



energia per ispirare il mondo

Comunicare e promuovere la Cybersecurity attraverso i criteri ESG

Andrea Chittaro – Senior Vice President Global Security & Cyber Defence Snam spa



How can boards and CISOs speak the same language?

Data di pubblicazione: 23 agosto 2021

OPINION

Talk to the board, not just IT, about ransomware

The spread of fast-moving cyberattacks accelerates the need for rapid, clear communication between end-users, security teams and the board.

Speak the Board's Language to Communicate the Value of Security

March 28, 2019 | By Gavin Kenny | [3 min read](#)

The Language of Business: Where the Board of Directors and Security Leaders Can Meet

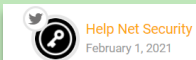
March 29, 2019 | By George Platsis | [4 min read](#)



Does Your Board Really Understand Your Cyber Risks?

by Daniel Dobrygowski and Derek Vadala

September 01, 2020



Share [f](#) [t](#) [in](#) [e](#)

Board members aren't taking cybersecurity as seriously as they should

WHY CYBER SECURITY MUST BE A BOARD-LEVEL CONCERN
[Advice, Cyber Essentials](#) / 1 February 2021

I responsabili della cybersecurity devono entrare nel board delle aziende



energia per ispirare il mondo

ENVIRONMENTAL, SOCIAL E GOVERNANCE

Quanto è di moda l'ESG: perché la sostenibilità è diventata un valore aggiunto per le aziende

NEWS

ESG (Environmental, Social, Governance): perché sempre più importanti?

COME MODERNIZZARE LA GOVERNANCE IN CHIAVE SOSTENIBILE

La trasformazione Esg del board

📅 30 Mar 2020 📄 Notizie 💬 Commenta ✉ Invia ad un amico

Un report Wbcsd identifica le sfide per i consiglieri di amministrazione. Attenzione a: struttura della governance; persone; processi, stakeholder e reporting. Le sei raccomandazioni chiave

Forbes

HEDGE FUNDS & PRIVATE EQUITY

ESG Is The Third Wave Of Change In Asset Management After Graham And MPT

Jacob Wolinsky Contributor

I write about hedge funds with a focus on emerging managers

Follow

Mar 28, 2022, 03:54pm EDT

U.S. Markets

Analysis: How 2021 became the year of ESG investing

By Ross Kerber and Simon Jessop



ENVIRONMENT • CORPORATE BOARDS OF DIRECTORS

Why modern boards need to invest in ESG for companies to thrive

By DAN REILLY

December 10, 2021 5:00 PM GMT+1

ESG & HORIZON SCANNING

Why Is ESG More Important Now Than Ever For Your Business?

POSTED ON 12TH MARCH 2022 BY AASHISH BEERGI



energia per ispirare il mondo



L'acronimo ESG si compone di 3 elementi:

ENVIRONMENTAL | SOCIAL | GOVERNANCE

3 dimensioni fondamentali per verificare, misurare, controllare e sostenere l'impegno in termini di sostenibilità di una impresa o di una organizzazione



- L'integrazione dei fattori ESG all'interno del processo decisionale favorisce una crescita sostenibile ed inclusiva che consente di creare e mantenere valore nel tempo.
- L'accesso al mercato dei capitali è sempre più vincolato al rispetto dei criteri di sostenibilità.
- Il sistema premiante del management sarà sempre più spesso correlato ad obiettivi in ambito ESG
- Le imprese necessitano di giustificare il proprio ruolo e la propria ragion d'essere



Criteri E (Environmental)

esaminano il modo in cui un'azienda contribuisce alle sfide ambientali (*rifiuti, inquinamento, emissioni di gas a effetto serra, deforestazione e cambiamenti climatici*) e le sue performance in tal senso

Criteri S (Social)

analizzano il modo in cui l'impresa tratta le persone (*la gestione del capitale umano, la diversità e le pari opportunità, le condizioni di lavoro, la salute e la sicurezza e la vendita abusiva di prodotti*)

Criteri G (Governance)

valutano il modo in cui un'azienda è amministrata (*remunerazione dei dirigenti, strategia e pratiche fiscali, corruzione e abuso d'ufficio, diversità e struttura del consiglio*)



- **Direttiva EU 2014/95 (Italia al d.lgs. 2016/254)** introduce l'obbligo per le aziende quotate (+500 dipendenti) di pubblicare annualmente la Dichiarazione non finanziaria (bilancio di sostenibilità) → FUTURO: estensione obbligo a tutte le aziende quotate e non quotate con +250 dipendenti
- **Action Plan europeo (2018)**, favorire uno sviluppo sostenibile che soddisfi le esigenze delle generazioni presenti e future, creando anche nuove opportunità di occupazione, investimento e garantendo la crescita economica.
- **Regolamento (UE) 2019/2088 – Sustainable Finance Disclosure Regulation**
- **Green Deal Europeo (2021)**

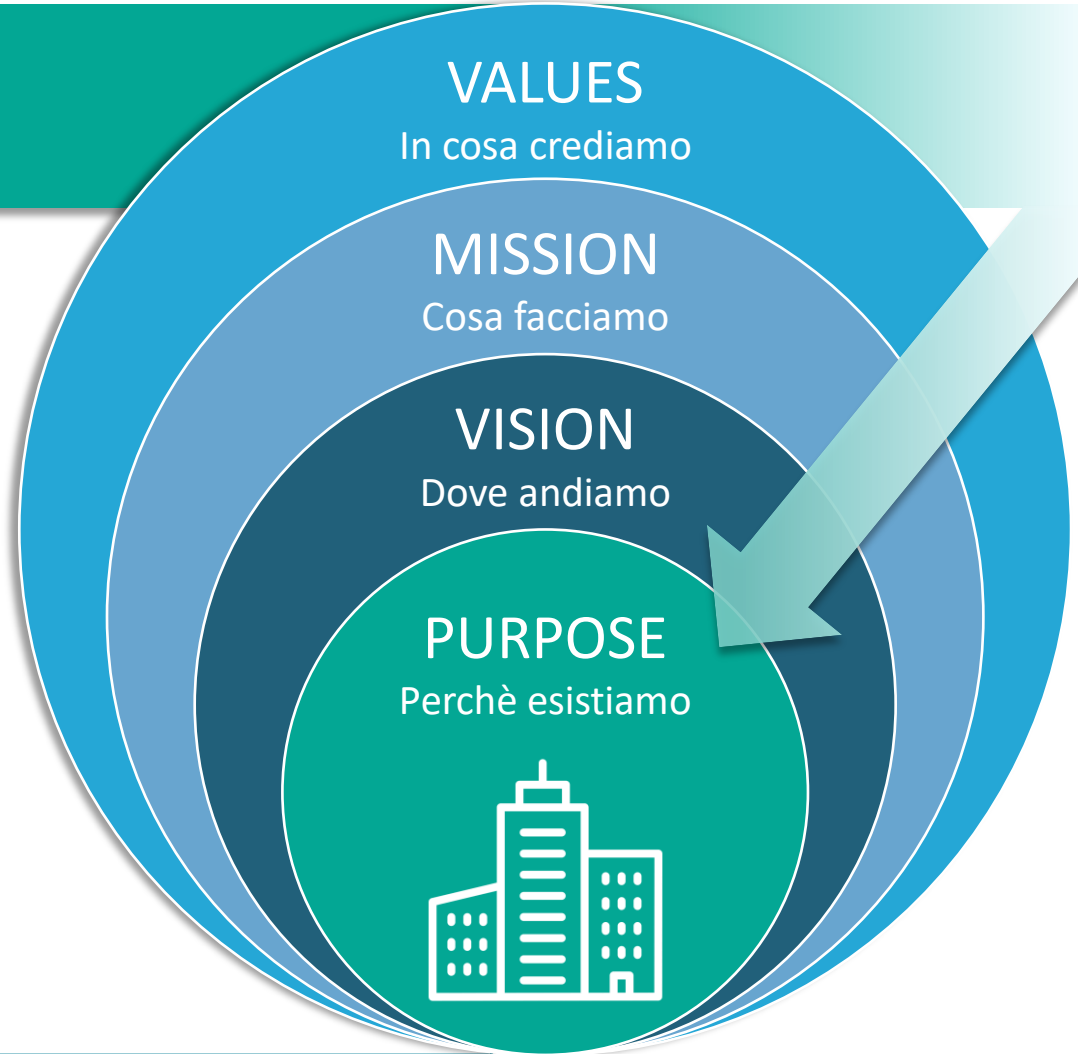


energia per ispirare il mondo



PURPOSE

- Insieme di idee, valori e propositi; lo scopo ultimo, la finalità per la quale **un'impresa esiste ed opera**
- Influenza il modo in cui è gestita l'azienda, **orientando le strategie e le decisioni soprattutto in momenti di crisi**
- Il **profitto** non è il punto di partenza, ma la **conseguenza di un circolo virtuoso**
- L'idea di un **business incentrato solamente sul miglioramento del bilancio** economico è ormai **obsoleta**





Cybersecurity e ESG



L'opinione di Johan Van Der Biest di Candriam

Un aspetto positivo: la cybersecurity a livello aziendale post-COVID 19

22 Dicembre 2021

ESG NEWS

CHI SIAMO NEWS E EVENTI GALLERY **aipsa** MEMBERSHIP NORMATIVE CONTATTI

Cybersicurezza, privacy, perimetro aziendale, ESG. Intervista ad Andrea Chittaro e Massimo Cottafavi

How does ESG relate to data privacy?

REDCL^oVER
ADVISORS

Even though privacy has not historically been considered an ESG issue, an increased focus on responsible data management has started a trend of including privacy-related disclosures in sustainability reports. This is especially true since the Global Reporting Initiative added a privacy standard. In fact, over the past five years, there has been a **920% increase** in corporate commentary on data privacy issues.



energia per ispirare il mondo

Global Cybersecurity: Why is it a Worldwide Social Concern?

J.P.Morgan

THE WALL STREET JOURNAL.

English Edition Print Edition Video Podcasts Latest Headlines

Subscribe
SPRING

Call to Action: Consider ESG Risk From Third Parties

With stakeholders increasing their demand for action on environmental, social, and governance issues, organizations should consider how these elements are addressed by engaged third parties.

CYBERSECURITY360

Cybersecurity Nazionale Malware e attacchi Norme e

Cybersecurity domestica e smart working: consigli per la sicurezza dei telelavoratori

CRISIS RESPONSE

Home About Us Editions News And Blogs Events Get Involved Subscribe Listen

Is cyber resilience the new ESG?

Andrea Bonime-Blanc and Maya Bundt say there is currently no way of gauging the cyber resilience of organisations, suppliers or service providers, as there is currently no information available. This has to change.

Cybersecurity is an environmental, social and governance issue. Here's why

WORLD
ECONOMIC
FORUM

10 **Economia** Lecco

LA PROVINCIA
MARTEDÌ 29 MARZO 2022

Sicurezza informatica sui banchi di scuola

La Cyber week. Il Badoni inaugura un ciclo di lezioni con la collaborazione dell'azienda Easynet. È il primo istituto a farlo, la didattica italiana ancora non si occupa di un tema molto caro alle aziende

ESIGENZE DI (CYBER) SECURITY

IMPOSTAZIONE ATTIVITÀ IN CHIAVE ESG

IDENTIFICARE DESTINATARI/ BENEFICIARI

MANAGEMENT

CLIENTI

FORNITORI E PARTNER

ISTITUZIONI

COLLETTIVITÀ



energia per ispirare il mondo



SECURITY AWARENESS



energia per ispirare il mondo



SECURITY AWARENESS

ESIGENZE DI (CYBER) SECURITY

RIDURRE L'ESPOSIZIONE ALLE
MINACCE RIVOLTE AGLI UTENTI
E A CUI GLI UTENTI POSSONO
ESPORSI ATTRAVERSO
COMPORTAMENTI SUPERFICIALI

IMPOSTAZIONE ATTIVITÀ IN CHIAVE ESG

INIZIATIVE DI AWARENESS

- Vademecum di Security
- Multimediali di Security
- Mail giornaliera cyber SOC
- Incontri periodici informali
- Simulazioni White Phishing



SECURITY AWARENESS

OH NO! SEI CADUTO NELLA RETE!

Hai cliccato su una mail di phishing creata per scopi formativi. Mail apparentemente legittime potrebbero essere un'esca: non abboccare!

Riconosci questo messaggio?

Non farti catturare!
Presta attenzione a:

Proteggiti!

INDIRIZZO MAIL

Il dominio del mittente potrebbe sembrare familiare ma con delle piccole differenze rispetto all'indirizzo mail della persona o società impersonificata dall'attaccante. Controlla sempre che l'indirizzo mail del mittente corrisponda a quello reale, spostando il cursore in corrispondenza del nome del mittente!

TESTO

Il messaggio potrebbe contenere errori grammaticali, di datatoc o refusi: leggi sempre molto attentamente le comunicazioni che ricevi!

CONTENUTO

L'e-mail potrebbe includere link o allegati sospetti contenenti minacce informatiche: per proteggere i tuoi dispositivi, poni sempre attenzione alla fattibilità e attendibilità della richiesta rispetto al contesto della comunicazione prima di dare seguito all'indirizzo riportato nel messaggio!

PIATTAFORME SERVIZI & SOCIAL MEDIA

L'e-mail potrebbe proporti dei servizi conosciuti o familiari rispetto al contesto aziendale di riferimento: verifica sempre quali sono le applicazioni autorizzate e utilizzate ufficialmente all'interno della tua organizzazione. Non utilizzare password e credenziali aziendali per la registrazione a servizi non legati all'attività lavorativa!

IDENTITÀ

L'attaccante potrebbe celare la propria identità dietro a generalità fittizie: diffida sempre da tutti quei mittenti sconosciuti che firmano un messaggio in maniera insolita o bizzarra. Accertati sempre sull'affidabilità del tuo interlocutore prima di dare seguito a richieste insolite o sospette!

Per maggiori informazioni su come gestire al meglio la casella di posta elettronica, ti invitiamo a consultare i video presenti all'interno della piattaforma LMS, cliccando sull'immagine in basso e digitando "Giochi di Security" nell'homepage:



Se credi di aver ricevuto una mail sospetta, utilizza il pulsante "segnala mail sospetta" presente in Outlook. Per chiarimenti o supporto, scrivi una mail a cybersecurity@snam.it

*Snam tutela la privacy dei propri dipendenti. Nessuna informazione personale (es. e-mail, Username, Password, etc.) è stata registrata nel corso della simulazione. Se ti è già successo di ricevere comunicazioni contenenti richieste simili, ti consigliamo sempre di modificare le tue credenziali d'accesso per una maggiore sicurezza.

Nell'ambito dell'iniziativa "A Virtual coffee with..." promossa ed organizzata da Snam, avrò il piacere di trascorrere del tempo con amici e colleghi per parlare di cybersecurity.

Sarà l'occasione per ribadire che la sicurezza delle informazioni, dei sistemi e di qualsiasi "oggetto" connesso in rete, tanto in ambito lavorativo quanto nella vita privata, non può essere tout court demandata a quelli che, più o meno a ragione, consideriamo essere gli "addetti ai lavori"; ognuno può fare la differenza, diventare la "prima linea di difesa", per sé e per gli altri... nel corso dell'incontro, insieme, vedremo come... ☺ Per le persone di Snam, su Easy tutte le info per partecipare!

#Snam4security #cybersecurity #securityawareness

BEST PRACTICES PER LA CYBERSECURITY

All'interno di una società digitalizzata e interconnessa come quella in cui viviamo, le possibilità di subire un attacco informatico sono aumentate sensibilmente: ogni 39 secondi si registra un tentativo di attacco o frode nel web e circa 30.000 siti internet vengono colpiti quotidianamente. Favorire la protezione di dati ed informazioni gestite digitalmente, siano esse personali o aziendali, è uno degli obiettivi che Snam si pone sul fronte della cybersecurity ed il suo raggiungimento implica il coinvolgimento di tutti gli utenti.

In molti casi si cerca infatti di sfruttare errori o comportamenti imprudenti da parte degli utenti per ottenere l'accesso a dati sensibili e informazioni riservate.

Due tipologie di attacco è in particolare bene che siano note a tutti in modo da rendere anche più facile identificarle e difendersi: il **Phishing** ed il **CEO Fraud**

Phishing

Sfruttando la posta elettronica, un malintenzionato simula l'inoltro di una comunicazione da parte di un mittente noto o attendibile per indurre in errore il destinatario e avere accesso a dati che dovrebbero rimanere privati, ad esempio inoltrando un link, un allegato o chiedendo

SNAM - SOC Daily Update - 21/04/2022



Buongiorno,

a seguire l'update relativo al periodo che va dalle 18:30 del 20/04/2022 ad ora:

Security Monitoring:

- **SIR0061461** - Predictable Resource Location - Aperto incident **INC0565206** per blocco IP.
- **SIR0061466** - Potential Exploit detected contenente Predictable Resource Location - Aperto incident **INC0565223**: Blocco IP
- **SIR0061467** - Potential Exploit detected contenente Predictable Resource Location - Aperto incident **INC0565224**: Blocco IP
- **SIR0061468** - Potential Exploit detected contenente Misc Exploit - Aperto incident **INC0565228**: Blocco IP

Security Prevention:

- **SIR0061465** - FBI: rilasciato alert sull'ALPHV Team - Aperto incident **INC0565220**: Blocco IP, Blocco HASH
- **SIR0061464** - Ucraina 106: Gamaredon Group continua a colpire organizzazioni del Paese con nuove varianti del malware Pterod - Aperto incident **INC0565221**: Blocco URL, Blocco HASH
- **SIR0061462** - Conti ransomware: variante Linux punta agli hypervisor ESXi - Blocco HASH

Attività in corso:

- Nessuna

Varie ed eventuali:

- Nessuna

Cordiali saluti,

CSRT – Cyber Security Response Team
Global Security & Cyber Defence Dpt.



Via dell'Unione Europea, 4
20097 San Donato Milanese (MI) - Italy
Ph. + 39 02 3703 9124
cybersecurity@snam.it
www.snam.it



energia per ispirare il mondo



SECURITY AWARENESS

ESIGENZE DI (CYBER) SECURITY

RIDURRE L'ESPOSIZIONE ALLE
MINACCE RIVOLTE AGLI UTENTI
E A CUI GLI UTENTI POSSONO
ESPORSI ATTRAVERSO
COMPORTAMENTI SUPERFICIALI

IMPOSTAZIONE ATTIVITÀ IN CHIAVE ESG

INIZIATIVE DI AWARENESS

- Vademecum di Security
- Multimediali di Security
- Mail giornaliera cyber SOC
- Incontri periodici informali
- Simulazioni White Phishing
- IRM

IDENTIFICAZIONE DESTINATARI/BENEFICIARI

UTENTI SOCIETÀ

FAMIGLIE DEI COLLEGHI

ISTITUZIONI (Compliance)

**SOCIETÀ | FORNITORI |
PARTNER (in via indiretta)**



SUPPLY CHAIN SECURITY



energia per ispirare il mondo

SUPPLY CHAIN SECURITY

ESIGENZE DI (CYBER) SECURITY

RIDURRE L'ESPOSIZIONE A
MINACCE DIRETTE O INDIRETTE
DERIVANTI DALLO
SFRUTTAMENTO DI
VULNERABILITÀ DI TERZE PARTI
COLLEGATE ALLA SOCIETÀ

IMPOSTAZIONE ATTIVITÀ IN CHIAVE ESG

- Processo di monitoraggio del cyber security rating delle terze parti
- Revisione Patto Etico
- Introduzione di clausole contrattuali ad hoc
- Security Intelligence e prevention

IDENTIFICAZIONE DESTINATARI/BENEFICIARI

FORNITORI E PARTNER

SISTEMA PAESE

ISTITUZIONI (Compliance)



REPORT DI SOSTENIBILITÀ

2021

Energy to inspire the world



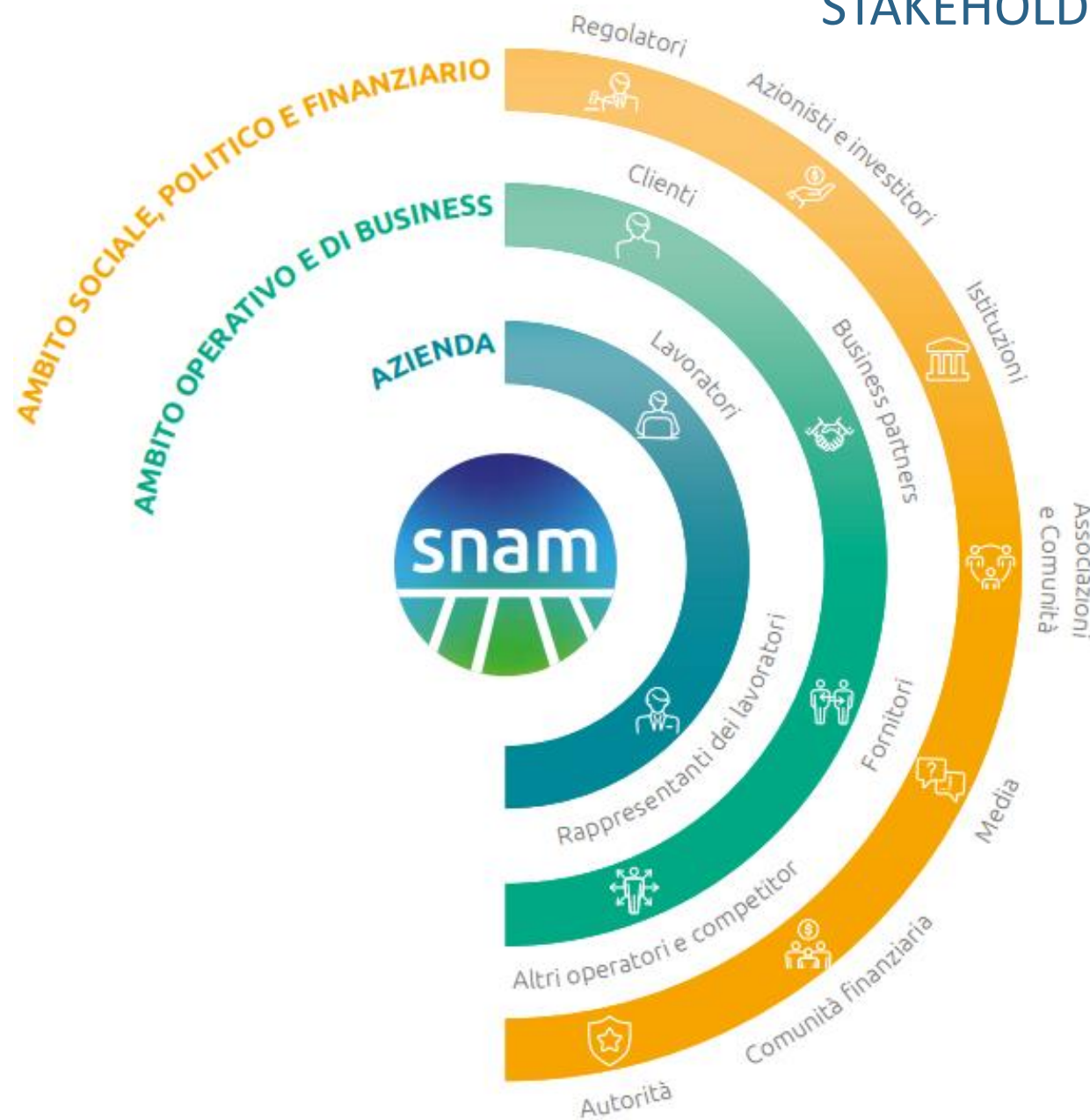
REPORT DI SOSTENIBILITÀ 2021

Energy to inspire the world



energia per ispirare il mondo

STAKEHOLDER SNAM

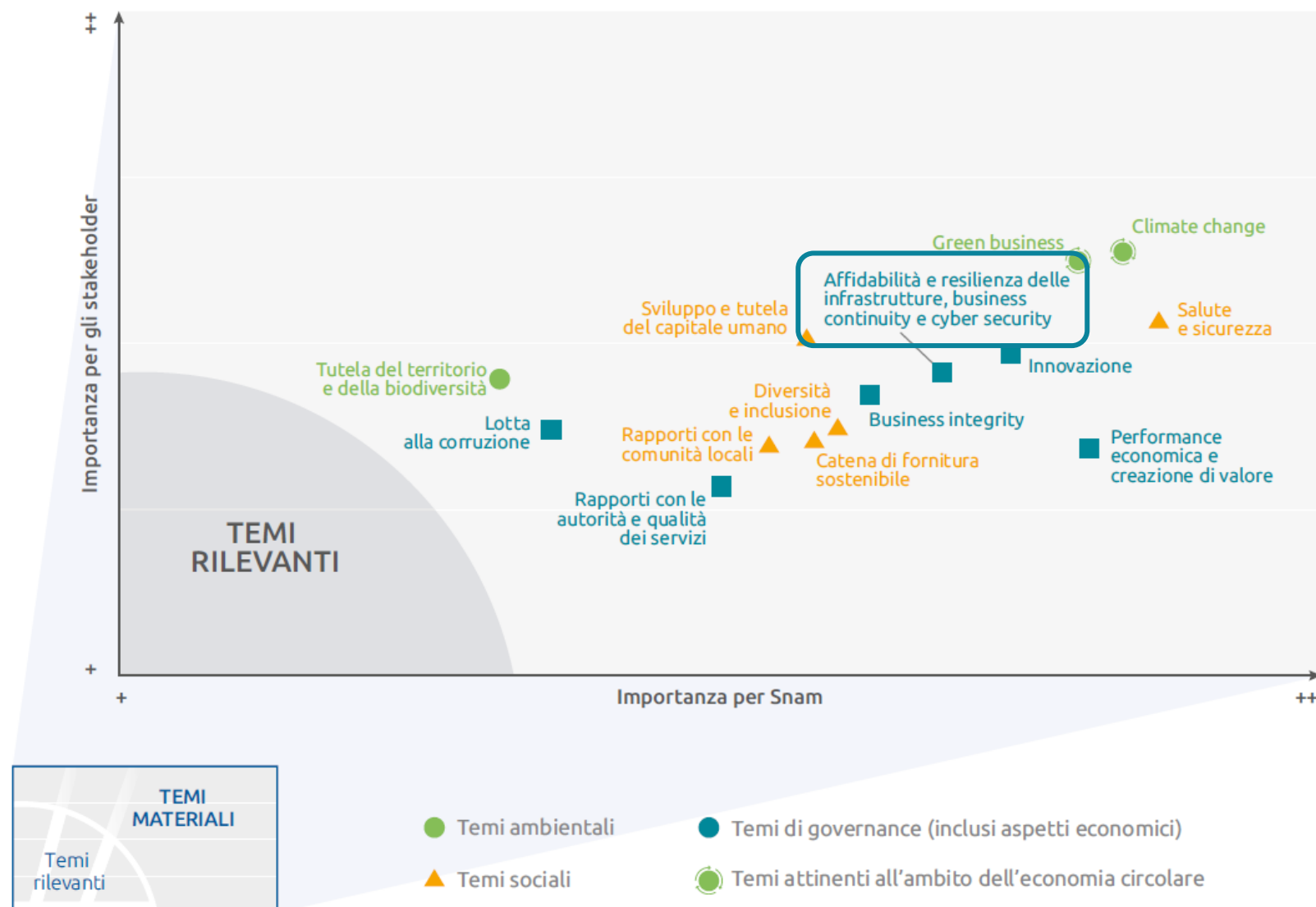


REPORT DI SOSTENIBILITÀ 2021

Energy to inspire the world



MATRICE DI MATERIALITÀ 2021 - TEMI MATERIALI



energia per ispirare il mondo

REPORT DI SOSTENIBILITÀ 2021

Energy to inspire the world



energia per ispirare il mondo

Come primo anno di applicazione di tale metodologia, di seguito sono rappresentati i risultati dell'analisi per 3 temi materiali, uno per ogni cluster della sfera E-S-G, sottoforma di case study, in cui per ognuno di essi sono riportati gli impatti di Snam verso l'esterno, nonché i rischi e le opportunità che influenzano il business.



Climate change



Sviluppo e tutela
del capitale umano



Affidabilità e resilienza
delle infrastrutture,
business continuity
e cyber security

GLI STAKEHOLDER AL CENTRO

Affidabilità e
resilienza delle
infrastrutture,
business continuity
e cyber security



Assicurare l'**affidabilità delle infrastrutture e dei servizi** al fine di prevenire e/o mitigare potenziali situazioni che potrebbero compromettere la continuità del business (es. emergenze, eventi pandemici). **Gestire la sicurezza informatica** con particolare riferimento a potenziali cyber attack.



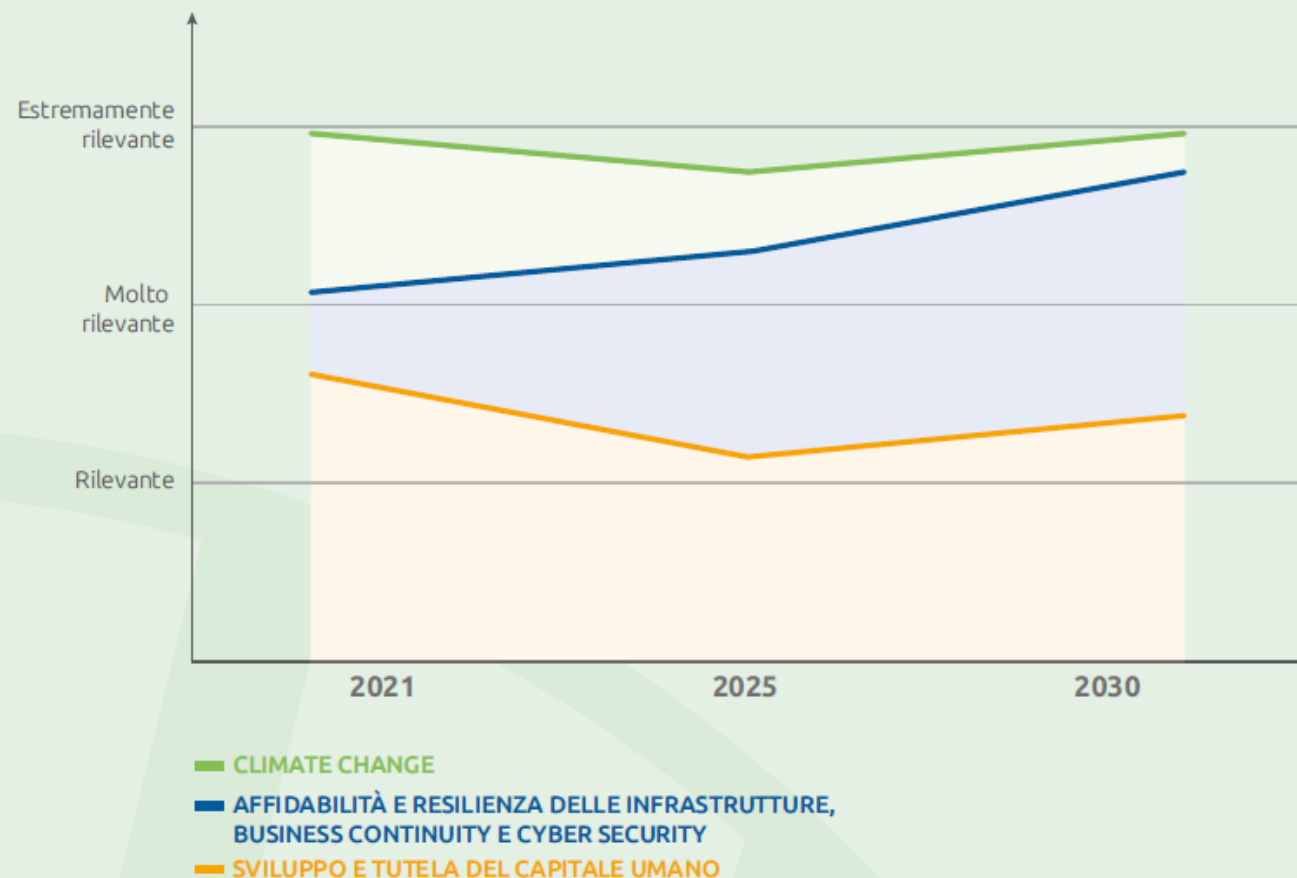
REPORT DI SOSTENIBILITÀ 2021

Energy to inspire the world



energia per ispirare il mondo

Per tale motivo, nel corso del 2021, Snam ha coinvolto il Top Management e alcune categorie di stakeholder, chiedendo loro di indicare possibili cambiamenti nella rilevanza dei temi materiali al 2025 e al 2030 (gli orizzonti temporali del Piano e della Vision di Snam). Prendendo in considerazione i temi analizzati nell'ambito della doppia materialità, emerge che la loro rilevanza rimarrà pressoché allineata a quella attuale. Nei prossimi anni, a seguito della pubblicazione delle linee guida metodologiche che definiranno il processo di doppia materialità, Snam affinerà ulteriormente la metodologia di analisi, fornendo i risultati per l'intero panel dei temi materiali.



REPORT DI SOSTENIBILITÀ

2021

Energy to inspire the world



Affidabilità e resilienza delle infrastrutture, business continuity e cyber security

L'evoluzione dei business, la sempre maggiore digitalizzazione dei processi, l'utilizzo di nuove tecnologie e il ricorso a soluzioni innovative idonee a migliorarlo, portano le aziende ad investire sempre maggiori risorse nell'ambito della cyber security, dove un sistema affinato e solido può contrastare minacce destinate sempre più ad evolvere in futuro in termini di numerosità, complessità e sofisticazione. Mantenere ed aggiornare con continuità un apparato aziendale di cyber security, orientato alla cyber-resilience (resilienza cibernetica), risulta infatti indispensabile per garantire la continuità operativa dell'organizzazione, la sicurezza dell'infrastruttura e la protezione dei dati. Al fine di presidiare costantemente il tema della continuità del business e dell'affidabilità delle infrastrutture, nonché della cyber sicurezza, Snam ha implementato una complessa architettura tecnologica, facendo affidamento ad un modello integrato di processi e soluzioni basati su elevati standard di affidabilità e qualità del servizio in grado di favorire la gestione efficiente del sistema gas per l'intero Paese. Inoltre, ha creato una funzione ad hoc per la sorveglianza e il presidio della cyber security, con l'obiettivo di prevenire e mitigare eventuali attacchi, nonché di diffondere all'interno e all'esterno dell'organizzazione una cultura sulla sicurezza informatica.



IMPATTO DI SNAM SU AMBIENTE, ECONOMIA E SOCIETÀ



La corretta manutenzione delle infrastrutture da parte dell'organizzazione garantisce l'erogazione del servizio



L'inadeguata manutenzione delle infrastrutture e / o l'indisponibilità dei sistemi IT, relativi ai servizi di trasporto e bilanciamento, nonché ai processi di dispacciamento, può generare disagio clienti e fornitori



La mancata/inadeguata gestione della sicurezza informatica da parte dell'organizzazione può comportare una perdita di dati sensibili di dipendenti, clienti e fornitori



Presenza del Cybersecurity Incident Response Team a garanzia della continuità del servizio e sicurezza di tutto il Sistema Paese

IMPATTO DEL CONTESTO ESTERNO SU SNAM



Rotture/lesioni alle condotte di responsabilità di terzi possono causare disservizi impiantistici impattando sulla continuità del servizio erogato, con possibili sanzioni per mancato ripristino nelle tempistiche prestabilite



Cyber attack da parte di cyber criminali, cyber hacktivist, gruppi d'azione state-sponsored con impatti nella business continuity, nella funzionalità degli asset e nella protezione di dati sensibili



Impatto positivo



Impatto negativo



energia per ispirare il mondo



energia per ispirare il mondo

Comunicare e promuovere la Cybersecurity attraverso i criteri ESG

Andrea Chittaro – Senior Vice Presidente Global Security & Cyber Defence Snam spa

