RISK ASSESSMENT

LA CHIAVE PER UNA GESTIONE AZIENDALE SICURA ED EFFICIENTE

LUCA TRICARICO
L-31 | UNIPEGASO | 2025

Introduzione

Gestione del Rischio Aziendale Oggi: *Un Imperativo Strategico!*

Nel contesto economico e tecnologico attuale, le aziende affrontano una crescente complessità di rischi, che spaziano dalla sicurezza informatica alle crisi finanziarie, fino alle sfide normative e ambientali. La **gestione del rischio aziendale** non è più solo una misura di protezione, ma un elemento strategico per garantire continuità operativa, competitività e crescita sostenibile.

Adottare un approccio proattivo nella gestione dei rischi consente alle imprese di **prevenire minacce, minimizzare perdite e cogliere opportunità**, trasformando l'incertezza in un vantaggio competitivo. Oggi, più che mai, il Risk Management è un pilastro fondamentale per il successo aziendale.

Oggi sempre più aziende stanno ricorrendo a **sistemi evoluti di *Risk Assessment*** per tutelare il proprio business.

L'aumento esponenziale delle **violazioni dei dati e della sicurezza** nelle imprese, l'inasprirsi dei **provvedimenti di legge** e dei regolamenti di settore, lo **sviluppo del panorama dell'IoT** e l'affermazione delle **piattaforme di risk management** nei principali istituti finanziari hanno permesso alle imprese di osservare la disciplina del rischio da una nuova prospettiva e di considerarla come un fattore imprescindibile a livello aziendale. Si calcola che il valore del mercato globale dei sistemi dedicati alla gestione del rischio, dovrebbe raggiungere i 18,50 miliardi entro il 2026, con una crescita media annuale del 14,6% (Rapporto Allied Market Research).

Che cos'è il Risk Assessment?

Il ***Risk Assessment*** è il processo di identificazione, analisi e valutazione dei rischi che possono influenzare un'azienda.

L'obiettivo è determinare il livello di pericolo associato a determinate attività o situazioni ed adottare misure preventive al fine di ridurre o eliminare i rischi; l'identificazione dei pericoli che potrebbero avere un impatto negativo sulla capacità di un'organizzazione produrre il proprio business.

Queste valutazioni aiutano a identificare i rischi aziendali reali e forniscono misure, processi e controlli per ridurre l'impatto di queste minacce sulle operazioni aziendali. Più precisamente, la valutazione del rischio identifica e analizza potenziali eventi (futuri) che possono avere un impatto negativo sugli individui, sui beni e/o sull'ambiente (ad esempio analisi dei pericoli). Esprime inoltre giudizi "sulla tollerabilità del rischio sulla base di un'analisi del rischio" tenendo conto dei fattori influenti (ad esempio valutazione del rischio).

Le aziende possono utilizzare un frame work di valutazione del rischio per stabilire le priorità e condividere i dettagli della valutazione, inclusi eventuali rischi per la propria infrastruttura informatica (IT). Nelle grandi imprese, il processo di valutazione del rischio viene solitamente condotto dal Chief Risk Officer/Manager il quale si occupa dello studio e dell'attuazione delle fasi del processo di risk management.

Le Fasi del Risk Assessment

Stabilire
- Stabilire il contesto in cui l'azienda opera

Identificare
- individuazione delle minacce potenziali (es. rischi finanziati, informatici, ambientali, operativi)

Valutare ed Analizzare
- Analisi della probabilità e dell'impatto di ciascun rischio

Definire
- Sviluppo di strategie per ridurre o eliminare i rischi

Monitorare e Revisionare
- revisione periodica per adattarsi a nuovi scenari e cambiamenti normativi

*link esempio Template da compilare in formato word, redatto da Leonardo S.p.a.
Template per Risk Management Plan

Vediamo adesso le vari fasi della valutazione del rischio:

Definizione del Contesto Aziendale

La Prima fase è La definizione del processo di gestione del rischio stabilisce i criteri in base ai quali i rischi saranno valutati.

L'ambito dovrebbe essere determinato nel contesto degli obiettivi organizzativi dell'azienda. I rischi sono incertezze che influenzano il raggiungimento degli obiettivi aziendali, pertanto non è possibile identificarli completamente se tali obiettivi e strategie non sono chiari.

La selezione degli obiettivi chiave all'interno dell'azienda dovrebbe essere guidata da una valutazione dei fattori esterni e interni che potrebbero avere un impatto attuale sull'azienda. Un'analisi del contesto esterno e interno all'inizio della pianificazione della valutazione del rischio aiuta a identificare i processi che potrebbero essere soggetti a rischi maggiori e, in quanto tali, trarrebbero il massimo valore dalla valutazione del rischio.

I rischi possono sorgere a causa di influenze esterne o interne:

- I rischi esterni sono esposizioni derivanti da condizioni ambientali sulle quali l'azienda solitamente non può avere influenza, come l'ambiente normativo e le condizioni di mercato.
- I rischi interni sono esposizioni derivanti dal processo decisionale e dall'utilizzo di risorse interne ed esterne, tra cui le operazioni dell'azienda e i suoi obiettivi.

L'Identificazione dei Rischi

La Seconda fase è L'identificazione dei rischi, un processo fondamentale volto a individuare e valutare le possibili minacce che potrebbero compromettere il raggiungimento degli obiettivi aziendali e si identificano in 4 diversi tipi:

1. Rischi finanziari: Questi riguardano la possibilità di perdite economiche come:

- **Insolvenze dei clienti:** quando i clienti non riescono a saldare i propri debiti, causando problemi di liquidità all'azienda.
- **Variazioni nei tassi di cambio:** fluttuazioni valutarie che possono influenzare negativamente le transazioni internazionali.
- **Costi imprevisti:** spese non pianificate che possono emergere e incidere sul budget aziendale.

2. Rischi operativi: Questi sono legati a problematiche interne che possono ostacolare le attività quotidiane:

- **Ritardi nelle consegne:** problemi logistici che impediscono la tempestiva distribuzione dei prodotti.
- **Problemi di approvvigionamento:** difficoltà nell'ottenere materie prime e/o componenti essenziali.
- **Guasti ai macchinari:** malfunzionamenti o rotture delle attrezzature che interrompono la produzione.

3. Rischi informatici: Questi riguardano minacce alla sicurezza dei sistemi IT:

- **Attacchi informatici:** tentativi esterni di compromettere la rete aziendale.
- **Malware:** software dannoso progettato per infiltrarsi e danneggiare i sistemi.
- **Errori umani:** azioni involontarie dei dipendenti che possono esporre l'azienda a vulnerabilità.

4. Rischi ambientali: Questi sono associati all'impatto ambientale delle attività aziendali come:

- **Emissioni atmosferiche:** rilascio di sostanze inquinanti nell'aria.
- **Gestione dei rifiuti:** smaltimento inadeguato dei residui di produzione
- **Utilizzo delle risorse naturali:** sfruttamento eccessivo e/o non sostenibile di materie prime.

La Valutazione del Rischio

La seconda fase è la valutazione del rischio è un processo fondamentale che permette di analizzare la **probabilità** e l'**impatto** di ciascun rischio identificato, questo aiuta a stabilire le priorità e a implementare misure di mitigazione adeguate.

Componenti della Valutazione del Rischio

La valutazione del rischio si basa su due elementi chiave:

- **Likelihood**: la possibilità che un determinato evento negativo si verifichi.
- **Impact**: il livello di danno o perdita che il rischio potrebbe causare

Metodi di Analisi del Rischio

Esistono diversi approcci per valutare il rischio l'analisi Qualitativa e quntitativa:

Analisi Qualitativa

Utile per una prima valutazione veloce, classifica i rischi in categorie generali come:

- **Basso**: impatto minimo, facilmente gestibile.
- **Medio**: impatto moderato, richiede azioni di mitigazione.
- **Alto**: impatto grave, necessita di interventi immediati.

Tecniche e metodi comuni utilizzati:

Matrice del rischio (Risk Matrix): rappresentazione grafica della probabilità e dell'impatto.

Sessioni di brainstorming: una tecnica creativa in cui un gruppo di persone interagisce per suggerire idee spontaneamente in risposta a uno stimolo.

Tecnica Delphi : Il fine principale della tecnica Delphi consiste nel produrre idee creative e attendibili o individuare e rielaborare informazioni utili per affrontare un certo problema.
EASW (European Awareness Scenario Workshop): una metodologia utile a elaborare prospettive e sviluppi, quindi utile per progettare il futuro attraverso scenari alternativi.

Analisi Quantitativa: *Calcola i possibili danni finanziari*

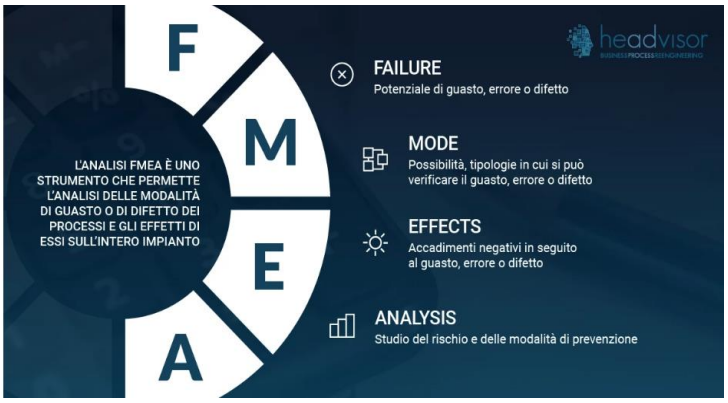
- **Formula del Rischio**:
  Rischio = Probabilità `× Impatto Rischio = Probabilità \ Tempo
  Impatto Rischio = Probabilità `× Impatto

Alcuni esempi comuni di Tecniche utilizzate:

. **Analisi Monte Carlo**

. **Valore atteso delle perdite**

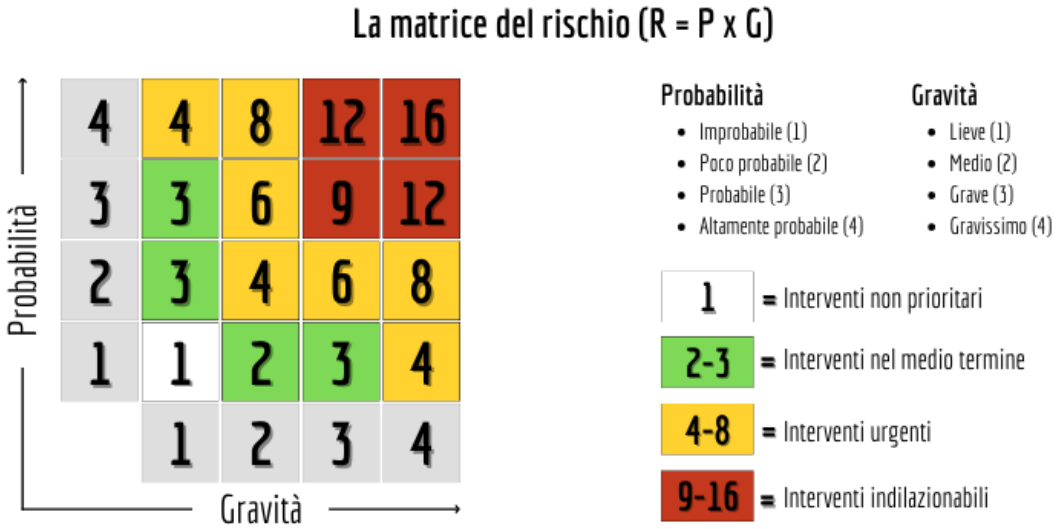
. **FMEA** (Failure Mode and Effects Analysis)



https://www.headvisor.it/sites/default/files/images/analisi-fmea-per-il-risk-management-headvisor.webp

Matrice di Valutazione del Rischio

Lo strumento analitico attualmente più diffuso per generare e **quantificare il rischio** residuo e stabilire una priorità rispetto al piano di adeguamento è la **matrice di rischio**, che incrocia la probabilità e l'impatto per determinare la gravità del rischio.



Risk Treatment

La quarta fase del processo è la Gestione del rischio, un insieme di strategie come valutare, prendere decisioni e pianificare tutte le attività necessarie per ridurre al minimo l'impatto negativo della variabilità sugli obiettivi aziendali e una serie di azioni per mitigarlo.

Che cos'è un piano di trattamento del rischio?
Un piano di trattamento del rischio è una parte essenziale del tuo programma di sicurezza informatica. È un piano completo per implementare controlli per ridurre la probabilità o l'impatto dei rischi. L'implementazione è la componente critica di un piano di trattamento del rischio. Un piano di trattamento del rischio è progettato per aiutare a garantire che i processi di trattamento del rischio siano effettivamente in atto.

Sviluppare un piano di trattamento del rischio
Determinare il livello di piani di trattamento richiesti per ciascun livello di rischio. Ad esempio, per i rischi classificati come "alti", è necessario sviluppare un piano di trattamento. Tuttavia, per i rischi classificati come "bassi e molto bassi" che presentano opportunità di miglioramento, lo sviluppo di un piano di trattamento può essere a discrezione del partner o dei partner. Un trattamento efficace del rischio si basa sull'impegno a raggiungere obiettivi realistici e tempi di attuazione precisi.

Per ogni rischio identificato, occorre specificare questi quattro punti:

1. **Specificare l'opzione di trattamento selezionata**:
   evitare, ridurre, condividere/trasferire o accettare.
2. **Documentare il piano di trattamento**: delineare l'approccio da utilizzare per trattare il rischio. È necessario evidenziare anche eventuali relazioni o interdipendenze con altri rischi.
3. **Assegnare un responsabile**, che sia responsabile del monitoraggio e della rendicontazione dei progressi nell'implementazione del piano di trattamento.
4. **Specificare una data di risoluzione target**: laddove i trattamenti del rischio prevedano tempi lunghi, valutare l'adozione di misure provvisorie.

Con la crescente complessità dei sistemi organizzativi e l'interconnessione dei processi aziendali, La giusta combinazione di un sistema di gestione del rischio è quella basato sull' integrazione dei sistemi 'ISO con le disposizioni del GDPR consente di affrontare questa complessità attraverso un monitoraggio continuo e l'adozione di misure preventive, come la crittografia o la pseudonimizzazione.

Per capire meglio diamo uno sguardo nello specifico alle seguenti **normative e regolamenti** come il **GDPR**, l'**ISO/IEC 27001** e la **Direttiva NIS2**:

GDPR General Data Protection Regulation
NIS2 Network and Information Systems Directive 2
ISO Organizzazione Internazionale per la Normazione

Il **GDPR** è il regolamento dell'Unione Europea (UE) che disciplina la protezione dei dati personali delle persone fisiche. È entrato in vigore il 25 maggio 2018 e ha un impatto globale, poiché si applica a tutte le aziende che trattano i dati di cittadini UE, indipendentemente dalla loro ubicazione.

Obiettivi principali:

- **Protezione della privacy**: Garantire che i dati personali siano trattati in modo sicuro e con il consenso esplicito della persona.
- **Rendere trasparente il trattamento dei dati**: Le aziende devono informare gli utenti su come i loro dati vengono raccolti, utilizzati, conservati e protetti.
- **Controllo degli utenti sui propri dati**: Gli utenti hanno il diritto di accedere, correggere, cancellare e limitare il trattamento dei propri dati personali. Hanno anche il diritto alla **portabilità dei dati**.
- **Notifica delle violazioni**: Le aziende devono notificare alle autorità competenti e agli utenti eventuali violazioni di sicurezza entro 72 ore.

Principali aspetti del GDPR:

- **Privacy by Design and by Default**: Le misure di protezione dei dati devono essere integrate nei processi aziendali fin dalla progettazione dei sistemi.
- **Consenso esplicito**: Le aziende devono ottenere un consenso chiaro e specifico per il trattamento dei dati personali.
- **Data Protection Officer (DPO)**: In alcune circostanze, le aziende devono nominare un Responsabile della Protezione dei Dati, che supervisioni la gestione dei dati personali.
- **Sanzioni**: Le violazioni del GDPR possono comportare multe che arrivano fino al 4% del fatturato annuo globale di un'azienda o a 20 milioni di euro (quello che è maggiore).

La **Direttiva NIS2** è una direttiva dell'Unione Europea che si concentra sulla **sicurezza delle reti e dei sistemi informativi**. È la versione aggiornata della precedente direttiva NIS (2016/1148) e ha come obiettivo quello di migliorare la resilienza e la sicurezza delle infrastrutture critiche in tutta l'UE.

Obiettivi principali:

- **Aumento della resilienza e della sicurezza delle reti e dei sistemi informativi**: NIS2 mira a garantire che i settori critici, come l'energia, i trasporti, la salute e la finanza, siano protetti contro le minacce informatiche.
- **Miglioramento della cooperazione tra i paesi membri dell'UE**: La direttiva promuove una maggiore cooperazione tra le autorità nazionali e le organizzazioni, per scambiare informazioni e rispondere rapidamente agli incidenti informatici.
- **Obblighi di reporting e notifica degli incidenti**: Le organizzazioni sono tenute a segnalare gli incidenti di sicurezza che abbiano un impatto significativo sui servizi forniti.

Principali aspetti della NIS2:

- **Ambito di applicazione ampliato**: La direttiva NIS2 si applica non solo alle aziende operanti nei settori critici, ma anche ad altre **entità essenziali** che dipendono da sistemi informatici, come i fornitori di servizi digitali, piattaforme cloud e piattaforme di e-commerce.
- **Gestione dei rischi**: Le organizzazioni devono adottare misure adeguate di gestione del rischio, come la protezione dei dati e la gestione delle vulnerabilità.
- **Piani di risposta agli incidenti**: Le organizzazioni devono avere piani operativi per rispondere rapidamente agli incidenti di sicurezza, ridurre l'impatto e informare le autorità competenti.
- **Ampliamento della vigilanza e delle sanzioni**: Gli Stati membri sono obbligati ad adottare politiche di vigilanza più rigorose e sanzioni per non conformità, comprese multe o azioni legali contro le organizzazioni che non rispettano la direttiva.

ISO/IEC 27001 è uno standard internazionale per la gestione della sicurezza delle informazioni. È utilizzato per proteggere la confidenzialità, l'integrità e la disponibilità delle informazioni all'interno di un'organizzazione, attraverso l'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni (**ISMS** - Information Security Management System).

Obiettivi principali:

- **Gestione del rischio**: Identificare e ridurre i rischi associati alla sicurezza delle informazioni, inclusi minacce interne ed esterne.
- **Protezione delle informazioni**: Implementare politiche, procedure e controlli per garantire la sicurezza dei dati e delle informazioni aziendali.
- **Continuità aziendale**: Assicurare che l'azienda possa continuare a operare anche in caso di incidenti o attacchi informatici.

Principali aspetti dell'ISO/IEC 27001:

- **Politiche di sicurezza delle informazioni**: Creare politiche che definiscano le pratiche di sicurezza, la gestione dei rischi e la protezione delle informazioni.
- **Valutazione del rischio**: Identificare le vulnerabilità e le minacce, quindi adottare misure di controllo per mitigare i rischi.
- **Controlli di sicurezza**: Implementare controlli tecnici e operativi per proteggere le informazioni. Questi possono includere la crittografia, l'accesso controllato ai dati, il backup dei dati e la gestione delle vulnerabilità.
- **Audit e miglioramento continuo**: L'organizzazione deve monitorare e riesaminare regolarmente il proprio sistema ISMS per garantire che rimanga efficace e risponda alle esigenze di sicurezza.

Certificazione ISO/IEC 27001:

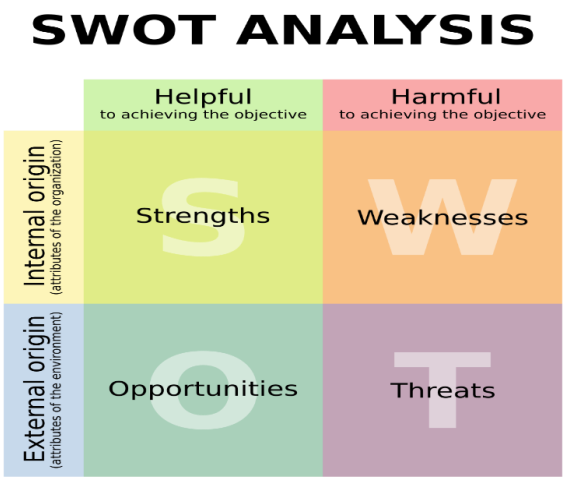
- La certificazione è volontaria, ma molte aziende scelgono di certificarsi per dimostrare ai clienti, partner e autorità di essere conformi alle migliori pratiche internazionali di gestione della sicurezza delle informazioni.
- Un'organizzazione certificata ISO/IEC 27001 dimostra il proprio impegno nella protezione delle informazioni sensibili e può ottenere vantaggi competitivi nel mercato.

Queste normative e regolamenti sono cruciali per le aziende digitali che operano in un ambiente complesso e interconnesso, poiché stabiliscono le fondamenta legali e operative per garantire la sicurezza, la protezione dei dati e la resilienza informatica.

Metodologie per l'identificazione dei rischi:

La quinta fase è la metodologia per individuare il rischio; per individuare efficacemente le minacce potenziali, le aziende possono adottare diverse tecniche, tra cui:

- **Analisi dei processi aziendali:**
  esaminare le attività operative per identificare punti critici.
- **Brainstorming con i dipendenti:**
  coinvolgere il personale per raccogliere percezioni e intuizioni sui rischi.
- **Revisione delle normative e dei requisiti legali:**
  assicurarsi che l'azienda sia conforme alle leggi vigenti per evitare sanzioni.
- **Utilizzo di check-list e strumenti di valutazione standardizzati:**
  applicare strumenti riconosciuti per una valutazione sistematica dei rischi.
- **La Matrice Swot** con la quale individuare punti di forza, punti di debolezza, nonché le opportunità o le minacce.



L'adozione di un approccio strutturato e proattivo nell'identificazione dei rischi consente alle organizzazioni di sviluppare strategie di mitigazione efficaci, migliorando la resilienza e garantendo una maggiore sicurezza operativa. Quindi Sarà importante avere o costruire delle policy o delle procedure aziendali che aiutino a definire le linee guida per la gestione dei rischi, affinché i processi, e i progetti o le singole attività, diventino parte integrante dell'organizzazione e quindi permettano di individuare e gestire tutti i rischi ed opportunità, che possono derivare da eventi interni o esterni rispetto al contesto in cui si trova a dover operare l'azienda. In questa fase sarà fondamentale la scelta delle risorse coinvolte (ruoli e responsabilità delle persone nei confronti dei rischi), gli strumenti e software da utilizzare per l'analisi dei rischi, le scale per misurarli, le tempistiche di monitoraggio con eventualmente le azioni di mitigazione da attuare.

L'importanza di una Consulenza nella Strategia Aziendale

E qui entra in gioco l'esperienza e la guida di esperti, ad oggi sono molte le aziende che offrono questi servizi, Il **Risk Assessment** è un elemento cruciale nella gestione strategica di un'azienda, affidarsi a una **consulenza specializzata** può fare la differenza tra una gestione del rischio efficace e una vulnerabilità operativa.

link per aziende di consulenza: Dogma.it - KPMG - DataGuard

Perché una consulenza è fondamentale nel Risk Assessment?

1.Competenza specialistica
Una società di consulenza porta **esperienza e metodologie consolidate**, aiutando l'azienda a individuare rischi nascosti e valutare scenari complessi.

2.Approccio oggettivo e analisi dettagliata
Un consulente esterno offre un **punto di vista neutrale** e basato su dati concreti, evitando distorsioni interne con un'analisi approfondita dei pericoli.

3.Personalizzazione della strategia di gestione del rischio
Ogni azienda ha esigenze uniche: una consulenza esperta permette di **adattare il Risk Assessment** al settore specifico e alle dimensioni dell'impresa, ottimizzando le risorse.

4.Conformità normativa e riduzione delle sanzioni
Il mancato rispetto delle normative può comportare **gravi sanzioni e danni alla reputazione**. I consulenti aiutano a garantire che l'azienda sia in linea con leggi e regolamenti in materia di sicurezza, ambiente e governance.

5.Miglioramento della continuità operativa
Una corretta valutazione dei rischi, supportata da consulenti esperti, consente di **prevenire interruzioni e crisi**, garantendo la resilienza aziendale e la competitività nel mercato.

6.Ottimizzazione delle risorse finanziarie
Identificare e mitigare i rischi in anticipo permette di **evitare perdite economiche**, costi imprevisti e investire in modo più efficiente nella sicurezza e nello sviluppo aziendali.

Uno Sguardo al Cyber Risk

Si dice **Cyber Risk** (o Rischio informatico) "*qualsiasi rischio di perdita finanziaria, distruzione o anche solo semplicemente un danno alla reputazione di un brand, azienda o realtà commerciale che sia da imputare a un malfunzionamento del sistema informatico*" (parole dell'Istitute of Risk Management). In altre parole, il Cyber Risk è il rischio più che comune di incorrere in ingenti perdite economiche a causa del verificarsi di alcuni eventi dannosi, siano essi accidentali o vere e proprie azioni dolose mirate a danneggiate il sistema informatico di un'azienda (hardware, software, banche dati, etc.).

Perché il Cyber Risk è un pericolo che non interessa solo le grandi aziende?

I media si riempiono ogni giorno di news che raccontano di attacchi informatici, sia per mano umana (hacker) che per mezzo di malware (tra cui i ransomware), e delle loro conseguenze. Non è un caso che gli attacchi di Cyber Crime siano al settimo posto nella classifica del World Economic Forum (WEF), che oltre a tenerne il conto ne valuta anche la gravità degli impatti sulla vita economico/finanziaria delle vittime. Non serve essere i titolari di grandi aziende per aver vissuto un episodio di Cyber Crime, come potrebbe essere, per fare un esempio, un profilo hackerato. Il Cyber Risk rappresenta uno dei pericoli più grandi per tutte le attività commerciali e non solo; grandi o piccole che siano.

Che cos'è un Rischio IT?

Il Cyber Risk, più nel dettaglio, si può manifestare in due modi principali: in primo luogo si potrebbe trattare di un RISCHIO IT, che consiste in tutte le conseguenze che derivano da danni accidentali ai sistemi informatici. Si pensi al caso di un incendio, un corto circuito, o perché no, anche a una decisione sbagliata o a un'imprecisione del tecnico informatico di riferimento, o alla più banale delle occorrenze, nel caso dovesse saltare la corrente. In questo caso, per quanto alto, il *rischio* non si traduce in un *crimine*.

Che cos'è un Cyber Crime?

Diverso è il caso in cui si verifichi un vero e proprio CYBER CRIME (reato informatico), che consiste in tutti i rischi connessi alle vere e proprie attività criminali messe in atto ai danni della vittima (che si tratti di una piccola così come di una grande azienda, ma anche di un semplice utente) per mano di un soggetto terzo. Si tratta di tutti quei fenomeni criminali legati alla pirateria informatica di cui molto spesso non si capisce nemmeno il nome: frodi informatiche, danni a dati, programmi e archivi, intercettazioni non autorizzate, fino alla riproduzione non autorizzata di programmi e documenti protetti, diversi tipi di operazioni messe in atto dalla figura di un cyber-criminale, di solito un hacker o pirata informatico.

L'importanza della Cyber Insurance

Che sia un errore umano *come una svista da parte di un dipendente che aprendo una mail infettata lascia entrare nel sistema un Virus o un Malware*, un evento accidentale o un vero e proprio attacco informatico (Malware, Ransomware, Phishing, Attacchi DoS o DDos, Spam), il succo non cambia Per far fronte alla minaccia crescente di danni al sistema informatico (e a tutte le conseguenze sul breve medio e lungo termine), negli ultimi anni sono nate diverse polizze assicurative dette "Cyber Insurance" o polizze Cyber Risk.

Conclusione

*In conclusione un efficace integrazione del **Risk Assessment** aiuta le aziende a:*

✓ *Prevenire incidenti e perdite economiche.*

✓ *Garantire conformità alle normative vigenti.*

✓ *Migliorare la sicurezza e la resilienza aziendale.*

✓ *Ottimizzare la gestione delle risorse aziendali.*

*"Sperare di non incorrere in un attacco informatico, al giorno d'oggi, è un po' come fare un tuffo nel mare e pensare di non bagnarsi". Allo stesso tempo è vero che, in tema di tecnologia digitale, **la sicurezza al 100% non esiste.*** lokky.it/blog

*Integrare un programma di valutazione **Risk Assessment** nella strategia aziendale con il supporto di una consulenza specializzata non è solo una scelta prudente, ma un investimento strategico per il futuro dell'impresa.*

*Una gestione efficace dei rischi migliora la **sicurezza, la conformità e la sostenibilità aziendale**, contribuendo alla crescita e alla stabilità sia strutturale che economica nel lungo periodo.*