LINEA GUIDA IN MATERIA DI GLOBAL SECURITY

Documento approvato dal Consiglio di Amministrazione in data 14 febbraio 2024

Sommario

1. Obiettivo e ambito di applicazione

Obiettivo della presente Linea Guida è illustrare i principi adottati da Snam per prevenire i rischi di security e ridurre l'impatto di eventi potenzialmente in grado di generare effetti negativi per la società.

Il documento si applica a Snam e alle società Controllate soggette ad attività di direzione e coordinamento ed è inoltre portata a conoscenza delle altre società partecipate allo scopo di promuovere principi e comportamenti coerenti con quelli espressi da Snam, conformi con le procedure interne di riferimento (*Linea Guida in materia di Privacy, Linea Guida Risk Assurance Compliance Integrata, Linea Guida Enterprise Risk Management, Policy sull'utilizzo etico dell'intelligenza artificiale*).

2. Principi fondamentali

La specificità del business in cui Snam opera, la presenza significativa sul territorio nazionale ed estero, i problemi socio-politici anche di livello locale, il ricorso massivo alle tecnologie digitali, gli eventi terroristici e le nuove forme di imprenditorialità illegale e criminale, sommandosi alle minacce tradizionali che una grande impresa si trova a fronteggiare, impongono un sempre maggior impegno nelle politiche di tutela della sicurezza del personale e del patrimonio aziendale. Tutto ciò induce ad eseguire, su base continuativa, una consapevole ed efficace valutazione e gestione dei rischi di security, attività questa a cui ciascuno è chiamato a partecipare per la parte di propria competenza e nell'ambito del proprio ruolo, attraverso:

- l'applicazione uniforme e puntuale degli indirizzi di security;
- l'allocazione delle risorse necessarie ad assicurare il dispiego delle idonee misure negli ambiti della sicurezza fisica, logica ed organizzativa;
- l'impegno a considerare la prevenzione dei rischi di security come parte integrante delle attività gestionali e di business;

- la diffusione della cultura della security anche supportando le iniziative di comunicazione, sensibilizzazione, formazione ed aggiornamento rivolte al personale e a terze parti che collaborano con la società.

Snam promuove un modello di gestione integrata della security aziendale volto ad ottimizzare risorse, processi e risultati.

A tal fine, elabora modelli di prevenzione e gestione dei rischi di security, idonei ad identificare le minacce e le vulnerabilità e a valutarne il relativo rischio, individuando ed attuando le misure di mitigazione più efficaci. Per tali finalità e alla luce delle previsioni di standard e best practices in materia, la Funzione Global Security & Cyber Defence definisce le linee guida tecniche e le metodologie, individua gli standard di riferimento, nonché garantisce la progettazione, la realizzazione e la gestione, delle attività relative ai seguenti ambiti di security:

1. **Physical & Personnel Security**: complesso di misure, soluzioni ingegneristiche, tecnologiche e procedurali, volte a prevenire o mitigare potenziali rischi di security gravanti sulle persone e sugli asset fisici del patrimonio aziendale, ivi compresa la sicurezza del personale espatriato ed in viaggio all'estero.
2. **Information & Cyber Security**: insieme degli assetti organizzativi, procedurali e tecnologici finalizzati alla protezione del patrimonio informativo aziendale definiti con l'obiettivo di prevenire e contrastare, ove necessario, fenomeni quali, a titolo esemplificativo, il furto di identità, il danneggiamento della normale funzionalità delle infrastrutture critiche, la manipolazione o sottrazione di informazioni privilegiate, l'alterazione delle informazioni utilizzate, il sabotaggio delle tecnologie implementate.
3. **Business Resilience & Crisis Management**: insieme di strategie, processi e modelli che favoriscono la capacità di operare anche in condizioni avverse e che garantiscono il governo delle azioni e delle iniziative che i diversi soggetti aziendali coinvolti sono chiamati ad attuare per assicurare l'operatività aziendale in presenza di emergenze e crisi di natura sistemica.

4. **Counterpart Risk Management**[1]: attività che, svolta nel pieno rispetto delle normative vigenti e del Codice Etico Snam, consente di fornire alle unità aziendali che ne facciano richiesta informazioni elaborate e correlate utili per le decisioni aziendali attuali e future, per la difesa dei diritti, delle persone, del patrimonio aziendale materiale e immateriale. Le attività di due diligence reputazionale riguardano persone fisiche e giuridiche che a qualsiasi titolo hanno o possono avere rapporti con Snam e costituiscono presidio primario nella prevenzione dei fenomeni corruttivi e di infiltrazione criminale.
5. **Investigation & Forensics**: attività di investigazione, svolte anche con il supporto di professionisti abilitati, nei confronti di minacce interne o esterne, attuate anche attraverso strumenti informatici.

3. Metodologia di lavoro

Al fine di contribuire alla creazione di valore e garantire il costante allineamento ai requisiti di business, nell'ambito della gestione della security aziendale viene posta particolare attenzione all'evoluzione delle minacce e ai cambiamenti imposti dall'innovazione tecnologica, con l'obiettivo di garantire la tempestiva adozione delle strategie di prevenzione e difesa più idonee al raggiungimento dei livelli di tutela ritenuti adeguati.

In tal senso la Funzione Global Security & Cyber Defence recepisce e fa propri i precetti e le migliori pratiche internazionali volte alla gestione dei rischi di security[2], impegnandosi a garantire che siano opportunamente attuate dal personale, dai fornitori e più in generale da tutti gli stakeholder.

Nel rispetto del principio del miglioramento continuo, è prevista sia una fase di verifica e controllo dell'efficacia delle iniziative attuate[3], sia un monitoraggio continuativo delle nuove esigenze.

Le attività il cui espletamento richiede specifiche professionalità in ambito security sono svolte esclusivamente da personale in possesso della necessaria esperienza e di adeguate competenze[4], ove necessario certificate ed in ogni caso tenute costantemente aggiornate attraverso attività mirate di formazione.

4. Processo di Security

Il processo di Security in Snam si fonda su un approccio olistico, il solo ritenuto in grado di fornire un quadro coerente di indirizzo, coordinamento e controllo dei diversi presidi ed attività.

Esso garantisce, inoltre, il costante monitoraggio e la valutazione degli eventi di sicurezza accaduti o potenziali, al fine di contenere eventuali incidenti ed affrontare con tempestività situazioni negative che possono incidere sulla capacità operativa della società minacciandone in via potenziale le prospettive di lungo termine e la reputazione.

Il summenzionato processo di security permette di supportare efficacemente l'azienda nel:

- tutelare dalle possibili conseguenze di un evento di security, l'asset ritenuto più importante, le persone;
- soddisfare i requisiti di business e, più in generale, gli aspetti connessi alla tutela dell'immagine e dell'operatività aziendale;
- rispettare i requisiti cogenti e regolamentari, sia imposti dallo Stato sia da altri enti di natura non statale, quest'ultimi discendenti da norme adottate su base volontaria;
- prevenire gli incidenti di security al fine di preservare il patrimonio aziendale dalle possibili conseguenze che il verificarsi di un evento indesiderato potrebbe comportare (ad es. danni economici, legali e/o reputazionali);
- contenere le conseguenze degli incidenti di security e garantire la resilienza aziendale, agevolando l'attuazione di risposte immediate ed in grado di riportare rapidamente l'azienda nelle condizioni di normalità;
- assegnare le risorse necessarie per un'efficace gestione della sicurezza fisica, logica ed organizzativa;

[1] L'attività di Counterpart Risk Management e Due Diligence Reputazionali è dettagliata nell'Allegato 1 alla presente Linea Guida.
[2] Ad esempio lo standard ISO 31000 - Risk Management.
[3] Le verifiche, effettuate nell'ottica del miglioramento continuo, possono avvenire secondo differenti modalità, quali ad esempio audit di sicurezza, verifiche puntuali su aspetti organizzativi o tecnologici, esercizi simulati, raccolta informazioni per mezzo di questionari.
[4] Come ad esempio previsto dalla norma UNI 10459.

- definire legami e relazioni con terze parti al fine di condividere informazioni e best practices;
- diffondere la cultura della sicurezza attraverso la sensibilizzazione e l'arricchimento del patrimonio conoscitivo dei singoli individui;
- indirizzare, anche nell'ambito delle attività di security, iniziative coerenti con i principi di etica e sostenibilità cui è ispirata l'intera azione della società in linea con i principi ESG.

Qualora ritenuto necessario[5], Snam implementa in determinati ambiti operativi Sistemi di Gestione formali e certificabili; a titolo di esempio, Sistemi di Gestione per la Continuità Operativa[6] e per la Sicurezza delle Informazioni[7].

5. Cyber Security & AI Committee e Management Meeting

Per rispondere proattivamente ai mutamenti nei bisogni di sicurezza dovuti alle repentine variazioni negli scenari internazionali, ai cambiamenti nel contesto di business, all'evoluzione tecnologica, alla crescente pervasività della Cyber Security in tutti gli ambiti di attività nonché alle esigenze di garantire la compliance al quadro normativo dettato dal Regolamento GDPR, dalla Direttiva NIS, dal Perimetro di Sicurezza Nazionale Cibernetica oltre che a temi correlati all'introduzione di strumenti di *Artificial Intelligence* e, più in generale, da ogni normativa afferente i temi di sicurezza nazionale e tutela delle infrastrutture critiche, viene individuato un Cyber & AI Security Committee (CSC), che si riunisce con cadenza mensile, presieduto dall'Executive Director Global Security & Cyber Defence e composto dal Director Cyber Security & Resilience e dai suoi diretti riporti, dal Chief Strategy And Technology Officer e suoi diretti riporti, dal Data AI Officer, dal Data Protection Officer nonché dall'Executive Director Organizational Development, Total Reward & Cost. In questo contesto vengono condivisi ed approfonditi i temi con il maggior grado di rilevanza e/o criticità per la corretta gestione della cyber sicurezza ed il mantenimento della più idonea postura di difesa. In particolare:

1. nel CSC: eventuali ulteriori referenti di altre funzioni aziendali possono essere invitati in funzione degli specifici argomenti oggetto dei singoli incontri.

[5] Ad esempio al fine di acquisire certificazioni di conformità a standard internazionali.
[6] Sistema di Gestione di Continuità Operativa basato sullo standard ISO22301.
[7] Sistema di Gestione della Sicurezza delle Informazioni basato sullo standard ISO/IEC 27001.

2. all'interno del Management Meeting: incontri periodici presieduti dall'Amministratore Delegato e a cui partecipano i suoi primi riporti, possono essere inseriti, in funzione delle esigenze di condivisione specifica, temi di security o cyber security. In tali occasioni ai meeting possono essere chiamati a prendere parte anche i referenti più idonei a relazionare sulla specifica materia.

6. Sensibilizzazione e formazione

Riconoscendo nelle persone la più importante risorsa e allo stesso tempo la prima linea di difesa aziendale in termini di security, Snam realizza iniziative di sensibilizzazione e di formazione del personale con l'obiettivo di promuovere la cultura della sicurezza aziendale e favorire la partecipazione attiva e responsabile dei singoli individui.

A tal scopo la Funzione Global Security & Cyber Defence, in accordo con le strutture aziendali preposte, sviluppa negli ambiti di pertinenza e secondo le metodologie didattiche più opportune sia programmi generali rivolti all'intera popolazione aziendale sia programmi rivolti a specifici ambiti operativi, in ciò avvalendosi anche delle soluzioni messe a disposizione dall'innovazione tecnologica.

7. Responsabilità di aggiornamento

La funzione Global Security & Cyber Defence riesamina periodicamente la presente Linea Guida, per assicurarne l'efficacia nel tempo e l'aderenza alle best practice.

Tutte le unità/posizioni aziendali coinvolte nelle attività sopra descritte sono responsabili, per quanto di competenza, di rilevare gli accadimenti aziendali che comportino la necessità di un adeguamento della presente Linea Guida e di segnalarli. La direzione Global Security & Cyber Defence, in collaborazione con la funzione Legale e Organizzazione, assicura il coordinamento delle attività di aggiornamento della stessa.