CYEN

The Uplift.

White Paper

Leveraging ESG & Cybersecurity for Resilient Organizations

Contributors

Iva TASHEVA

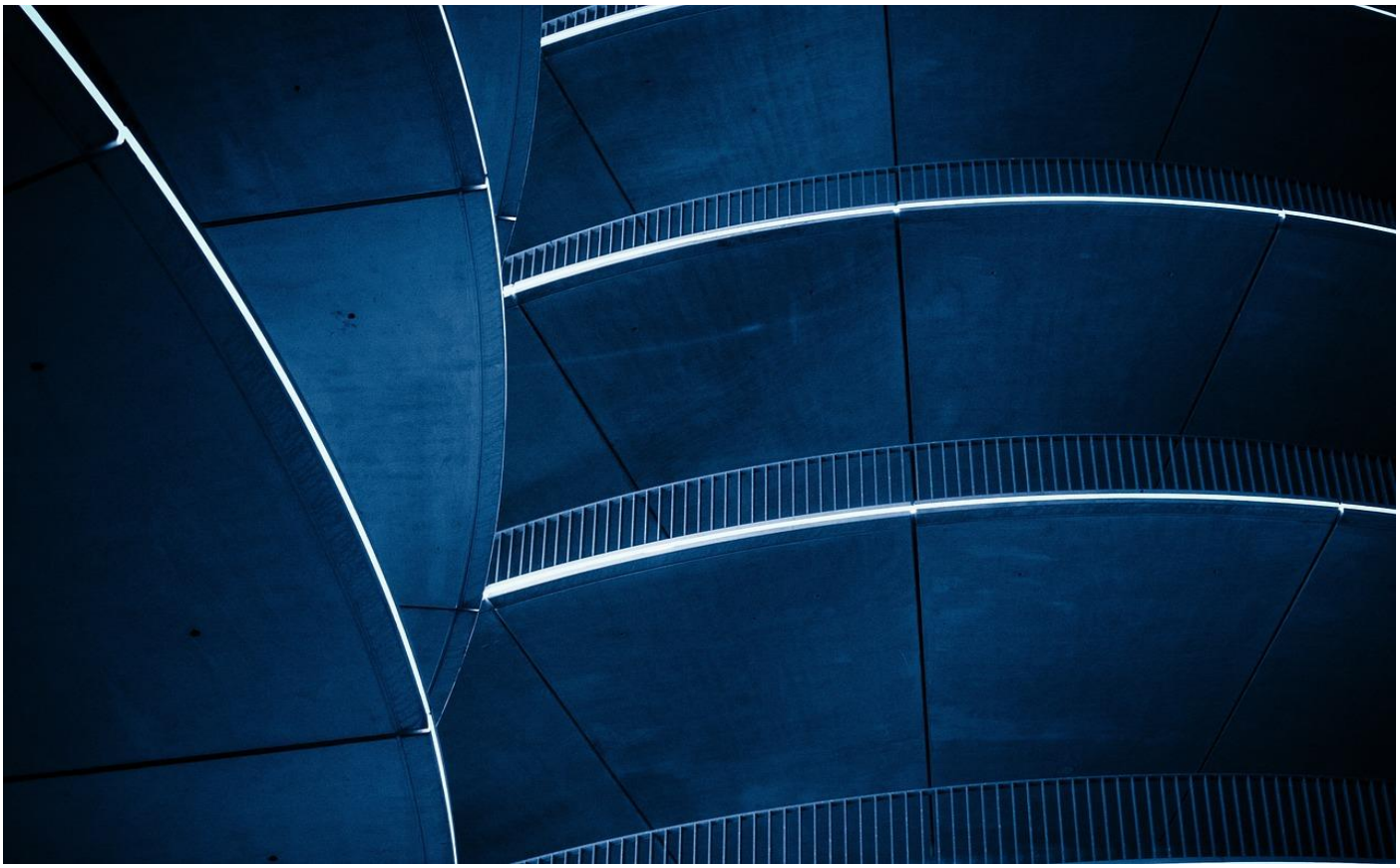
Clémence BETESUKU

TABLE OF CONTENTS

Executive summary

This paper, written by two experts in cybersecurity and sustainability, **explores the integration of cybersecurity and Environmental, Social and Governance ("ESG") practices,** highlighting how European regulatory frameworks are setting unified standards across both domains. It emphasizes that **similar assessment methods**, using the "People-Process-Technology" framework, are being **used to evaluate and advance organizational maturity in cybersecurity and sustainability**.

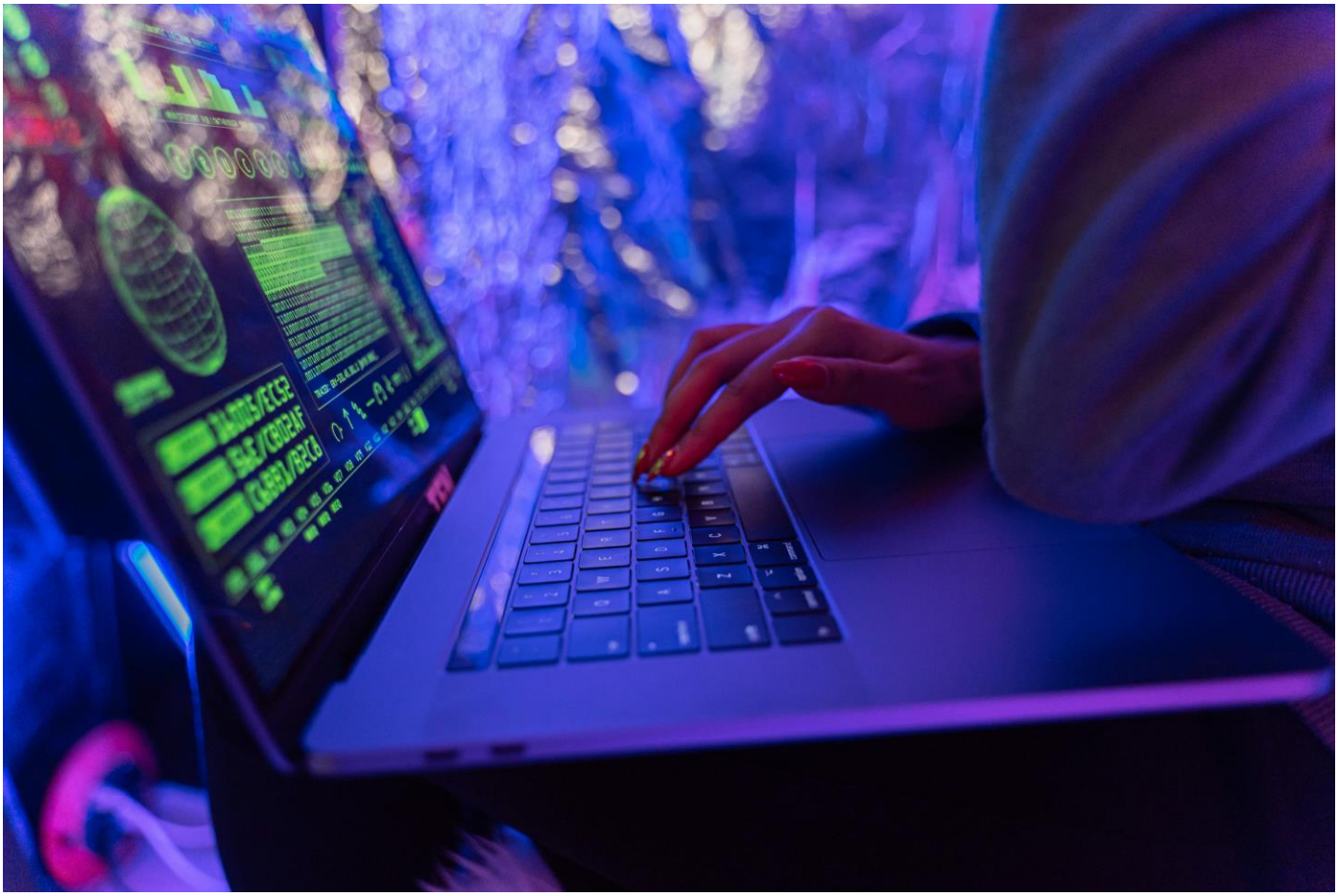
The article illustrates the evolution of processes and regulatory impacts, offering a **clear roadmap for organizations to adapt to the rapidly changing landscape**. It also focuses on the **challenges and opportunities faced by Small and Medium Enterprises ("SMEs")** in implementing these integrated practices and points out the maturity gap between large corporations and SMEs, which often results in a lack of awareness and preparedness among smaller firms. Through a **compelling case study**, the authors demonstrate how **proactive strategies** can help companies — non-EU aiming to capture EU market shares — to not **only comply with regulatory demands but also gain a competitive advantage**.



Introduction

The Colonial Pipeline Cyber Incident (2021) – a *ransomware attack which caused an American oil pipeline to take the proactive measure to shut down its network as a precaution* – is a perfect example of how cybersecurity and Environmental, Social and Governance ("ESG") intersect. This **caused economic damage and could have resulted in an environmental disaster**.

Whilst it is easy to see how climate fits into ESG, it is less obvious in the case of cybersecurity. This paper, inspired by a collaboration between two leading experts in the fields of cybersecurity and ESG, will highlight how these different areas – which are often siloed – converge and diverge, and how, **when de-siloed**, they can **leverage companies' resources and contribute to business success**. Case studies are developed to give practical and tangible examples of the areas covered. Our primary focus is SMEs operating with or within Europe, with a certain level of digitalization achieved. While SMEs account for about 90% of all companies worldwide, they are **often overlooked**. A **more inclusive & sustainable society cannot happen without their involvemen**t. Nonetheless, this paper's principles and conclusions could be applied to large corporations, adapting the context.



1. Definitions

1.1. What is ESG?

ESG is a non-financial set of criteria used to evaluate a company's sustainability and ethical impact. It is composed of 3 pillars:

- **Environmental**: how well is a company managing its environmental resources;
- **Social**: addressing social issues and;
- **Governance**: maintaining strong governance practices (risk management, internal policies…).

It has been proven that implementing ESG strategies will improve a company's performance[1].

1.2. What is cybersecurity?

Cybersecurity is "*the art of protecting networks, services, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*[2]".

Information security – a related concept –, is defined as "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability*[3]".

In practice, the terms cybersecurity & information security are often interchangeable. In the context of EU policies, they cover the full scope of securing all information & Information & Communication Technology System ("ICT").

1.3. Cybersecurity falls under all pillars of ESG

Reviewing these definitions, one thing is certain: cybersecurity contributes to all the pillars of ESG. We could even go so far as to say that **an ESG framework is not strong without the inclusion of cybersecurity**. In the opening example of the Colonial Pipeline, the incident resulted in a **social consequence** (uncertainty and inability to transport people), and a **governance consequence** (cybersecurity policies – such as disaster recovery plan –, were not aligned with the business needs). It could have resulted in an **environmental disaster**, had the technology used to move the oil been impacted.

[1] 2025 Executive Benchmark Survey – Workiva, https://www.workiva.com/resources/2025-executive-benchmark-integrated-reporting

[2] Cybersecurity & Infrastructure Security Agency, "What is Cybersecurity?" https://www.cisa.gov/news-events/news/what-cybersecurity

[3] NIST Computer Security Resource Center, Glossary https://csrc.nist.gov/glossary/term/INFOSEC

Cyberattack on a French hospital – a 7-million-euro loss with damaging consequences[4]

In November 2022, there was a cyberattack on André-Mignot, a French hospital. The consequences were devastating. Several of them can be mapped to ESG:

- **Social aspect**: personal data exposure + surgeries postponed;
- **Governance aspect**: to limit the damage, the hospital had to shut down its computer systems. With no monitoring, the staff had to revert to using pens & notebooks.

The financial loss is around 7 million euros. Overall, it took **18 months for the hospital to build a new IT system**.

What are the **best practices in minimizing the risk of cyberattacks**? We asked an asset manager. Indeed, **asset managers rank cybersecurity as their 2nd biggest concern among ESG-related themes[5].**

"We limit such risks by outsourcing key operations and related infrastructures to third parties that have robust cybersecurity measures in place. Since our inception in 2010, we have been a staunch supporter of telecommuting (now conventionally known as "remote work") to minimize ***negative environmental impacts*** *and, as such,* ***sound cybersecurity measures*** *have always been a component in the company's risk management plan".*

Peterson Frederick*, Chairman & Interim Chief Executive Officer of Northern Providence Investments.*

[4] [4]Capital "L'hôpital André Mignot de Versailles bloqué depuis trois mois par une cyberattaque massive" https://www.capital.fr/economie-politique/lhopital-andre-mignot-de-versailles-bloque-depuis-trois-mois-par-une-cyberattaque-massive-1464519

[5] RBC Global Asset Management, "2022 Key Findings" RBC Global Asset ManagementResponsible Investment Survey, 2022

2. Leveraging cybersecurity & ESG

2.1. The EU regulator is paving the way on both issues

Both cybersecurity & ESG risks are governed by EU regulations. In both cases, the EU regulator expects companies to use a **risk-based approach** i.e., to focus on high-risk parts of the value chain where damage is more likely.

2.1.1. Focus on cybersecurity legislations

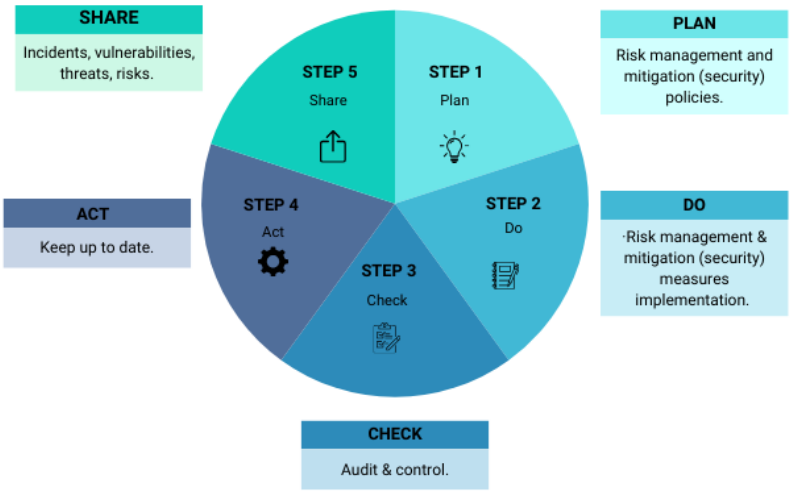
There are two types of EU cybersecurity regulations: the **product-based ones** (focusing on the sector of the operations and applied at an organization-level) and the **processed-based ones** (focusing on the product based on the EU market by the organization).

What happens when companies fall **within one or both categories of regulations**?

- **Processed-based regulations**: the goal is no overlap between processed-based regulations. The stronger one should apply. For instance, the Digital Operational Resilience Act ("DORA") is applicable to the financial sector, as it is more stringent than Measures for a high common level of cybersecurity across the EU ("NIS 2");
- **Product-based regulations**: the picture is **more complex**. Depending on the type of products produced, there may be multiple product-based regulations to consider.

Plan-Do-Check-Act-Share (PDCA)

These regulations circle around the PDCA (Plan-Do-Check-Act-Share), an iterative method whose purpose is to **continuously improve processes and products**.



2.1.2. Focus on ESG legislations

The EU has developed The European Green Deal, a **growth model based on a clean & circular economy**. As part of the European Green Deal, legislations pertaining to ESG have been adopted. They are designed to **help companies in reporting their performance** related to sustainability, social responsibility & ethical governance. All these regulations are interconnected.

The interconnexion between EU ESG legislations[6]

The Omnibus Regulation: a setback for European corporate sustainability?

In November 2024, the European Commission announced a simultaneous revision of the EU taxonomy, CSRD and CSDDD. This revision is part of a legislative package known as "Omnibus". Its goal is to **simplify the EU's business environment to push innovation and to make the EU more competitive**. Concerns were raised by large corporations who pushed back against the Omnibus[7]: oversimplification could undermine what has been done regarding ESG.

In February 2025, the "Sustainability Omnibus" was published. The **key takeaways** are:

- **80% of companies to be removed from CSRD & EU Taxonomy scope:** under this proposal, reporting is mandatory only for companies with over 1000 employees;
- **2-year delay** for companies under the 2nd & 3rd waves of reporting of CSRD ("stop the clock")[8];
- **Reduction of European Sustainability Reporting Standards ("ESRS") data points.**
- **CSDDD weakened:** for instance, monitoring frequency reduced from every year to once every 5 years**.**

Is this the **end of corporate sustainability?** No.

- First, this is **a proposal** i.e., it is hard to predict the outcome.
- **ESG reporting is here to stay** despite the current climate of uncertainty. Stakeholders (investors, clients…) will continue requesting sustainability data. More than ever, dialogue is important.
- Finally, **let's not forget** that embracing ESG practices is more than performing a compliance exercise. It is a **tool for risk management**, a **driver for profitability and consequently, a competitive advantage**. And most importantly, it is **an essential component of making society more inclusive and sustainable**.

[6] For more details on EU ESG regulations, please refer to Annex 2 – Major EU ESG Regulations.
[7] Open letter by major businesses, Jan 2025: https://media.business-humanrights.org/media/documents/Omnibus_Business_Statement_17_January_2025.pdf
[8] CSRD has 4 waves of reporting with the first wave starting in 2025.

2.1.3. Cybersecurity imperatives fit into ESG considerations

With the CSRD adoption, **cybersecurity is now part of sustainability disclosure**. The message is clear:

- There's a **shift in the way cybersecurity is perceived**: from an **industry issue to a global social issue**.
- Analyzing the cybersecurity risk through the ESG lens helps in having a **better understanding of a company's internal operational system** & it helps investors in their **decision-making process**.

Note: when working on sustainability disclosures, companies never really start from scratch. They can **use the existing risk management processes**.

Before the adoption of the CSRD	After the adoption of the CSRD – a significant change in companies' cybersecurity practices
No cybersecurity disclosure requirements in the area of sustainability.	Cybersecurity is now an **essential part of sustainability disclosure.**
Companies were free to decide if and to "*what extent they would disclose cybersecurity information in their annual report*"	**ESRS S4 consumers and end-users:** with this disclosure, stakeholders are now able to have an understanding on how a company *"identifies, assesses, mitigates, and remediates this material impact".*
	From a **cyber-risk perspective**, it means that some of the measures adopted in compliance with Article 32 GDPR & Article 21 NIS 2 can be **disclosed in the annual report to meet the disclosure requirements of ESRS S4**.

2.1.4. ESG considerations should fit into cybersecurity imperatives

While the **governance aspect of ESG is at the core of cybersecurity imperatives** (continuous assessment, reporting…), the **same cannot be said about the social and environmental aspects**.

Society protection is a trigger for many EU regulations (NIS2, DORA to name a few…). However**, concrete assessment of the societal impact of security measures is lacking**. Are **security monitoring cases designed fairly, with no discrimination or biased results**? Is cybersecurity a universal right?
In the cybersecurity landscape, while **environmental threats are considered, the environmental objectives aren't** (example: the intensive energy use by AI models is largely debated but not estimated yet). More research is needed to provide data form an informed decision aligning both cybersecurity imperatives and ESG considerations.

What should companies do then? When choosing cybersecurity measures, consider their environmental & social impact and select those that are the most "**appropriate & adequate**".

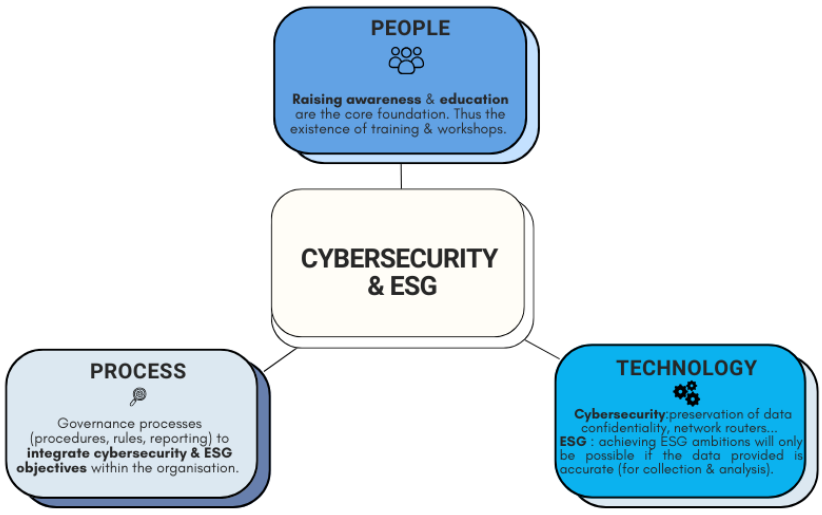
2.2. Voluntary frameworks to reinforce the commitment to ESG & cybersecurity

Companies can adopt voluntary standards/frameworks – **aligned with the company strategy** – to **reinforce their commitment to cybersecurity & ESG** and to **stand out from the competition**. As with regulations, we can find cybersecurity aspects in sustainability standards.

Note: a company is never starting from scratch. Mapping **regulations to standards or cybersecurity obligations to sustainability requirements** can simplify the process.

Sustainability standards containing cybersecurity aspects	Other notable sustainability standards	Information security standards
Sustainability Accounting Standards Board Requires companies in the software industry to report cybersecurity attacks.	Voluntary Sustainability Reporting Standards for non-listed SMEs (VSME) For SMEs outside the CSRD scope but who face growing sustainability requests from business counterparties[9].	Many of them contain **environmental threats** but no sustainability objectives: ISO27001 – Information Security Management Includes controls for protection vs. environmental threats (fire, floods)
Global Reporting Standards Contains guidance on the disclosure of cybersecurity & data privacy issues.	B-Corp Certification Measurement of the entire company's social & environmental status.	

2.3. The "people-process-technology" framework



[9] i.e., banks, investors, or larger companies for which non-listed SMEs are suppliers.

2.4. Tracing the Maturity Phases of ESG and Cybersecurity

Understanding the current state and direction of both industries is crucial for businesses to be able to **address growing stakeholder concerns**. It is widely agreed that ESG, despite its different history, appears to be following a similar "maturity curve" to cybersecurity.

Three phases can be identified: **awareness**, **regulation-led** & the **automation** phase.

PHASE 1 – AWARENESS (PRE-2000s)

Cybersecurity: pre-NIS 1 directive, the industry and policy makers were mostly discussing **privacy & data security issues**.

Sustainability: mostly seen as a communication tool. The context was prone to greenwashing. Actions were mostly **voluntary & standalone**.

PHASE 2 – REGULATIONS ARE PAVING THE WAY (2010 – 2030)

Cybersecurity is **no longer just an "IT issue"**: it's a global issue with **business survival** at stake.

92% of SMEs recognize cybersecurity as a **key element** of their company[10].

57% of SMEs admit that they would likely **go out of business** six months after a cyber incident[11].

Only 16% of SMEs feel **well prepared** for an attack[12]

Legislations hold Board and C-level executives accountable. New legislations are being adopted existing ones updated. **Significant cybersecurity incidents reporting** is a regulatory requirement.

ESG-wise, the **Green Deal** came into force with competent authorities **building a standardized sustainability framework**. Disclosures are now a **regulatory requirement**.

20% less **Climate related greenwashing incidents** in the EU banking sector in 2024[13].

- Since the adoption of these regulations, the EU-decision making bodies composition has changed and there's been a shift regarding legislation: it went **from creating new regulations to prioritizing simplification**.
- One might wonder about the **disclosure of confidential information**: the legislation allows companies to omit sensitive information from reports, as long as the omission is disclosed.

PHASE 3 – AUTOMATION & MATURITY (2030s onwards – likely scenario)

The prominent use of AI: Machine learning and **AI will take over the technical domains of cybersecurity** (i.e., monitoring, detection,).

ESG data providers will reach maturity and data collection will be standardized. The debate will be around the **development of a sustainable AI**.

Experts with a system-oriented perspective? As automation tools become more efficient, the need for specialized experts will decrease. However, experts with a system-oriented perspective (e.g., IT, people, sustainability…) will be needed for **strategic decisions** (e.g. system improvement & guiding AI development).

[10] Google (2023) Europe's SMEs in the Digital Decade 2030: Building Cyber-resilience, Overcoming Uncertainty, available at https://storage.googleapis.com/grow-with-goog-publish-prod-media/documents/Europes_SMEs_in_the_Digital_Decade_2030_report.pdf(2023)
[11] ENISA (2021) Cybersecurity for SMEs - Challenges and Recommendations, available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf
[12] Ibid
[13] RepRisk, Special report (2024) "A turning tide in greenwashing? Exploring the first decline in six years" https://www.reprisk.com/research-insights/reports/a-turning-tide-in-greenwashing-exploring-the-first-decline-in-six-years?mtm_campaign=pressreleaseq424-greenwashing2024&mtm_kwd=reportsq424&mtm_source=pressrelease-traffic

3. Integrating cybersecurity & ESG practices across the entire supply chain: a challenge & opportunity for SMEs

Because they do not possess the same resources & capacity as big corporations, integrating cybersecurity & ESG practices into the entire supply chain can be a challenge for SMEs: there seems to be a **maturity gap between large corporations and SMEs**.

3.1. A maturity gap between large corporations and SMEs

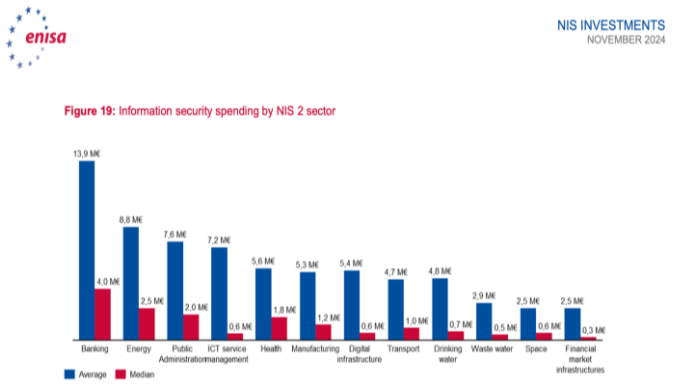
3.1.1. Proactive approach from large corporations

Large corporations are **proactive in addressing ESG and cybersecurity as part of their business strategy**, driven by increased accountability from legislation.

For instance, Orsted – a Danish multinational power company – voluntarily published its CSRD-compliant report from the 2023 reporting year (i.e. **before the regulatory deadline**). The same holds true for cybersecurity: due to economies of scale, corporations have control over/possess their own AI & data-driven tools.

Moreover, **large firms are not slowing down on their investments in cybersecurity & ESG**:

- Despite the "shifting political winds", they are not stopping their investments in the green transition. In January 2025, Nicolai TAIGEN, the CEO of Norges Bank Investment Management – the world's largest sovereign fund – reiterated the Bank's commitment to ESG. In 2024, the fund divested from 49 companies based on sustainability assessments.
- **Financial firms are leading the way** when it comes to cybersecurity: in 2021, Bank of America CEO announced spending more than USD 1 Billion in cybersecurity yearly. A report[14] revealed that, in 2023, in Europe, **banks are leading the way in terms information security investment**, **with EUR 13.9 million average yearly spendings**, compared to 8.8 million for the next highest critical sector (energy).



3.1.2. Reactive approach from SMEs

In contrast, SMEs are **reactive in addressing ESG and cybersecurity** i.e., they tend to view them as compliance issues. They act on them mainly due to **supply chain requirements**.

[14] Enisa European Union Agency for Cybersecurity "NIS Investments 2024" (2024)
https://www.enisa.europa.eu/publications/nis-investments-2024

3.2. Resulting in a lack of awareness for SMEs

SMEs need to be more aware of the extent of their supply chain regarding both ESG & cybersecurity risks.

- 71%[15] of "the smallest organizations by annual revenue **have not been asked to prove their cyber security posture by their supply chain partners**".
- 71%[16] of the largest organizations by annual revenue **have been asked this question**. This makes SMEs more prone to cyberattacks.

Many SMEs tend to minimize their ESG actions. Some are **not even aware that some of their existing actions are ESG practices** (like mentoring young entrepreneurs). They do not communicate on it and **miss the reputational benefits from informing the public.**

To build a secure cyber environment, collaboration and communication between the various stakeholders is crucial.

71% of the smallest organizations by annual revenue

have not been asked to prove their cybersecurity posture by their supply chain partners.

71% of the largest organizations by annual revenue

have been asked to prove their cybersecurity posture by their supply chain partners.

3.3. SMEs are indirectly hit by regulatory requirements

Even though most of them are out of scope, the evolving regulatory landscape is still affecting SMEs through their relationship with large corporations (supply chain) even though they are outside of the regulatory scope.

NIS2: the businesses under its scope must consider the vulnerabilities specific to each direct supplier and service provider as well as the quality of their product. Should **the suppliers & services providers be considered "high risk", the business will change suppliers & service providers**.

CSRD: it requires companies to collect ESG data from their suppliers for reporting. In other words, **SMEs outside the scope of EU regulations may still need to implement the minimum requirements and provide relevant data to their clients in the EU**.

Failing to comply **may limit SMEs' customer recruitment and retention**, as clients may prioritize NIS2/DORA/CSRD-compliant or low-risk suppliers.

3.4. An opportunity for SMEs to implement robust practices?

Incorporating cybersecurity & ESG practices into the supply chain is not just about compliance – it is **an opportunity for companies to enhance competitiveness**. Collaboration between corporations is essential for a **smooth supply chain**. It will enable SMEs to:

- Deepen their relationships with large corporation: it has been shown that the productivity of SMEs and large firms **SMEs productivity and large is interconnected**[17];
- Develop **robust cybersecurity & ESG practices** that will make them more competitive.

[15] World Economic Forum, "Global Cybersecurity Outlook 2024" (2024) https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
[16] Please refer to footnote 16.

[17] McKinsey Global Institute, "A microscope on small businesses: Spotting opportunities to boost productivity" (2024) https://www.mckinsey.com/mgi/our-research/a-microscope-on-small-businesses-spotting-opportunities-to-boost-productivity

4. Case study

Non-EU companies looking to expand into the EU market should develop cybersecurity and ESG practices if they want to work with larger companies (and increase their market shares).

SCENARIO (proactive approach):

Company A – *an ICT company based in the UK (30 employees)* – is considering developing cybersecurity & ESG strategies to collaborate **with larger companies** (>1000 employees) in the EU & **increase its turnover**. It lacks a dedicated cybersecurity nor ESG team.

There's a double challenge: **strengthening its cybersecurity system while developing sustainable practices**. However, it is unsure on where to start given the latest regulatory updates & debates on both topics. Guidance is needed.

Step 1 – ESG strategy development

Before exploring the requirements (both mandatory and voluntary), let's **identify the Sustainable Development Goals**[18] ("SDGs") that an ICT company can attain. **Data analytics** will also play a key role in **framing the ESG strategy & defining the ESG objectives**.

a. Preliminary work: framing the strategy

A deep dive into company's A universe led by a sustainability specialist[19] will be conducted to create a **tailored sustainability plan** (several departments involved**)**.
Here are a few examples of **SDGs that company A could work on** as an ICT company.

SGD 12: Responsible consumption and production
The solutions developed should aim to reduce costs & consumption i.e., environmental footprint.

SGD 8: Decent work & economic growth
Company A should aim to create smart manufacturing and IT solutions.

SGD 5: Gender equality
The IT sector suffers from a shortage in women which prevents it from being competitive[20]. Actions should be put in place to reduce this gap.

b. Identification of the applicable requirements

Regulation

Company A is a non-EU company + non-listed SME = **outside of the CSRD scope = CSRD non-applicable.**

Supply chain requirements: an EU large company will *request ESG data from company A* to include them in their report. Should company A be unable to provide such data, **gaining contracts with large EU companies will be difficult = necessary to adopt voluntary frameworks/standards**.

Voluntary framework

Company A wants to increase its presence in the EU. **VSME framework = best option[21].**

VSME basic module or **VSME comprehensive module** [22]?

- **Basic module** since *small size & non-existence of sustainability practices*.

Conduct a gap analysis for the VSME basic module → roadmap with **key performance indicators to reach**.

[18] There are 17 SGD. Created by the United Nations in 2015, they aim to bring peace and prosperity for people and the planet, while tackling climate change and working to preserve the environment and oceans.
[19] According to a report by the UK firm Burges Salmon, out of the 361 U.K companies polled, 32% were "completely unprepared" to meet their supply chain disclosures obligations, and only 29% believe their companies fully understand the legislative and regulatory landscape governing ESG corporate disclosure.
[20] McKinsey Digital "Women in tech: The best bet to solve Europe's talent shortage" (2023) https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/women-in-tech-the-best-bet-to-solve-europes-talent-shortage
[21] For SMEs outside the CSRD scope.
[22] The VSME framework is divided into two modules to cater to the diverse needs of SMEs: the basic module (an entry-level framework) and the comprehensive module (for larger SMEs or SMEs with advanced sustainability practices).

Step 2 – Cybersecurity requirements assessment

a. Assessment

When choosing cybersecurity measures, companies must consider their environmental & social impact and select those that are the most "appropriate & adequate" and **aligned with the ESG strategy**.

Regulation

Company A needs to **list its client sectors & locations** to identify which regulations would be relevant or expected by its customers, partners, or regulators.

- **Sectoral regulation verification:** cf. *Annex 1 – EU-wide cybersecurity legislations* to identify the regulations applicable to its business or clients.
- Is company A **placing any products in the EU market** (i.e., making available for purchase a standalone product or service)**?**
  → If yes, necessary to **look into product regulations to identify which regulations apply** (annex 1).

Conformity procedures

Are there any **standards or certifications** required or accepted as a presumption of conformity?

- **Ex-post checks** like GDPR will allow doing business but assume an audit after an incident.
- **Ex-ante conformity assessment** like CRA or MDR would require planning of compliance efforts before placing the product on the market.

b. Implementation (up to a few months)

Collaborative effort

Management, IT/security department, HR, team leads, suppliers, possibly **external specialized cybersecurity compliance** consultants.

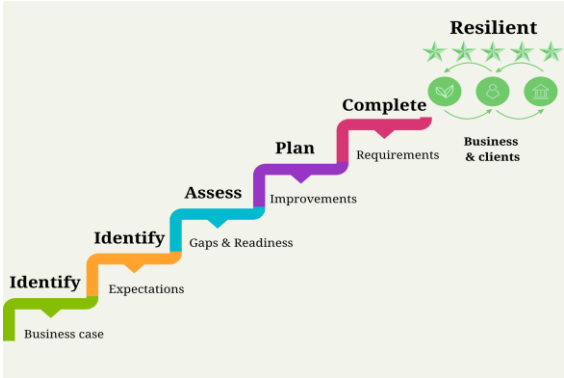
Gap assessment + roadmap

Some **sector-specific requirements** (e.g., DORA in the financial sector) will be difficult (time + cost) to implement in the short term. Company A may decide to put aside the financial sector as a target and prioritize other sectors for its general services.

Cybersecurity map

The applicable requirements for the selected sectors will feed into the **cybersecurity plan** (priorities, timeline, budget…).

Step 3 – Leveraging ESG & Cybersecurity efforts



Once the gap analyses have been performed and that actions have been put in place, company A can start **working on the VSME-compliant report**.

Overview of the VSME-compliance report content

General information

Company profile + "*practices, policies and future initiatives for transitioning towards a more sustainable economy*":

Compliance with both cybersecurity & ESG requirements (policies implemented, risk management processes…);

Targets to monitor the implementation of these policies **+ progress achieved** towards meeting these targets;

Efforts to **reduce the environmental footprint, Gender equality** improvement in the workplace **H**ow technology **innovation helped creating a smart solution.**

Metrics disclosure

Environmental metrics:

Total energy consumption (and include how much of it is renewable).

Emissions owned or controlled by a company[23].

Emissions that a **company causes indirectly** like the emissions caused when generating the electricity in the company building[24].

Social metrics:

Training programs: for instance, is there a training related to cybersecurity? How many people did attend this training?[25]

Workforce composition: reduction of the shortage of women in the workplace?

- **Sign of reliability** to large companies under the CSRD scope that seek aligned suppliers.
- Demonstrates a **commitment to social responsibility & talent upskilling.**
- **Raises investors' interest** should company A be looking for investors (due diligence).
- And don't forget **to communicate about your efforts!**

[23] Also known as Scope 2 emissions.
[24] Also known as Scope 3 emissions.
[25] Can be obtained from the info collected from the cybersecurity requirements.

Conclusion & Calls to Action

General statement

Cybersecurity & ESG intersect. More than that, **cybersecurity falls within the three pillars of ESG** - good governance, social and environmental impact.

- Both **give organizations a competitive edge**: by integrating them in their business strategy, companies will find themselves in a better position to protect themselves from cyber & ESG risks. This will **unlock growth opportunities**;
- **Adequate cybersecurity measures must be selected to prevent breaches** that could lead to environmental crises (*cf. opening example of the Colonial Pipeline incident*).
- **Geopolitical (and by extension social) effects on cybersecurity should not be underestimated by organizations**: After the Russia-Ukraine conflict escalated, 51% of organizations updated their business continuity and risk plans.

Call to action for companies

To **fully enjoy the benefits of integrating cybersecurity & ESG practices into their business**, companies should:

- Adopt a **proactive approach towards both ESG and cybersecurity** by integrating it into the business strategy.
- **Implement industry regulations and standards** (even when they are voluntary): it reinsures the audience & can open new markets.
- **Leverage cybersecurity & ESG regulations & standards** to build dual-compliance strategies.
- Balance the **benefits of cybersecurity with its environmental impact/cost**.
- Use **data analytics to design a sustainable business strategy;**
- **Embrace automation for daily tasks** so that teams can focus on enhancing the existing frameworks.
- **Upskill teams**: prioritize cybersecurity talent development alongside ESG training.

Call to action for policymakers

- Consider **cybersecurity in ESG requirements & vice-versa**.
- **Synchronise governance requirements**.
- Identify opportunities and **support the update of cybersecurity and ESG certifications**.

For more information, please contact:

Iva TASHEVA**, Cybersecurity Lead -** iva.tasheva@cyen.eu

Clémence BETESUKU, **ESG Lead -** clemence@theupliftagency.fr

Sources

Reports :

- Global Cybersecurity Outlook - Insight Report January 2024, *World Economic Forum*: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- Responsible investment 2024 - *Norges Bank Investment Management:* https://www.nbim.no/en/responsible-investment/divesting-from-companies/
- A microscope on small businesses - spotting opportunities to boost productivity, *McKinsey Global Institute* : https://www.mckinsey.com/mgi/our-research/a-microscope-on-small-businesses-spotting-opportunities-to-boost-productivity
- NIS Investments 2024, *Enisa*: https://www.enisa.europa.eu/publications/nis-investments-2024
- Cybersecurity for SMEs - Challenges and Recommendations, ENISA 2021 : https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf

Research paper :

- Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework - *Science Direct:* :https://www.sciencedirect.com/science/article/pii/S0267364924000542
- Which SMEs are greening? Cross-country evidence from one million websites, *OECD SME, and Entrepreneurship Papers*:https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/which-smes-are-greening_ffa14385/ddd00999-en.pdf
- 2025 Executive Benchmark on Integrated Reporting, *Workiva*: https://www.workiva.com/resources/2025-executive-benchmark-integrated-reporting

Press Release :

- Decrease in greenwashing for first time in six years, *RepRisk* : https://www.reprisk.com/research-insights/news-and-media-coverage/reprisk-data-shows-decrease-in-greenwashing-for-first-time-in-six-years-but-severity-of-incidents-is-on-the-rise

Articles :

- Why cybersecurity is a critical component of ESG - *WeForum.org* : https://www.weforum.org/stories/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/
- ESG & C: Does Cybersecurity Deserve its own pillar in ESG Frameworks - *Harvard Law, School Forum on Corporate Governance* : https://corpgov.law.harvard.edu/2022/11/14/esg-and-c-does-cybersecurity-deserve-its-own-pillar-in-esg-frameworks/
- Colonial Pipeline Cyber Incident, *US Department of Energy* : https://www.energy.gov/ceser/colonial-pipeline-cyber-incident
- Exclusive: The EU Commission's draft programme for 2025, *Euractiv* : https://www.euractiv.com/section/politics/news/exclusive-the-eu-commissions-draft-programme-for-2025/
- Women in tech: The best bet to solve Europe's talent shortage, *McKinsey* : https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/women-in-tech-the-best-bet-to-solve-europes-talent-shortage

Others :

- CSRD-CSDDD-Taxonomy > Our position on the Omnibus , *Open Letter by corporations* ; https://www.we-support-the-csddd.eu/wp-content/uploads/2025/01/240106-lt-C3D-Lettre-Commission-europeenne-6-janvier-2025.pdf
- CEO of World's Biggest SWF applies for Second Term, *Bloomberg Live*: https://www.youtube.com/watch?v=pp91Px7Cgsg

Annex 1 – EU-wide cybersecurity legislations

Process Legislation	**Measures for a high common level of cybersecurity across the EU (NIS2)** Directive (EU) 2022/2555 - applied across countries since **Oct 2024**	• Extensive list of cybersecurity requirements, incl. Suppliers, incidents reporting, and Board/C-level accountability. • Applicable to specific sectors: critical infrastructure ('Essential entities') or economic sectors, such as manufacturing, digital providers, research ('Important entities').
	Digital Operational Resilience Act (DORA) Regulation (EU) 2023/2554 - applied since **Jan 2025**	• Extensive list of ICT resilience & testing requirements, incl. suppliers, and incident, threats, vulnerability and risks' reporting. • Applicable to the financial sector at large (banks, insurance, digital infrastructure…)
	General Data Protection (GDPR) Regulation (EU) 2016/769 - applied since **May 2016**	• Article 32: Security of processing mandates implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk. • Scope: Processing of personal data of EU entity or persons in the EU
Product & process Legislation	**Cyber Security Act (CSA)** Regulation (EU) 2019/881 **-** applied since **Oct 2018**	• Lays down minimum requirements for cybersecurity certification, defines its level of assurance in a risk-based approach, and lays down governance standards. • Scope: ICT products, services and processes • Several candidate frameworks, incl. EUCC for trust products (active), Cloud & 5G (under development), digital identity wallets (to start)
Product Legislation	**Cyber Resilience Act (CRA)** Regulation (EU) 2024/2847 **-** applied as from **Sep 2026 - Dec 2027**	• Lays down minimum-security requirements, incident and vulnerabilities notification, user transparency of cybersecurity risks and mitigation measures. • Scope: Products with digital element placed on the EU market (e.g. consumer electronics, software, firewalls)
	AI Act Regulation (EU) 2024/1689 - cybersecurity requirements applied as from **Jul 2026**	• Lays down cybersecurity objectives for high-risk AI systems lifecycle.
	Medical Devices (MDR) Regulation (EU) 2017/745 **-** transition period ended in **May 2024**	• Manufacturers shall set out minimum IT security requirements, incl. protection against unauthorised access, necessary to run the software as intended. • Scope: Medical devices placed on the EU market.

Annex 2 – Major EU ESG legislations

	EU Taxonomy - entered into force in July 2020.
Process Legislation	• Classification system establishing a list of environmentally sustainable economic activities to facilitate sustainable investments. • **Scope**: aligns with the scope of the Corporate Sustainability Reporting Directive.
Product & process Legislation	**Sustainable Finance Disclosure Regulation (SFDR) - applicable since March 2021.**
	• Sets out how financial market participants must disclose sustainability information. • Applies to all financial market participants & financial advisors within the EU (asset managers, institutional advisors, insurance companies, pension funds, investment firms among others…) & to all financial products.
Process Legislation	**Corporate Sustainability Due Diligence Directive ("CSDDD") - entered into force in July 2024.**
	• Companies must now conduct **appropriate human rights and environmental due diligence** with respect to their operations, operations of their subsidiaries and operations of their business partners in companies' chain of activities. • **Scope**: EU companies with more than 1000 employees if they had an annual worldwide net turnover of more than 450M EUR in the last financial year / Non-EU companies with a net turnover in the UE of more than 450M EUR in the financial year preceding the last financial year.
	Corporate Sustainability Reporting Directive (CSRD) – applicable since January 2024.
	• Replaces the **Non-Financial Reporting Directive.** • **Modernizes and strengthens** the rules concerning the social and environmental information that companies must report. A key component of this regulation is **double materiality** i.e., the impact of sustainability on a company business and the company impact on sustainability. • **Scope and timeline**: please see Annex 3 - CSRD Scope. • **Limited external assurance on sustainability reporting**: level of assurance provided by auditors or reviewers. • Introduces the **European Sustainability Reporting Standards (ESRS)** for reporting under the CSRD. There are 12 ESRS with a simplified version for: listed SMEs, small banks & capture insurers. A mapping between **sustainability matters and the ESRS** is also to be performed.