Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 2

La capacità di rispondere alle domande di chiarimento del top management è il primo passo per avere successo nel presentare efficacemente il rischio di sicurezza delle informazioni. Nella gestione del rischio aziendale, la difficoltà sta nel combinare tra loro dati di natura spesso diversa, e nello stesso tempo, riuscire a fornire un dettaglio esaustivo senza eccedere in particolari di tematiche specialistiche, come discusso in "Comunicare il rischio di sicurezza delle informazioni in modo semplice ed efficace, parte 1". Nel caso della comunicazione aziendale, la perdita o la devianza dal dettaglio specialistico è controbilanciata dal guadagno in chiarezza espositiva. La corretto valutazione delle risorse di sicurezza delle informazioni è un beneficio all'efficacia dell'intero processo di information and communication technology (ICT).

Dalle minacce al rischio aziendale

Molti dei fattori di rischio dei processi ICT agiscono a livello di attività operativa, mentre le decisioni per contrastarli sono prese a livello di vertice aziendale. Questo significa, che dopo aver illustrato al management la gravità delle minacce per ogni processo impattato, rispetto agli obiettivi aziendali, si deve passare ad un livello espositivo di maggior dettaglio per chiarire lo scenario di rischio e descrivere le conseguenze dell'agire o del non agire. Il decisore finale è spesso in una posizione organizzativa che non ha una conoscenza dettagliata delle operazioni specialistiche.

La descrizione del contesto di rischio di ogni risorsa rilevante, è il primo livello di dettaglio richiesto, e sarà focalizzato sull'importanza che riveste per il business e per tutti i processi collegati. Discussioni troppo tecnologiche degli argomenti dovrebbero essere evitate. Una volta esaurita la presentazione dello scenario di rischio, se vengono richiesti dettagli aggiuntivi, si ricorre ad una descrizione organizzativa delle azioni coinvolte, descrivendo i ruoli impattati, le attribuzioni di responsabilità ed i legami con gli altri processi. Questo modo di bilanciare aspetti organizzativi, operativi e riferimenti d'insieme, crea una prospettiva contestuale che agevola la comprensione degli argomenti senza richiedere troppo dettaglio tecnico.

Come esporre il contesto del rischio

L'analisi approfondita dello scenario delle minacce dovrebbe concentrarsi su un singolo rischio alla

Luigi Sbriz, CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL v4, UNI 11697:2017 DPO
È stato il responsabile del monitoraggio dei rischi presso un'azienda multinazionale del settore automotive per oltre sette anni. In precedenza, è stato responsabile della gestione dei servizi e delle risorse ICT nell'area Asia-Pacific (Cina, Giappone e Malesia) e, prima ancora, è stato responsabile della sicurezza delle informazioni a livello mondo per più di sette anni. Per quanto attiene al monitoraggio interno del rischio, ha sviluppato una metodologia originale unendo un'analisi del rischio operativo con una conseguente valutazione del rischio guidata dal livello di maturità dei processi. Inoltre, ha progettato uno strumento di cyber monitoring e un sistema integrato per monitoraggio del rischio, modello di maturità e audit interno. Sbriz è stato anche consulente per sistemi di business intelligence per parecchi anni. Può essere contattato su LinkedIn (*https://it.linkedin.com/in/luigisbriz*) oppure su *http://sbriz.tel*.

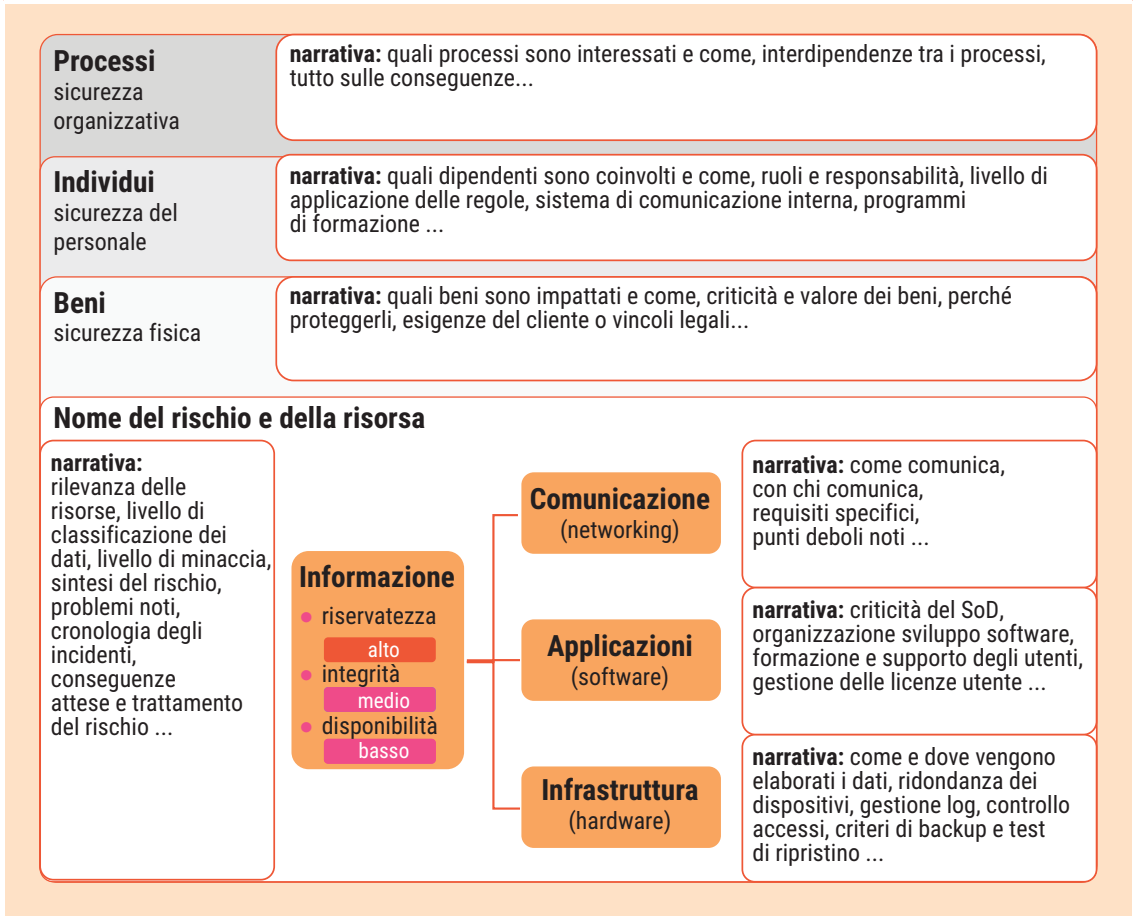
volta e, attraverso un'unica vista d'insieme, dovrebbe collegarsi ai processi coinvolti, alle risorse umane coinvolte ed ai beni utilizzati. Dovrebbe inoltre contenere una descrizione del valore della risorsa da proteggere. Infine, tutte le informazioni riassunte in questo prospetto devono essere presentate in modo comprensibile per l'alta direzione. Il modello per questo prospetto è rappresentato in **figura 1**. Si richiama l'attenzione sul centro del grafico, dove è descritta la risorsa da proteggere.

Un report che esplode le informazioni di rischio per una specifica risorsa può essere pensato composto da due parti: la parte centrale descriverà la risorsa (o gruppo di risorse omogenee) assieme alle ragioni per proteggerla e alle sue criticità implementative, e la parte più esterna, che avvolge quella centrale, descriverà sinteticamente il contesto aziendale che subirà l'impatto delle conseguenze nel caso di mancata applicazione delle misure di trattamento del rischio.

Il contesto aziendale è definito da tre ambiti—processi, individui e beni—ciascuno focalizzato alla descrizione del proprio stato corrente con enfasi sui requisiti, le criticità e la gravità delle conseguenze. Il metodo scelto per presentare queste informazioni è il narrative. I tre narrative del contesto sono sullo stesso piano e vanno presi in considerazione assieme, pertanto, non c'è necessità alcuna di evidenziare un ambito rispetto ad un altro, ad esempio con uso di colori. Di seguito i tre ambiti ed i principali temi che devono essere trattati.

- **Processi**—con focalizzazione sulla sicurezza organizzativa. Il narrative descrive l'importanza delle relazioni inter funzionali tra i processi

Figura 1—Modello per uno scenario di rischio di una risorsa critica



coinvolti e gli eventuali problemi di continuità del business in caso di compromissione di uno di questi. Indica eventuali criticità legate alla qualità del sistema di governo dei processi (insieme delle procedure).

- **Individui**—con focalizzazione sulla sicurezza personale. Il narrative descrive l'importanza delle regole assegnate ed il piano di formazione per diffondere la conoscenza e assicurare il rispetto. Riportare gli eventuali controlli sul rispetto delle regole e lo schema di assegnazione delle responsabilità. Evidenziare criticità sul clima interno o sulla mancanza di competenze o sull'esigenza di aumentare l'organico o sul rischio di perdita di know-how. In generale regole comportamentali per gli ambienti fisici, le dotazioni individuali, le relazioni interpersonali e l'attività sulle piattaforme digitali.
- **Beni**—con focalizzazione sulla sicurezza fisica. Il narrative descrive l'importanza degli asset impiegati a supporto della risorsa da proteggere e le modalità di accesso ed utilizzo. Ad esempio, elencare le misure di controllo per l'accesso fisico, le infrastrutture e attrezzature necessarie, le criticità delle aree fisiche ad accesso limitato e gli scopi del sistema di videosorveglianza. Mettere in evidenza la criticità di eventuali servizi funzionali alla risorsa o alla sua protezione.

La risorsa da proteggere è valutata sul rispetto degli obiettivi di confidenzialità, integrità e disponibilità (terna CIA[1]) ed in funzione dei requisiti funzionali di comunicazione, applicativi e sistemistici. Come risorsa possiamo avere qualunque asset, sia tangibile che intangibile, oppure un gruppo di asset omogenei sotto il profilo del trattamento del rischio.

Il narrative della risorsa serve a evidenziare in modo sintetico la sua importanza, la classificazione del dato, il rischio di fallimento degli obiettivi, le potenziali conseguenze e la proposta di trattamento. La classificazione del dato è espressa tramite la terna CIA utilizzando un colore che evidenzi quando secondo il rischio corrente è atteso uno scostamento dall'obiettivo. Ulteriori informazioni, nel caso sia utile dichiararle, potrebbero essere inserite come se fosse una to do list (ad esempio, uno schematico piano economico per il trattamento del rischio, le clausole rilevanti o un accordo sui livelli di servizio [SLA] dei contratti di outsourcing[2] oppure le regole di escalation della gestione incidenti).

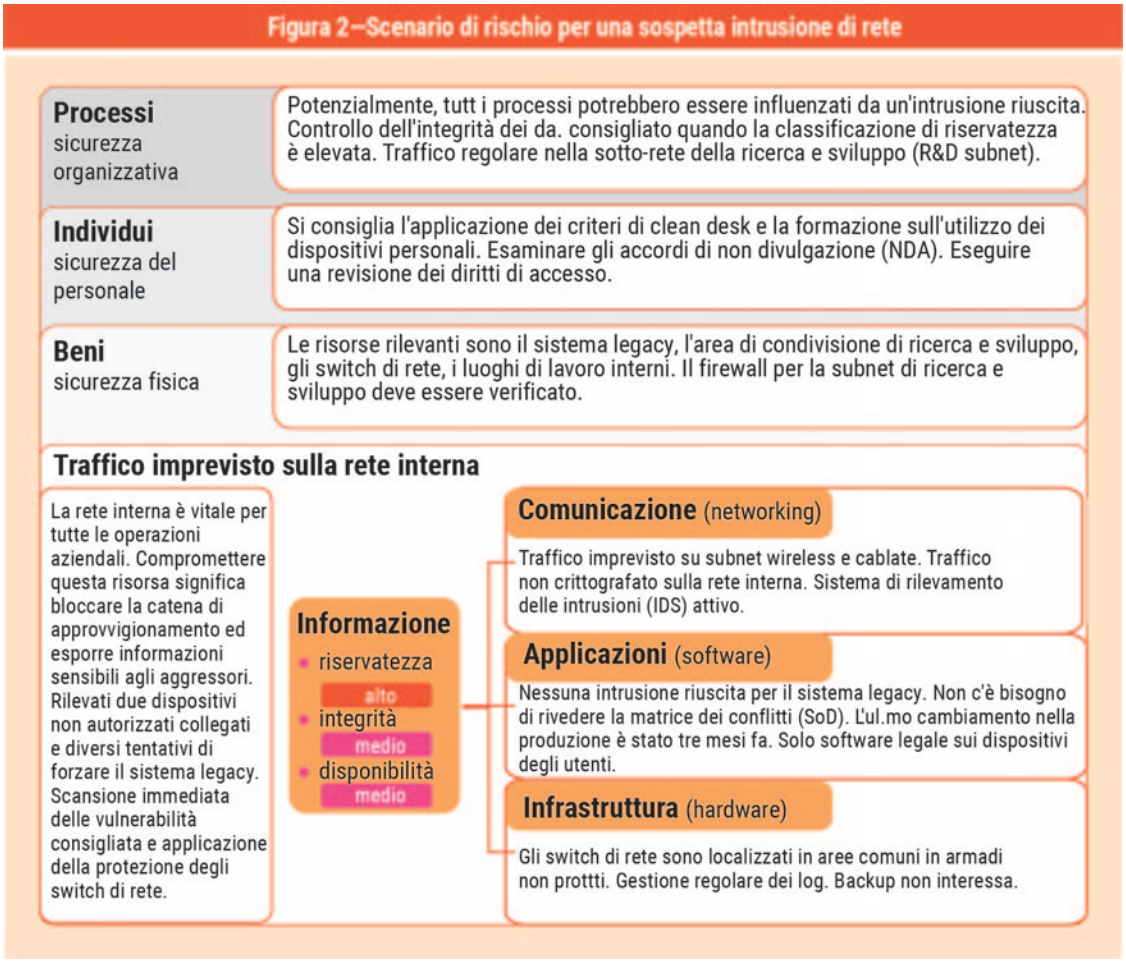
Gli ambiti operativi della risorsa sono ripartiti in tre macro aree. Ciascuna con una propria descrizione sintetica solamente con il fine di descrivere le funzionalità o di evidenziare le criticità. L'area del narrative sarà vuota nel caso non sia pertinente per quella risorsa.

Nell'ambito del processo di comunicazione e di condivisione dati ritroviamo le tematiche tipiche del networking. Gli eventuali temi da trattare sono relativi alla segregazione della rete, all'uso di reti private virtuali (VPN), ai canali crittografati, all'uso di email o chat, al comportamento sui social, al disegno della rete con soluzioni di continuità, all'organizzazione del lavoro remoto, al controllo del traffico di rete, ai metodi di condivisione dati oppure ai criteri di autenticazione in rete.

Nell'ambito delle funzionalità applicative e dello sviluppo ritroviamo il mondo tipico del software, dallo sviluppo alle funzionalità di elaborazione. Si possono esporre i temi più rilevanti riguardanti la decisione di acquisizione o di sviluppo applicativo, le regole della segregation of duty (SoD[3]), la gestione di un change applicativo, la gestione delle licenze d'uso, le regole del patch management, l'amministrazione del database, l'organizzazione del servizio di ticketing utente, il controllo dei sorgenti, l'obsolescenza applicativa e la valutazione delle vulnerabilità.

Nella gestione dell'elaborazione dei dati e dei sistemi di archiviazione dei dati (infrastruttura informatica), sia interni che esterni, ne fanno parte hardware e virtualizzazioni. Le tematiche affrontate in questo ambito riguardano i sistemi di ridondanza per migliorare la resilienza degli apparati, le performance dei sistemi, l'uso di sistemi in cloud o fisici, la protezione verso eventi naturali o di accesso non autorizzato, i metodi di sorveglianza delle aree critiche, la procedura di controllo dei logs, i requisiti ed i test per l'archiviazione storica. L'esempio di compilazione di questa scheda è nella **figura 2**.

Figura 2—Scenario di rischio per una sospetta intrusione di rete



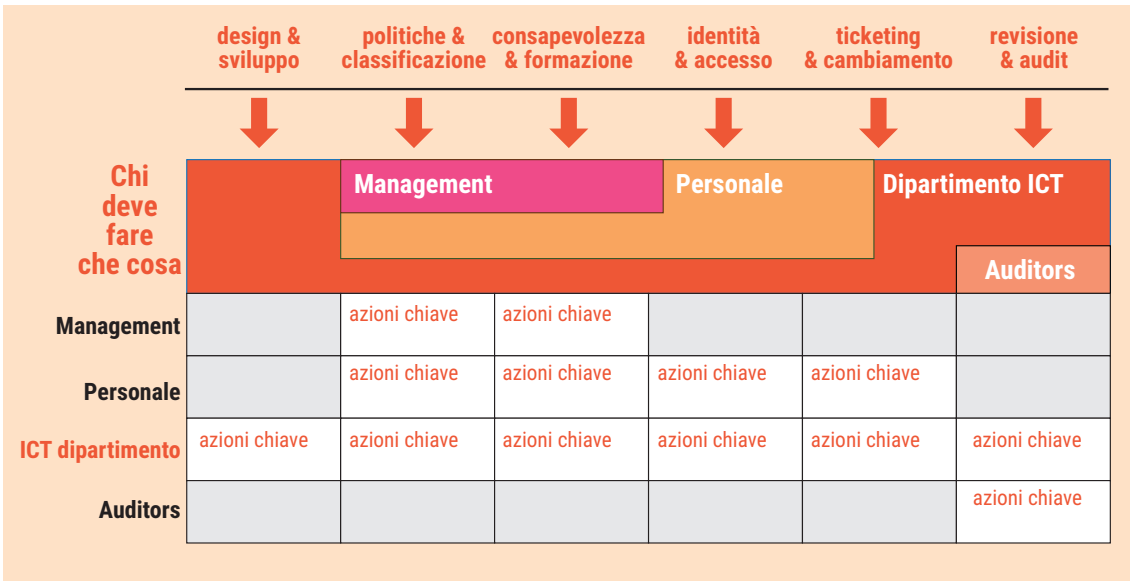
La scrittura dei narrative, come già detto, avrà uno stile volutamente non tecnico. Tutta la scheda avrà un aspetto pulito e ordinato concedendo un po' di colore alla sola classificazione dei dati. Lo scopo è di far riflettere sulle implicazioni delle azioni di contrasto proposte tramite le descrizioni dei temi visti in ottica di interazione tra processi ed attività piuttosto che una narrazione monotematica e tecnica della soluzione. Si bilanciano informazioni organizzative che descrivono i processi aziendali con le attività collegate alla risorsa da proteggere.

Come introdurre l'impatto della soluzione sui processi aziendali

Nel caso sia necessario spingersi verso un differente livello di dettaglio, per comprendere meglio lo scenario organizzazione ed il coinvolgimento delle risorse umane nel partecipare alla soluzione di contrasto al rischio, si può utilizzare un nuovo prospetto. Non si usa assolutamente un diagramma di Gantt[4] perché è prematuro in questa fase dettagliare in modo così spinto un soluzione che forse non verrà attuata. Non è neppure appropriata la classica matrice delle responsabilità RASCI[5] per la stessa ragione—ossia, mancano ancora molti elementi di dettaglio.

E' possibile però ricorrere ad una specie di matrice, pur simile alla RASCI ma rivista per macro responsabilità e sotto processi (**figura 3**), e con qualche elemento decorativo per enfatizzare le attività più critiche. In questa fase non dobbiamo dimostrare la fattibilità oppure i benefici ma solo far comprendere il livello di coinvolgimento di alcuni ruoli organizzativi per avere un'idea di come e

Figura 3—Modello per attività e responsabilità dei sottoprocessi ICT

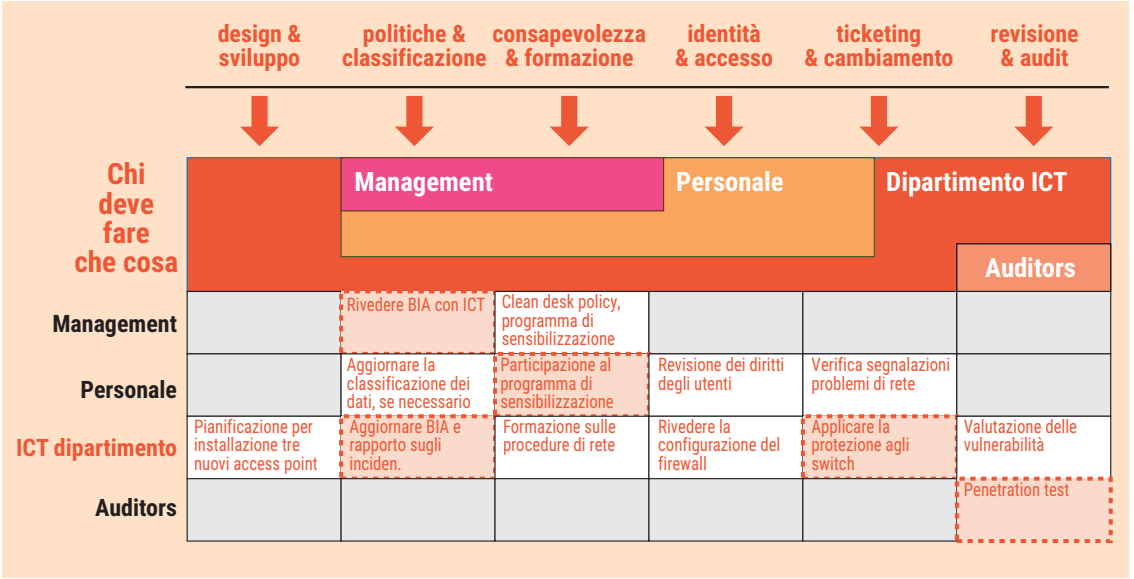


quanto sono impegnati nello svolgimento dei sotto processi. Il grado di dettaglio è basso ma si focalizza sulle correlazioni e sull'impegno necessario. La lettura avviene per colonne, dall'alto verso il basso, ciascuna dedicata ad un sotto processo ed attraversando i colori si rappresentano i ruoli e con le attività chiave in basso, si richiama la severità del compito.

Nella zona inferiore del prospetto c'è in estrema sintesi l'insieme dei compiti primari per ruolo con l'indicazione di quelli più critici alla riuscita dell'azione di trattamento del rischio.

- **Management**—Il ruolo manager è coinvolto per fornire gli indirizzi attuativi alle proprie risorse, anche migliorando i processi formativi o modificando gli aspetti organizzativi. Inoltre, hanno il compito di controllo sul rispetto delle norme assegnate e di misurare le performance dei processi.
- **Personale**—Il ruolo personale include tutte le risorse umane dedicate ai compiti assegnati per attuare il contrasto alle minacce. Deve operare nell'ambito delle istruzioni operative ricevute, mantenere un livello di competenza adeguato allo svolgimento delle proprie mansioni ed operare nel rispetto della separazione dei compiti (SoD), per questo le attività devono essere tracciabili. Nel caso il personale rilevi problemi o possibilità di miglioramento deve essere parte attiva segnalando i problemi (tramite apertura ticket).
- **ICT**—Il ruolo ICT è attribuito al fornitore dei servizi di gestione delle informazioni. Se interno, generalmente non si stabilisce un formale SLA ma tramite le policies ed un set di procedure interne, si definisce sia la modalità attuativa del servizio che quella di controllo del livello di erogazione dello stesso. Ha la gestione esclusiva di tutte le fasi dalla progettazione al rilascio delle soluzioni, attua un monitoraggio continuo di tutte le attività, misura le prestazioni e interviene in supporto agli utenti o in modifica di applicativi o dell'infrastruttura, quando necessario.
- **Auditor**—Il ruolo auditor interviene nella fase di auditing, quando è richiesto un parere indipendente per garantire il rispetto delle regole. Può essere coinvolto personale di auditing interno od esterno ma questa differenza va specificata. Un auditor interno potrebbe essere usato per l'attività istituzionale programmata, mentre l'auditor esterno, a costo presumibilmente superiore ma con tutte le specializzazioni possibili, si ingaggia solo su specifiche esigenze estemporanee.

Figura 4—Esempio di attività e responsabilità dei sottoprocessi ICT



Nell'area dei compiti (key actions), questi sono riassunti sinteticamente in brevi elenchi e servono a fornire il corretto posizionamento delle attività rispetto ai centri di responsabilità. Un esempio di un prospetto compilato con l'indicazione di attività critiche è riportato in **figura 4**.

Il risultato finale è una mappa di azioni, localizzate dalle coordinate del sotto processo e della responsabilità. Aiuta il top management a comprendere meglio l'estensione dello sforzo necessario ad implementare l'intero processo. È un'alternativa all'uso delle classiche tabelle per presentare i contenuti, enfatizzando i fattori organizzativi critici senza l'uso dei numeri.

Conclusioni

Con i modelli presentati, è possibile attirare l'attenzione su quegli eventi con un alto livello di rischio. Per coinvolgere pienamente il top management nelle azioni da intraprendere, è necessario utilizzare delle modalità che si focalizzino sui temi più strettamente legati al contesto organizzativo. Introducendo una prospettiva diversa, è possibile mettere a fuoco concetti che altrimenti non sarebbero comunicati in modo chiaro.

Le diverse sfere di competenza e sensibilità, e le diverse prospettive di esperti di processo e top manager, rendono necessario trovare un terreno comune per migliorare la comunicazione, massimizzare la comprensione delle questioni rilevanti e consentire un processo decisionale veramente informato. Quando si comprende il livello di rischio, è più facile sviluppare soluzioni efficaci.

Per la presentazione completa dei risultati del rischio di sicurezza delle informazioni al top management, è stato proposto un processo in tre fasi: comprendere lo scenario delle minacce di sicurezza informatica, descrivere gli eventi di rischio di specifiche risorse critiche, ed infine, definire la relazione tra attività e responsabilità nel trattamento del rischio. L'obiettivo subito ricercato è la comunicazione semplice e non tecnica per quanto possibile. Il contesto tecnico della soluzione rimane all'interno di una scatola nera, dove le minacce nel contesto operativo in input, si trasformano in output nel livello di protezione atteso, enfatizzando solo le interazioni tra i processi, non i dettagli tecnici delle soluzioni.

La comunicazione è efficace solo se tutte le parti interessate comprendono il problema. L'aspettativa è una scelta consapevole, sempre orientata agli obiettivi di business. Gli strumenti da usare nella

comunicazione possono essere non convenzionali ma ciò non implica un abbandonano degli standard metodologici. Questi standard sono semplicemente arricchiti con componenti che si adattano alle esigenze di ciascuna organizzazione.

Riferimenti

1 ISACA®, "Communicating Information Security Risk Simply and Effectively, Part 1," *ISACA® Journal*, vol. 6 2021, *https://www.isaca.org/archives*
2 ISACA, "Information Security," ISACA Glossary, *https://www.isaca.org/resources/glossary*
3 ISACA, "Service Level Agreement (SLA)," ISACA Glossary, *https://www.isaca.org/resources/glossary*
4 ISACA, *CISA Review Manual, 26th Edition*, USA, 2015, *https://www.isaca.org/resources*
5 Weaver, P.; "Henry L. Gantt, 1861–1919: A Retrospective View of His Work," Mosaic Projects, 2012, *https://www.mosaicprojects.com.au/PDF_Papers/P158_Henry_L_Gantt.pdf*
6 Baker, D. A.; *Multi-Company Project Management: Maximizing Business Results Through Strategic Collaboration*, J. Ross Publishing, USA, 2009