
[3]"Ukrane says it is fighting first 'hybrid war'," BBC, [Online]. Available: https://www.bbc.com/news/technology-60622977.

Sustainability and ESG are two terms that are often used in the context of business. Sustainability is a broad concept that refers to meeting the needs of the present without compromising the future. Sustainability encompasses environmental, social, and economic aspects of human activities.

On the other hand, ESG is a specific framework that evaluates the environmental, social, and governance aspects of a business or an investment.

ESG and sustainability are not just concerned with health, safety and the environment. Cybersecurity is a major consideration, as cyber-risk is one of the top threats facing organisations and their stakeholders today. In its 2022 *Global Cybersecurity Outlook* report, the World Economic Forum refers to the prevalence of cybersecurity risks as "the new normal".[4] Therefore, it stands to reason that it should become a mainstream part of ESG reporting.



Linking cybersecurity and sustainability: a natural gas case study

Often-repeated examples of past cyber-intrusions are worth re-examination, as these cases demonstrate how damaging attacks on large and strategically significant systems, such as utilities, banks, and hospitals can be mapped onto the environment, society, and business aspect of sustainability, and why they should be reported.

The attack on the US Colonial Pipeline in 2021 demonstrated how a cyber-attack can interrupt the flow of gas in a critical network. This attack confirmed that Industrial Control Systems (ICS) managed via Supervisory Control and Data Acquisition (SCADA) systems are very much at risk, with far-reaching implications. Consider the impact to society when industrial plants or businesses that rely on gas for production must stop operations, or lay people off. Consider the loss of revenue to governments and the cascading effect that has on communities. Consider the impact to the country if stoppage of gas-generated electricity is extended for long periods. Consider the severe reputational damage on gas companies and their executives.

Governance also comes into play when investors, customers, and even the upstream gas players, want to know that the gas aggregators are diligent in addressing their cybersecurity resilience. Reporting on cyber-risk metrics can offer a window into overall corporate behaviour as it relates to securing the key assets of the company.

Proving cyber-resilience in the ICS operations through transparent reporting has the potential to attract more investors and even increase international ratings.[5]

Companies managing energy systems, such as gas utilities and power producers, have a greater responsibility to prepare for and mitigate cybersecurity risks. A greater emphasis on holistic ESG reporting inclusive of cyber-risk is therefore essential. In fact, according to auditing firm KPMG, companies should prepare for the day when cybersecurity risk and resilience form part of ESG regulatory requirements.[6] ■

[4]"Global Cybersecurity Outlook 2022," World Economic Forum, [Online]. Available: https://www.weforum.org/reports/global-cybersecurity-outlook-2022/.
[5]"What Is Environmental, Social, and Governance (ESG) Investing?," Investopedia, 2023. [Online]. Available: https://www.investopedia.com/terms/e/environmental-social-and-governance-esg-criteria.asp.
[6]KPMG.com, "Cyber Security: Don't report on ESG without it.," KPMG, 2021.