KPMG

Cybersecurity in ESG

It’s time to view ESG and cybersecurity through the same lens.

kpmg.ch/cyber
kpmg.ch/esg

Contents

Introduction 3

Environmental considerations 4

Social considerations 6

Governance considerations 9

Conclusion — Creating new links between ESG and security 12

How KPMG professionals can help 13

Introduction

In today's digital economy, businesses face challenges in simultaneously meeting their environmental, social, and governance (ESG) targets and ensuring robust cybersecurity and privacy measures. Concerns relating to these areas have been at the forefront of global risk maps for several years.[1]

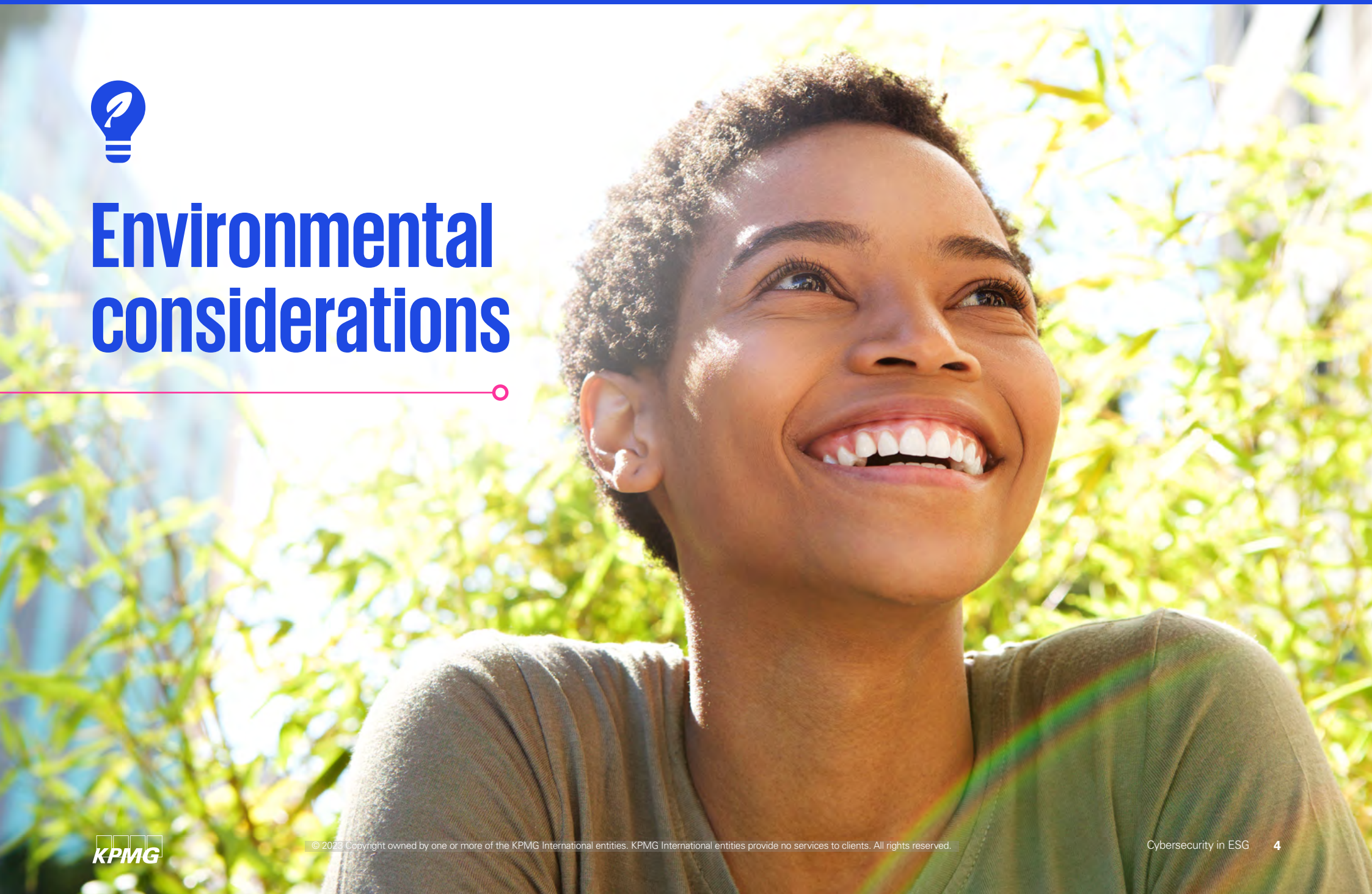
According to the KPMG 2022 CEO Outlook survey,[2] ESG and cybersecurity are crucial for corporate success. While environmental aspects of the ESG agenda have received significant attention, other elements such as cybersecurity and privacy have not been as well-developed. This is concerning as cyber threats are soaring in frequency — impacting business operations, continuity and reputations.

This paper aims to explore the connection between ESG and cybersecurity. It will discuss the expected benefits of managing these issues together and how an integrated approach can help safeguard an organization's health, business future, and the interests of their customers, clients, and business partners.

[1] www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
[2] CEO Outlook, KPMG, 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Environmental considerations



© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Critical infrastructure faces significant new risks

When it comes to ESG, environmental factors are a key consideration. However, ESG's link to cybersecurity, although less obvious, is becoming increasingly important. According to the 2022 KPMG survey, 64 percent of companies acknowledge climate change as a risk to their business.[3] KPMG professionals are starting to see cyberattacks that endanger the environment by targeting critical infrastructure such as power plants and water-processing facilities. Additionally, these attacks on industrial control systems can cause equipment malfunctions, environmental damage and hazards. Organizations need strong cybersecurity to protect their critical infrastructure against threats to their sophisticated and interconnected operational technology. As these incidents become more common, we anticipate greater regulatory focus.

Connect security to decarbonization, CO_2 reduction and the circular economy

Most plans for decarbonization and CO_2 reduction rely on digital transformation and the application of smart technologies and automated systems that monitor and manage energy production, distribution and consumption. However, these solutions can create new opportunities for cybercrime and demand a high level of cybersecurity and data protection. Similarly, introducing new technology solutions to support the circular economy when those systems involve significant financial transactions to incentivize green behaviors, can raise concerns over new fraud patterns.

Embedding cyber into these programs can help anticipate the cyber threat and ensure safe and secure operations. At the same time, adhering to data protection principles such as data minimization can reduce the risk of data breaches and ensure regulatory compliance.

The digital economy has led to a surge in data processing, resulting in the construction of data centers worldwide. Criminals have found opportunities to exploit weaknesses in the security of data centers and cloud services to steal computing resources, including cryptocurrency mining at scale. Unfortunately, the use of these systems has a negative impact on energy consumption and the carbon footprint, for example, implementing the required or best-practice cyber controls like having a secondary data center for improved resilience can lead to higher use of resources and energy.

Organizations today need to consider both the pros and cons of cyber resilience, striking a balance with cybersecurity and ESG targets.

[3] 'Big shifts, small steps' Survey of Sustainability Reporting, KPMG, 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Social considerations

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Impacts on society's digital landscape

Social considerations are also a critical aspect of ESG, and cyber risk can significantly impact society, particularly as global cyberattacks become more frequent and impactful. Digital applications and systems are now integrated into every aspect of our lives, from the personal devices we rely on and the social media we interact through to the sophisticated automated platforms and systems that support digital workplaces and lifestyles. The 2022 KPMG survey found that 49 percent of companies acknowledge social elements as a risk to their business.[4]

Data protection is critical

This integration can make you vulnerable to cyber risks that can lead to the theft of personal and sensitive information resulting in identity theft, financial fraud and other social harms. Cyberattacks can also disrupt critical healthcare, transportation and emergency services. To address these risks, organizations need strong privacy and cybersecurity measures to protect their data. Additionally, they should have robust incident response plans to minimize the impact of a cyberattack on critical services.

Ransomware attacks are soaring

Lucrative ransomware attacks continue to increase globally and can quickly cripple an organization's operations and reputation. Amid the severe consequences, many organizations are tempted to pay the ransom. Unfortunately, ransomware payments only encourages more crime and creates a costly cycle. To combat ransomware attacks, modern cybersecurity measures should be put in place to minimize their social and financial impact.

Freedom of speech faces new threats

Privacy and cybersecurity also play vital roles in protecting freedom of speech and securing today's proliferating digital communications channels. Legal protections, promoting digital and media literacy, and supporting diversity and inclusion in online spaces are also important measures. Encryption technologies can ensure that only intended recipients can access information without fear of eavesdropping or surveillance. Cybersecurity can also help mitigate the effects of disruptive attacks targeting websites and online platforms that facilitate free speech and expression.

Protect customer information to foster trust

Privacy controls can also play a key role in limiting the exploitation and misuse of personal information without consent or knowledge. This is vital in maintaining the public trust in organizations.

Before regulations such as the EU General Data Protection Regulation, many organizations believed they had ownership over the public's personal data. This changed with the introduction of these regulations. Individuals now have the right to their own personal data, including the right to know what data a company holds and the right to have it deleted.

[4] 'Big shifts, small steps' Survey of Sustainability Reporting, KPMG, 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

New concerns on AI and data ethics

Using artificial intelligence (AI) tools can speed up data collection but raises questions about ethical data usage by algorithms and machine learning. Biases can unfairly affect individuals or society as a whole. Organizations can positively or negatively impact society based on how they assess risks and safeguard the data they process. New regulations, like the EU AI Act, aim to ensure that AI is used in a way that does not harm.

Raising cyber awareness and literacy

Many organizations are emphasizing their purpose and social responsibility. They recognize that they have a role to play in promoting cybersecurity literacy and awareness, whether across their customer base or supplier ecosystem. These actions can help prevent fraud, encourage brand loyalty and reduce exposure to supply chain attacks.

Some organizations also pursue altruistic aims of building societal awareness of cyber threats, helping develop skills and promoting cybersecurity as a profession while supporting organizations such as charities that may not have the capacity and capability to fully secure their own systems. October is Cybersecurity Awareness Month, an annual campaign aimed at raising awareness about cybersecurity and providing resources for individuals and organizations to improve their cybersecurity practices. KPMG, among other organizations, are actively participating in this campaign to enhance security for all.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Governance considerations

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Keeping regulations in focus amid change

Governance is the third aspect of ESG as cyber risks can pose significant governance implications. There are various industry or market-specific cyber regulations, such as the US' Cybersecurity Risk Management for Investment Advisers, Strategy, Governance and Incident Disclosure, Investment Company Names Disclosure, and Nasdaq's Board Diversity Rule. In the EU regulations include the General Data Protection Regulation (GDPR), Digital Operational Resilience Act (DORA) and the revised Network and Information Systems Directive (NIS2).

ESG-related regulations include the European Union Sustainable Finance Disclosure Regulation (SFDR) and Corporate Sustainability Reporting Directive (CSRD). In the US, obligatory disclosure regulations include commission guidance regarding disclosure related to climate change, enhancement and standardization of climate related disclosures, rule ammendments to reg S-K Items 101, 103, 105 and enhanced disclosures by certain investment advisers and investment companies about environmental, social, and governance investment practices.

Measuring the effectiveness of an organization's privacy, cybersecurity and data management practices can help to determine how well they govern the data they process and share both internally and across borders.

ESG data and reporting need to be accurate

ESG data comes from four main sources: third party data, reported data, derived and functional data, and firm-owned raw data. Significant efforts are being put into ESG reporting and reporting assurance, but can you trust that the data is accurate and reliable? Cybersecurity is a critical factor critical factor in ensuring trustworthy ESG reporting. It works to protect data at its sources while being collected, in transit, and after it has been analyzed and reported. In addition, data privacy compliance is also required when personal data is processed in generating ESG reports.

ESG compensation models, reporting and data collection can involve automated processes, as well as data modeling and analysis. It is vital that these processes are not manipulated or biased to ensure accurate reporting.

Cybersecurity is relevant to all three ESG dimensions, so organizations at any stage of their ESG journey should consider reporting cyber posture as part of their ESG reporting. This helps to develop and sustain trust with their customers, employees and external stakeholders.

SASB and other standards focus on transparency

The Sustainability Accounting Standards Board (SASB) provides industry-specific standards for reporting on sustainability factors, including environmental, social and governance. The standards are financially important and aim to increase transparency and comparability in corporate reporting, which can help investors make more-informed investment decisions. However, fewer than half of companies have leadership level representation for sustainability.[5]

[5] 'Big shifts, small steps' Survey of Sustainability Reporting, KPMG, 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

One of the sustainability factors that SASB covers is cyber risk, which falls under the technology and communications industry, but many other sectors mention it too. Cyber risk is a factor that companies should consider disclosing in their public filings and is included under the Data Security disclosure topic, This topic covers a range of cyber threats that could compromise sensitive information and provides guidance on cyber risk management.

A similar standard, the Global Reporting Initiative (GRI), is widely used for sustainability reporting. GRI standards include guidance on how companies should disclose their management of cybersecurity and data privacy issues.

By including cyber risk as a material sustainability factor, SASB and GRI both recognize that cyber threats can significantly impact a company's financial performance, reputation and long-term sustainability. Companies that disclose their cyber risk management practices and provide information about their data security policies and procedures can improve their transparency and accountability to stakeholders, including investors, customers and regulators.

However, fewer than half of companies have leadership level representation for sustainability.[6]

Customers expect trustworthy services

Customers are more likely to do business with a company they trust to protect their personal and financial information. This is especially true for corporate customers, who value the safeguarding of their confidential data and intellectual property. Many industries have regulatory requirements for cybersecurity, and organizations that comply with these regulations are preferred by stakeholders. The KPMG survey found that less than half of companies disclose their governance risks.[7]

Both private and corporate customers want to ensure that the services they purchase meet their ESG and cybersecurity expectations. A company's commitment to ESG can be a sales enabler — enhancing its reputation, driving innovation, managing risks, ensuring compliance and improving access to capital. Therefore, it is important to consider how sustainable a company's privacy and cybersecurity practices are when doing business.

By addressing cyber risks within the context of ESG, companies can safeguard their operations, customers and reputation while fulfilling their broader social and environmental obligations.

[6-7] 'Big shifts, small steps' Survey of Sustainability Reporting, KPMG, 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Conclusion — creating new links between ESG and security

Organizations can benefit greatly by exploring the close connection between cyber and ESG risks. Both areas focus on identifying and managing risks and opportunities, leading to enhanced products and solutions and a better society. This connection is being increasingly recognized by markets, including ESG rating providers who strive for greater transparency and fairness in measuring and comparing organizations.

To protect their critical infrastructure, industrial control systems, and customer data, companies should have robust privacy and cybersecurity measures in place. Good news is many companies already do, which should positively impact their ESG performance. Additionally, companies should invest in sustainable technology solutions to help reduce environmental impact and minimize exposure to cyber risks.

Finally, companies should have strong governance structures to oversee privacy and cybersecurity risk management and ensure compliance with legal and regulatory requirements. By addressing cyber risks within the context of ESG, companies can safeguard their operations, customers and reputation while fulfilling their broader social and environmental obligations.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

How KPMG professionals can help

There's growing pressure for businesses to be transparent on their corporate commitment activities in cybersecurity and ESG. Cybersecurity is on the agenda for many regulators with growing demands for timely and comprehensive incident notification and disclosure of cyber security control maturity. And its connection to the ESG agenda is playing a huge role in the future of corporate social responsibility.

KPMG firms' have experience across the continuum — from the boardroom to the data center. In addition to assessing your cybersecurity and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, implement and monitor ongoing risks, helping you respond effectively to cyber incidents. No matter how you engage, you can expect to work with people who understand your business and your technology.

And whether you're entering a new market, launching products and services, or interacting with customers in a new way, sustainable growth is the only way to build a successful and resilient business.

KPMG professionals are committed to working with you to enhance trust, mitigate risk and unlock new value as you build a resilient business for a more sustainable future. With access to industry-leading experience, data-driven technology, and global alliances, you can turn insight into opportunity for your business, your people, and the planet. KPMG professionals can help you anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

KPMG. Make the difference.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Contacts

Mika Laaksonen
Global Cyber Security ESG Leader
and Partner
KPMG in Finland
mika.laaksonen@kpmg.fi

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG in India
atuteja@kpmg.com

Prasad Jayaraman
Americas Cyber Security Leader
and Principal
KPMG in the US
prasadjayaraman@kpmg.com

Dani Michaux
EMA Cyber Security Leader
and Partner
KPMG in Ireland
dani.michaux@kpmg.ie

Matt O'Keefe
ASPAC Cyber Security Leader
and Partner
KPMG Australia
mokeefe@kpmg.com.au

Nadine Hönighaus
Global ESG Governance Lead
and Partner
KPMG in Germany
nhoenighaus@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, unless otherwise indicated by quotation marks, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name:Cybersecurity in ESG | Publication number: 138862-G | Publication date: July 2023

Your contacts in Switzerland

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

Dr. Matthias Bossardt
Partner
Head of Cyber Security &
Digital Risk Consulting

+41 58 249 36 98
mbossardt@kpmg.com

Dr. Thomas Bolliger
Partner
Cyber

+41 58 249 28 13
tbolliger@kpmg.com

Patrick Schmucki
Director,
Financial Services,
Corporate Responsibility Officer

+41 58 249 27 35
pschmucki@kpmg.com

Nicolas Tinguely
Director
Cyber

+41 58 249 21 44
ntinguely@kpmg.com

Yves Bohren
Director
Cyber

+41 58 249 48 95
ybohren@kpmg.com

kpmg.ch/cyber

kpmg.ch/esg

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2023 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.