Economia Aziendale Online

Business and Management Sciences
International Quarterly Review

Cybersecurity e gestione del rischio informatico nella governance aziendale: evidenze dalla letteratura e strumenti operativi

Vincenza Vota

Pavia, September 30, 2025
Volume 16 – N. 3/2025

DOI: 10.13132/2038-5498/16.3.1031-1054

www.ea2000.it
www.economiaaziendale.it

PaviaUniversityPress

Electronic ISSN 2038-5498
Reg. Trib. Pavia n. 685/2007 R.S.P.

Cybersecurity e gestione del rischio informatico nella governance aziendale: evidenze dalla letteratura e strumenti operativi

Vincenza Vota
Phd in Management, Finance and Accounting
Department of Economics, University of Insubria, Varese. Italy.

Corresponding Author:

Vincenza Vota

vincenza.vota@uninsubria.it

Cite as:

Vota, V. (2025). Cybersecurity e gestione del rischio informatico nella governance aziendale: evidenze dalla letteratura e strumenti operativi. E*conomia Aziendale Online*, *16*(3), 1031-1054.

Section:

Refereed Paper

ABSTRACT

In un contesto economico sempre più digitalizzato e interconnesso, la gestione del rischio informatico rappresenta una leva strategica fondamentale per la competitività delle imprese. Il presente contributo, infatti, analizza l'integrazione strutturale della cybersecurity nei sistemi di controllo di gestione e nella governance aziendale valorizzando l'approccio proattivo della gestione delle performance basata sul rischio (risk-based performance management) e il paradigma della *cybersecurity by design*. Particolare attenzione è dedicata al ruolo dell'Enterprise Risk Management (ERM) come cornice concettuale per una gestione integrata e trasversale dei rischi digitali. L'analisi si concentra sui principali modelli normativi (GDPR, NIS2, DORA, ISO/IEC 27001) e sugli strumenti tecnico-economici, tra cui le coperture assicurative, che consentono la prevenzione, la mitigazione e il monitoraggio degli attacchi informatici. È inoltre approfondita l'evoluzione del mercato della cyber insurance, con riferimento alle sue criticità strutturali e alle prospettive di sviluppo come strumento di resilienza organizzativa. L'articolo propone infine un modello integrato di gestione del rischio informatico, orientato all'efficienza operativa, alla sicurezza dei sistemi e alla creazione di valore sostenibile nel lungo termine.

In an increasingly digitised and interconnected economic context, IT risk management is a key strategic lever for business competitiveness. This paper analyses the structural integration of cybersecurity into management control systems and corporate governance, highlighting the proactive approach of risk-based performance management and the cybersecurity by design paradigm. Particular attention is paid to the role of Enterprise Risk Management (ERM) as a conceptual framework for integrated and cross-cutting digital risk management. The analysis focuses on the main regulatory models (GDPR, NIS2, DORA, ISO/IEC 27001) and technical-economic tools, including insurance coverage, that enable the prevention, mitigation and monitoring of cyber-attacks. It also examines the evolution of the cyber insurance market, with reference to its structural criticalities and prospects for development as a tool for organisational resilience. Finally, the article proposes an integrated model of cyber risk management, geared towards operational efficiency, system security and the creation of long-term sustainable value.

Received: September 2025
Published: 30/09/2025

Keywords: Contratto di rete, network, piccole-medie imprese, performance, pandemia

1 – Introduzione

Negli ultimi decenni si è assistito alla graduale digitalizzazione dell'economia globale, verificatasi a partire dalla metà del secolo scorso, attraverso l'inclusione graduale dei cosiddetti "beni intangibili" che rappresentano una nuova forma di capitale, i quali includono dati, informazioni e tecnologie che affiancano i tradizionali beni capitali, posti al centro del modello economico convenzionale (Rifkin, 2019). Questo processo è stato agevolato dallo sviluppo di tecnologie avanzate, quali soluzioni cloud, comunicazioni 5G e intelligenza artificiale, che hanno consentito agli attori economici di conservare, scambiare, elaborare e analizzare dati e informazioni in quantità sempre crescenti ed in modo sempre più soddisfacente (Provasi, & Guizzetti, 2019). Detto ciò, però, la digitalizzazione dell'economia non rappresenta solo una fonte di enormi opportunità di sviluppo ed innovazione, ma anche l'accrescersi di minacce nuove che in alcuni casi potrebbero portare a conseguenze molto gravi. In un periodo relativamente breve, infatti, la società contemporanea è stata esposta a cambiamenti molto intensi legati all'integrazione delle tecnologie dell'informazione e della comunicazione nella maggior parte dei settori dell'attività umana. La dipendenza dalle *Information and Communications Technology* (ICT) ha diversi aspetti negativi, che vanno prontamente combattuti, tra cui attacchi e crimini informatici (Gazzola *et al*., 2020). È necessario rispondere a questi fenomeni creando uno spazio per l'implementazione e l'attuazione dei principi di *cybersecurity* e di sicurezza delle informazioni su tutti i livelli e nei confronti di tutte le parti interessate (Bon *et al*. 2016). Pertanto, diventa necessaria la predisposizione di misure di sicurezza e prevenzione che tengano debitamente conto del mutato scenario economico-sociale, che assume un'importanza strategica, che non può prescindere dall'adozione di idonei modelli di valutazione e gestione del rischio, includendo i rischi *cyber*. Nondimeno, lo sviluppo tecnologico rende sempre più difficoltoso prevedere le minacce future.

A livello aziendale, la tecnologia ha assunto un ruolo imprescindibile. La cosiddetta Quarta Rivoluzione Industriale (4IR)—detta anche Rivoluzione Industriale 4IR o 4.0—deriva da "Industria 4.0", una tendenza all'automazione industriale che integra alcune tecnologie produttive per migliorare le condizioni di lavoro e aumentare la produttività e anche la qualità produttiva degli impianti. La data d'inizio della rivoluzione 4IR non è ancora stata stabilita in via ufficiale, probabilmente perché è tuttora in corso e solo a posteriori sarà possibile indicarne l'atto fondante (l'argomento è stato al centro del World Economic Forum 2016, dal 20 al 24 gennaio a Davos, in Svizzera, intitolato appunto "Mastering the Fourth Industrial Revolution"). Laq rivoluzione 4IR è caratterizzata dalla crescita esponenziale *dell'Internet of Things* (IoT)—l'estensione di internet al mondo degli oggetti e dei luoghi concreti—e dalla diffusione di infrastrutture immateriali—come banche dati trasversali e piattaforme digitali condivise—ha reso necessaria una profonda revisione dei modelli operativi e tecnologici delle imprese.

Tali trasformazioni, pur portando con sé opportunità in termini di efficienza e competitività, hanno anche introdotto nuove forme di vulnerabilità, sconosciute ai paradigmi organizzativi tradizionali di queste organizzazioni. In particolare, l'aumento dei rischi *cyber* è una diretta conseguenza dell'evoluzione degli ecosistemi digitali d'impresa. Pertanto, in questo scenario, la digitalizzazione diffusa ha determinato una vera e propria evaporazione dei confini geografici e funzionali relativi all'accesso, al trattamento e alla protezione dei dati. Un singolo incidente informatico, pertanto, può generare danni ingenti e sistemici, compromettendo intere filiere produttive e provocando ricadute reputazionali e legali di lungo periodo. La *cybersecurity*, in tal senso, non può essere concepita come un dominio statico, infatti, la rapidità con cui evolvono le

minacce richiede un adattamento dinamico delle strategie di difesa, incluse quelle assicurative, che devono costantemente aggiornarsi per rispondere alle nuove criticità emergenti.

Alla luce di queste premesse, il presente contributo si propone di esplorare come la crescente complessità delle minacce digitali, congiunta all'adozione pervasiva delle tecnologie, imponga alle imprese moderne l'integrazione strutturata della cybersecurity nel sistema di controllo di gestione. L'analisi si concentrerà, in particolare, su come i principi e gli strumenti di gestione del rischio informatico – comprese le coperture assicurative e i modelli normativi di riferimento (GDPR, NIS2, DORA, ISO 27001) – possano essere incorporati nei processi di controllo direzionale e nei sistemi informativi aziendali, contribuendo così a una governance più efficiente, proattiva e resiliente. Dal punto di vista metodologico, l'articolo adotta un approccio qualitativo e multidisciplinare, fondato sull'analisi critica della letteratura scientifica, degli standard internazionali e delle principali fonti normative europee e internazionali in tema di cybersecurity. Inoltre, sono stati inoltre considerati report istituzionali e *industry-based* (es. CLUSIT, ENISA, OECD), al fine di fornire una visione integrata e attuale della gestione del rischio informatico. Pertanto, l'approccio metodologico adottato si fonda sulla triangolazione concettuale delle fonti (Denzin, 1978), combinando evidenze provenienti dalla letteratura scientifica, da normative internazionali e da report istituzionali, con l'obiettivo di fornire una visione integrata e aggiornata della gestione del rischio informatico nella governance aziendale. L'impostazione si basa su una revisione narrativa, orientata a mettere in luce le interconnessioni tra cybersecurity, governance aziendale e strumenti di controllo direzionale (Webster & Watson, 2002; Tranfield, Denyer & Smart, 2003; Brunetti, 2012).

2 – Il rischio informatico: definizioni, minacce e impatti

A causa della complessità e dell'interdisciplinarità dell'argomento, non esiste una definizione standard e universalmente accettata di "*cyber risk*". Il termine si riferisce a una molteplicità di fonti di rischio che coinvolgono le risorse informatiche e tecnologiche di un'organizzazione. La *cybersecurity*, infatti, è una disciplina trasversale che integra aspetti sia tecnici – relativi a reti, sistemi e infrastrutture digitali – sia economici, connessi alla gestione del rischio, agli impatti reputazionali e alla continuità operativa.

Nel tempo sono state proposte diverse definizioni autorevoli, tra cui quella contenuta nello standard ISO/IEC 27005:2018, che descrive il *cyber risk* come "la possibilità che una determinata minaccia sfrutti le vulnerabilità di un bene o di un gruppo di beni e causi quindi un danno all'organizzazione" (ISO, 2018). Occorre anche far riferimento alla definizione strutturata proveniente dal National Institute of Standards and Technology (NIST) degli Stati Uniti, secondo cui il rischio informatico è "una misura con cui un'entità è minacciata da una circostanza o un evento potenziale, e tipicamente è una funzione degli impatti negativi che potrebbero verificarsi se la circostanza o l'evento si verificasse e della probabilità che ciò accada" (NIST, 2012). Ed infine, un ulteriore contributo è quello fornito dall'Agenzia dell'Unione Europea per la Cybersecurity (ENISA), che definisce il *cyber risk* come "il rischio di una perdita finanziaria, a causa di un'interruzione operativa o di un danno alla reputazione di un'organizzazione a seguito di un malfunzionamento dei suoi sistemi informatici" (ENISA, 2016). Queste definizioni, pur differenti nella formulazione, convergono nel descrivere il rischio informatico come un rischio multidimensionale, derivante dall'interazione tra minacce tecnologiche, vulnerabilità sistemiche e potenziali conseguenze operative, economiche o reputazionali.

Nel contesto accademico, le prime elaborazioni teoriche del concetto di *cyber risk* si sono concentrate prevalentemente sulle minacce connesse all'uso di Internet, evidenziando i pericoli legati all'accesso alla rete e alla fragilità dei sistemi operativi interconnessi (Gordon *et al*., 2003). Con il progressivo sviluppo del cyberspazio e delle tecnologie digitali, la nozione si è ampliata fino a includere una varietà di rischi emergenti in un ambiente informativo sempre più dinamico e interdipendente (Refsdal *et al*., 2015). Un contributo particolarmente significativo in questa direzione è quello di Cebula e Young (2010), i quali definiscono il *cyber risk* come un "rischio operativo legato agli asset tecnologici, con conseguenze che riguardano la confidenzialità, la disponibilità e l'integrità delle informazioni o dei sistemi informatici". Questa impostazione evidenzia il legame tra rischio informatico e sicurezza delle informazioni, ponendo l'accento sull'impatto potenziale su *asset* strategici. Ulteriori sviluppi concettuali si devono al World Economic Forum (2012), che definisce il *cyber risk* come "una combinazione della probabilità di un evento nei sistemi informativi di rete e degli effetti di tale evento sui beni e sulla reputazione di un'organizzazione", sottolineando così la dimensione probabilistica del rischio e la sua rilevanza economica e reputazionale.

Negli ultimi anni, la letteratura ha posto crescente attenzione alla natura sistemica e interdisciplinare del rischio informatico, in particolare nella sua connessione con la resilienza organizzativa, il rischio operativo e la continuità del business. Böhme *et al*. (2018) hanno sottolineato come la valutazione del *cyber risk* debba tener conto non solo della natura tecnica delle vulnerabilità, ma anche delle asimmetrie informative, delle esternalità negative e dei rischi correlati generati da minacce comuni a più entità economiche. Nel contesto post-pandemico, il concetto di cyber risk ha ulteriormente ampliato il proprio perimetro, includendo anche i rischi associati al lavoro da remoto, all'intelligenza artificiale e all'automazione delle infrastrutture critiche (Cavusoglu *et al*., 2022; ENISA, 2023).

L'adozione accelerata delle tecnologie digitali ha infatti aumentato la superficie d'attacco, mentre la maggiore disponibilità di strumenti per la compromissione dei sistemi ha reso più probabili attacchi sofisticati come quelli ransomware, supply chain attacks e deepfake-based frauds (Cheng *et al*., 2021). La Tabella 1 raccoglie le principali definizioni fornite le quali hanno contribuito a standardizzare la terminologia, riflettendo la varietà di approcci che ancora oggi connota il *cyber risk* quale fenomeno complesso e multidimensionale.

Come detto sopra, il *cyber risk* comprende una moltitudine di rischi che possono provenire da una serie di fonti, spesso impreviste e i cui impatti possono variare nel colpire un'azienda. Tali rischi possono derivare da errori umani o di sistema, nonché da attività criminali informatiche, spesso motivate da scopi delittuosi, come furti, rapine o sabotaggi. Detto ciò, nell'attuale panorama informatico gli incidenti informatici possono generare diverse tipologie di danni, comunemente classificate in tre macro-categorie (Mauceri, 2016):

1. *DANNI MATERIALI DIRETTI E INDIRETTI*: comprendono i danni fisici, parziali o totali, subiti da beni tangibili come server, reti in fibra ottica, personal computer, dispositivi mobili, macchinari o altre apparecchiature elettroniche. Tali danni derivano da diversi eventi, tra cui incendi, calamità naturali, furti, atti vandalici o comportamenti umani dolosi e/o colposi.

2. *DANNI IMMATERIALI DIRETTI E INDIRETTI*: riguardano la compromissione di beni intangibili ma fondamentali per il funzionamento dell'impresa, come i dati e i s*oftware*. Rientrano in questa categoria eventi quali la cancellazione accidentale di *database* contenenti informazioni critiche, l'infezione da *malware* o virus informatici e i guasti del software che determinano l'indisponibilità di servizi digitali. I danni immateriali diretti si concretizzano, ad esempio,

nell'impossibilità per l'azienda di proseguire la propria attività operativa. A differenza dei sinistri materiali tradizionali, l'interruzione causata da un attacco informatico è spesso totale, immediata e può estendersi anche a sedi remote. I danni immateriali indiretti includono invece la perdita di reputazione, il deterioramento dell'immagine aziendale e l'erosione di quote di mercato conseguente all'interruzione dei servizi o alla compromissione della fiducia degli stakeholder.

3. *RICHIESTE DI RISARCIMENTO PER RESPONSABILITÀ VERSO TERZI:* questa categoria si riferisce ai costi sostenuti per far fronte a richieste di indennizzo provenienti da soggetti esterni, quali clienti, fornitori o partner. Tali richieste possono insorgere in seguito all'interruzione di servizi causata da un incidente informatico, che impatti negativamente sull'adempimento delle obbligazioni contrattuali o sui livelli di servizio attesi.

Tabella 1 – Sintesi delle definizioni accademiche e degli sviluppi concettuali sul rischio informatico *(Fonte: Elaborazione dell'autore)*

Autori	Definizione/ focus	Elementi concettuali
ISO/IEC 27005 (2018)	"Possibilità che una minaccia sfrutti una vulnerabilità di un bene informativo causando un danno all'organizzazione."	Approccio sistemico, rischio come combinazione di minaccia, vulnerabilità e impatto.
NIST (2012)	"Misura del grado in cui un'entità è minacciata da una specifica fonte che potrebbe sfruttare una vulnerabilità."	Misurabilità del rischio, enfasi su minaccia, vulnerabilità e danno alle operazioni.
ENISA (2016)	"Rischio di perdita finanziaria, interruzione operativa o danno reputazionale per malfunzionamento dei sistemi."	Enfasi su conseguenze economiche, operative e reputazionali.
Gordon *et al.* (2003)	Focus sulle minacce derivanti da Internet e vulnerabilità della rete.	Concetto iniziale di cyber risk legato alla connettività e alla fragilità dei sistemi.
Refsdal *et al.* (2015)	Estensione a rischi emergenti in ambienti dinamici e interconnessi.	Cyber risk come rischio evolutivo, sistemico e interdipendente.
Cebula & Young (2010)	"Rischio operativo legato agli asset informativi con impatto su confidenzialità, disponibilità e integrità."	Legame tra cyber risk e sicurezza informatica (CIA Triad).
World Economic Forum (2012)	"Combinazione della probabilità di un evento e dei suoi effetti sui beni e sulla reputazione."	Dimensione probabilistica e rilevanza economica/reputazionale.
Böhme *et al.* (2018)	Considerazione di esternalità, asimmetrie informative, rischi sistemici.	Approccio interdisciplinare, impatti interorganizzativi.
Cavusoglu *et al.* (2022); ENISA (2023)	Estensione del rischio a IA, automazione, lavoro da remoto.	Cyber risk come rischio dinamico legato a tecnologie emergenti e nuove superfici d'attacco.
Cheng *et al.* (2021)	Attenzione su ransomware, attacchi alla supply chain, deepfake-based frauds.	Evoluzione del rischio verso forme sofisticate e pervasive.

Questa classificazione è utile per comprendere l'ampiezza delle conseguenze potenziali di un sinistro informatico e per valutarne le implicazioni economiche e assicurative (Mauceri, 2016). Gli incidenti informatici, quindi, possono potenzialmente portare a diversi tipi di perdite,

insieme a diverse forme di responsabilità rivolte verso le parti coinvolte nell'incidente, come clienti, fornitori, dipendenti e azionisti.

2.1 – *Le principali minacce informatiche e le implicazioni aziendali*

Nel contesto aziendale, la gestione del rischio informatico rappresenta una componente cruciale della strategia di governance e controllo interno, in quanto le minacce informatiche possono compromettere seriamente l'operatività, la reputazione e la sostenibilità economica di un'organizzazione. Pertanto, per l'azienda, tali minacce si manifestano come attacchi intenzionali o incidenti involontari che colpiscono le infrastrutture informatiche e compromettono gli obiettivi fondamentali di sicurezza, ossia riservatezza, integrità e disponibilità dei dati (Jang-Jaccard & Nepal, 2014). La capacità delle imprese di gestire queste minacce è diventata una dimensione determinante della resilienza organizzativa.

2.1.1 – Phishing

Il phishing rappresenta una delle minacce più insidiose per le imprese, poiché sfrutta l'errore umano – anello debole della sicurezza – per ottenere accesso a informazioni riservate, credenziali aziendali e dati finanziari (Jakobsson & Myers, 2007). In tal caso, le conseguenze per un'organizzazione includono violazioni dei dati, truffe, furti d'identità digitale e perdita di fiducia da parte di clienti ed investitori. Tra le principali varianti di phishing che possono colpire un'organizzazione, la forma più comune è rappresentata dall'email phishing, che si manifesta attraverso l'invio massivo di messaggi fraudolenti indirizzati a dipendenti, dirigenti o clienti, con lo scopo di carpire informazioni sensibili o indurre all'accesso a siti web malevoli. Accanto a questa modalità tradizionale, si sono diffuse tecniche più sofisticate e mirate come lo smishing e il vishing. Nel primo caso, gli attacchi vengono veicolati tramite messaggi di testo (SMS), mentre nel secondo avvengono attraverso chiamate vocali. Entrambe le modalità sono spesso utilizzate per aggirare i sistemi di protezione delle comunicazioni aziendali, colpendo in particolare i reparti di customer care o le aree amministrative. Un'altra forma emergente è il social media phishing, che si serve delle piattaforme di networking (come Facebook, Instagram o X) per assumere l'identità di persone o aziende note, allo scopo di ingannare dipendenti e clienti. Questo tipo di attacco, oltre al rischio di furto di dati, comporta potenziali danni reputazionali rilevanti per l'impresa. Infine, il pharming rappresenta una tecnica più avanzata, che si basa sulla compromissione dei sistemi DNS aziendali. In questo caso, gli utenti vengono inconsapevolmente reindirizzati verso siti web fraudolenti che imitano quelli legittimi, con gravi rischi per i processi aziendali digitali, in particolare quelli legati all'e-commerce o all'utilizzo di piattaforme interne (Zhou *et al*., 2007).

2.1.2 – Malware

Il malware è una minaccia altamente pervasiva che può compromettere la continuità operativa di un'azienda, provocando perdita di dati critici, interruzioni nei servizi IT, blocco delle catene di fornitura e richieste di riscatto nei casi di *ransomware*. Le imprese, specialmente nei settori manifatturieri, bancari e sanitari, sono bersagli frequenti per malware progettati con finalità di estorsione economica o spionaggio industriale (Egele *et al*., 2012). In ambito aziendale, i malware si presentano in diverse forme, ciascuna con caratteristiche e conseguenze specifiche per la sicurezza e la continuità operativa. Tra le tipologie più rilevanti, spiccano innanzitutto i *ransomware*, *software* malevoli che, una volta infiltrati nei sistemi aziendali, cifrano i dati e ne

bloccano l'accesso fino al pagamento di un riscatto. Questo tipo di attacco può paralizzare interi reparti aziendali, causando interruzioni operative prolungate e costi ingenti per il ripristino delle funzionalità (Kharraz *et al*., 2015). Altrettanto insidiosi sono i *trojan* e gli *spyware*, programmi progettati per agire in modo subdolo all'interno dei sistemi informatici, raccogliendo informazioni sensibili senza che l'utente ne sia consapevole. Nel contesto aziendale, ciò può significare l'esfiltrazione di dati strategici, proprietà intellettuale o informazioni riservate su clienti e dipendenti, con gravi implicazioni sia legali sia reputazionali. Infine, i *worms* rappresentano una minaccia pervasiva, poiché sono in grado di autoreplicarsi e diffondersi rapidamente attraverso le reti aziendali, compromettendo server e dispositivi connessi, oltre ad aggravare l'estensione dell'attacco e limitare il suo contenimento.

2.1.3 – Attacchi Man-in-the-Middle (MITM)

Gli attacchi Man-in-the-Middle, se condotti con successo, possono compromettere la riservatezza delle transazioni finanziarie, la sicurezza dei flussi di comunicazione interna e l'integrità delle comunicazioni con stakeholder esterni. Le imprese che gestiscono dati sensibili (es. nel settore legale, finanziario o sanitario) sono particolarmente esposte a questo tipo di minaccia, soprattutto se operano in ambienti *cloud* o con connessioni mobili non protette (Conti *et al*., 2016).

2.1.4 – Attacchi DoS e DDoS

Gli attacchi Denial of Service (DoS) e Distributed Denial of Service (DDoS) compromettono la disponibilità dei servizi aziendali, rendendo inaccessibili siti *web*, piattaforme *e-commerce*, sistemi ERP o servizi *cloud*. Le implicazioni economiche sono spesso dirette: perdita di ricavi, penalizzazioni contrattuali, danni reputazionali e spese straordinarie per il ripristino dei servizi (Zargar, Joshi & Tipper, 2013). Gli attacchi di questo tipo possono manifestarsi attraverso diverse modalità operative, ciascuna finalizzata a compromettere la disponibilità dei servizi digitali di un'organizzazione. Tali attacchi rappresentano una minaccia significativa per le imprese, poiché sono in grado di interrompere i flussi operativi, bloccare piattaforme online e generare perdite economiche immediate (Zargar, Joshi, & Tipper, 2013). Una delle tecniche più comuni è rappresentata dai TCP *floods*, che consistono in un'elevata quantità di richieste di connessione inviate ai server, senza completare correttamente il processo di *handshake*, causando così la saturazione delle risorse di rete. Similmente, gli attacchi volumetrici mirano a inondare le reti aziendali con picchi di traffico ingestibili, rendendo impossibile l'accesso ai servizi da parte degli utenti legittimi (Douligeris & Mitrokotsa, 2004). Diversamente, gli attacchi applicativi si concentrano su specifiche funzioni digitali, come ad esempio i sistemi di pagamento o le interfacce per la prenotazione, colpendo in modo mirato i componenti critici dell'infrastruttura IT (Kumar *et al*., 2020). Questi attacchi, sebbene meno evidenti, possono avere un impatto immediato sull'esperienza dell'utente e sulla capacità dell'impresa di generare valore. Infine, gli attacchi di frammentazione sfruttano pacchetti di dati incompleti o manipolati, inducendo i server a spendere risorse computazionali per ricostruirli, con conseguente degrado delle prestazioni complessive. Le imprese che non adottano sistemi efficaci di business continuity e disaster recovery sono particolarmente esposte a queste minacce. In assenza di strategie preventive e di risposta, anche un attacco della durata di pochi minuti può tradursi in perdite di fatturato, sanzioni contrattuali e danni alla reputazione aziendale (ENISA, 2023).

3 – Normativa

Oggi esistono numerosi *standard* di sicurezza informatica elaborati da enti nazionali e internazionali, ciascuno concepito per rispondere a esigenze specifiche di protezione dei sistemi informativi. L'adozione di *standard* adeguati consente alle organizzazioni di migliorare la condivisione delle informazioni, garantire maggiore trasparenza e rafforzare la capacità di risposta agli attacchi informatici. Pertanto, oggi, la molteplicità di *standard* riflette la crescente complessità e diffusione delle minacce cibernetiche, che ha indotto l'Unione Europea a rafforzare le proprie strategie difensive, con l'obiettivo di tutelare l'integrità, la sicurezza e la resilienza dell'infrastruttura digitale dell'UE.

Pertanto, con il progresso tecnologico, gli standard continueranno ad evolversi per rispondere a nuove sfide emergenti, legate ad ambiti innovativi come l'*IoT*, i *Big Data* e i servizi in *cloud*. In questo contesto, non esiste un unico standard universalmente valido per tutti i settori: piuttosto, ogni organizzazione deve individuare il *framework* più adatto alle proprie esigenze operative e ai rischi specifici cui è esposta, valorizzando gli strumenti realmente efficaci rispetto alle minacce di settore.

3.1 – *Una panoramica della legislazione in materia di cyber risk*

In Italia non esiste attualmente una normativa organica e specifica in materia di cybersecurity. L'ordinamento giuridico nazionale si presenta infatti frammentario e privo di un quadro normativo sistematico in grado di orientare in modo efficace imprese, organizzazioni e istituzioni nella gestione del rischio informatico. Le disposizioni esistenti si limitano a regolare, in modo settoriale, le responsabilità civili, penali o amministrative connesse a specifiche ipotesi di danno, come ad esempio la violazione della privacy o l'accesso abusivo a sistemi informatici. A colmare parzialmente tale lacuna è intervenuta l'Unione Europea, che negli ultimi anni ha adottato un *corpus* sempre più articolato di atti normativi in materia di sicurezza informatica. Tuttavia, anche la disciplina europea si caratterizza per una struttura multilivello, composta da regolamenti, direttive, raccomandazioni e linee guida, non sempre dotati di efficacia vincolante. Ne risulta un panorama normativo complesso, talvolta disomogeneo, nel quale coesistono standard differenti tra i vari comparti del settore finanziario, spesso sovrapposti o non perfettamente coordinati, con conseguenti difficoltà applicative per gli operatori coinvolti.

3.1.1 – Direttiva NIS e NIS 2

Con il Decreto Legislativo 18 maggio 2018, n. 65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha recepito nell'ordinamento nazionale la Direttiva (UE) 2016/1148, nota come Direttiva NIS (Network and Information Security). Si è trattato della prima iniziativa legislativa orizzontale dell'Unione Europea volta a garantire un livello elevato e omogeneo di sicurezza delle reti e dei sistemi informativi negli Stati membri. Uno degli aspetti qualificanti della direttiva è stato l'obbligo, per gli operatori di servizi essenziali (OSE) e per alcuni fornitori di servizi digitali (FSD), di adottare misure tecniche e organizzative adeguate atte a prevenire e gestire gli incidenti informatici, nonché di notificarli alle autorità competenti. L'impatto della Direttiva NIS è stato rilevante, infatti essa ha contribuito al rafforzamento delle capacità nazionali in materia di cybersecurity e ha promosso la cooperazione tra Stati membri, migliorando la resilienza complessiva degli attori pubblici e privati coinvolti. Tuttavia, l'evoluzione del panorama delle minacce e la crescente digitalizzazione hanno evidenziato i

limiti del quadro normativo introdotto. Per rispondere in modo più efficace alle nuove sfide poste dall'aumento della superficie di attacco digitale e dalla complessità delle infrastrutture interconnesse, nel dicembre 2022 è stata adottata la Direttiva (UE) 2022/2555 (c.d. Direttiva NIS2). Quest'ultima rafforza i requisiti di sicurezza, estende il campo di applicazione a nuovi settori e introduce meccanismi di vigilanza, *enforcement* e *reporting* più rigorosi, con l'obiettivo di garantire una maggiore uniformità e resilienza a livello europeo.

3.1.2 – GDPR

Il Regolamento (UE) 2016/679, noto come General Data Protection Regulation (GDPR), in vigore dal 25 maggio 2018, disciplina il trattamento dei dati personali nell'ambito dell'Unione Europea, segnando un'evoluzione significativa da un approccio meramente formale alla protezione dei dati verso una tutela sostanziale dei diritti degli interessati. Il regolamento si fonda sul principio della *data protection by design and by default*, imponendo che ogni trattamento di dati sia progettato fin dall'origine con l'obiettivo prioritario di salvaguardare la riservatezza e i diritti delle persone fisiche. Per tale scopo, il GDPR richiede l'adozione di misure tecniche, anche in ambito di sicurezza cibernetica, organizzative ed operative, volte a ridurre al minimo i rischi di accesso non autorizzato, perdita o alterazione dei dati. Tra i principali strumenti di tutela figurano la valutazione d'impatto sulla protezione dei dati (DPIA), la nomina di un *Data Protection Officer* (DPO), nonché l'adozione di politiche interne coerenti con i principi di responsabilizzazione (accountability). In base a questo, il regolamento rafforza significativamente i diritti degli interessati, che includono, tra gli altri, il diritto di accesso, rettifica, cancellazione (diritto all'oblio), limitazione del trattamento, portabilità dei dati e opposizione al trattamento, in particolare per finalità di marketing diretto. Inoltre, vengono introdotti vincoli stringenti all'uso dei dati da parte di terzi, obblighi di trasparenza nelle informative, e criteri rigorosi per il trasferimento di dati verso Paesi terzi. In merito a ciò, particolare rilievo assumono i principi della minimizzazione dei dati, secondo cui i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del trattamento, e della limitazione della conservazione, che impone di conservare i dati solo per il tempo strettamente necessario (art. 5, par. 1, lett. c) e d), GDPR). Il Regolamento prevede inoltre un quadro sanzionatorio severo per le violazioni, con multe che possono arrivare fino al 4% del fatturato annuo globale dell'organizzazione.

3.1.3 – Normativa ISO/IEC 27001

La ISO/IEC 27001 è lo standard internazionale di riferimento per la gestione della sicurezza delle informazioni e costituisce il cuore della famiglia di norme ISO/IEC 27000 – comunemente indicata anche come ISO 27k – dedicata alla sicurezza informatica e alla protezione dei dati. Questo insieme normativo offre un quadro strutturato per l'adozione di politiche, controlli e procedure volte a garantire la protezione efficace delle informazioni. Più nel dettaglio, la ISO 27000 fornisce un glossario condiviso e i concetti fondamentali; la ISO 27001 definisce i requisiti per la progettazione e l'implementazione di un Information Security Management System (ISMS); la ISO 27002 fornisce linee guida pratiche per la gestione della sicurezza delle informazioni; la ISO 27005 si concentra sulla valutazione e gestione del rischio informatico. Altri standard, come la ISO 27033 sulla sicurezza di rete o la ISO 27034 sulla sicurezza delle applicazioni, approfondiscono aspetti tecnici più specifici. Tra queste, la ISO/IEC 27001 rappresenta la norma centrale e più applicata, in quanto stabilisce un modello sistemico per

proteggere la riservatezza, l'integrità e la disponibilità delle informazioni – la cosiddetta triade CIA:

1. Riservatezza: l'accesso ai dati è consentito solo a persone autorizzate;
2. Integrità: i dati possono essere modificati solo da soggetti autorizzati;
3. Disponibilità: le informazioni devono essere accessibili quando necessario da chi ne ha diritto.

L'approccio proposto dalla ISO 27001 è basato sul ciclo di miglioramento continuo (Plan-Do-Check-Act) e prevede l'identificazione dei rischi, la loro valutazione e l'adozione di misure di sicurezza coerenti con la criticità delle informazioni trattate. L'adozione dello standard, seppur volontaria, è fortemente raccomandata in ambito aziendale, poiché consente di rafforzare la resilienza organizzativa, garantire la compliance normativa (ad es. con il GDPR), tutelare gli *asset* informativi critici e aumentare la fiducia da parte di stakeholder e clienti. La flessibilità della norma consente la sua applicazione trasversale a qualunque tipo di organizzazione, indipendentemente dal settore, dalla dimensione o dalla struttura, rendendola uno strumento essenziale nella governance del rischio informatico.

3.1.4 – DORA

Il Digital Operational Resilience Act (DORA) è un regolamento dell'Unione Europea che istituisce un quadro giuridico vincolante e integrato per la gestione del rischio legato alle tecnologie dell'informazione e della comunicazione (ICT) nel settore finanziario europeo. Presentato dalla Commissione Europea nel settembre 2020, il DORA fa parte di un più ampio pacchetto legislativo sulla finanza digitale, volto a regolamentare anche le criptovalute e rafforzare la strategia dell'UE in materia di digitalizzazione dei mercati. È stato formalmente adottato nel novembre 2022 e diventerà pienamente applicabile dal 17 gennaio 2025. L'obiettivo principale del DORA è creare un sistema normativo armonizzato e coerente che rafforzi la resilienza operativa digitale degli operatori finanziari. L'Unione Europea ha infatti riconosciuto l'urgenza di superare le disomogeneità tra le normative nazionali e di colmare le lacune regolamentari, così da garantire una risposta efficace e tempestiva alle minacce informatiche. Il regolamento introduce per la prima volta un approccio sistemico e integrato alla gestione del rischio ICT, promuovendo una cultura della sicurezza digitale condivisa e vincolante per tutti gli attori coinvolti nel sistema finanziario.

Il campo di applicazione del DORA è estremamente ampio, esso infatti non si rivolge solo agli enti creditizi, alle imprese di investimento, alle compagnie di assicurazione e ai fornitori di servizi per cripto-attività, ma anche a soggetti meno tradizionali, come i gestori di fondi alternativi, gli intermediari finanziari, le agenzie di rating e le piattaforme di crowdfunding. Il regolamento si estende inoltre ai fornitori terzi di servizi ICT, soprattutto se questi offrono soluzioni critiche per l'operatività degli operatori finanziari. Il DORA prevede una serie di obblighi chiave per le entità soggette alla normativa. In primo luogo, questo regolamento impone l'adozione di un solido quadro di governance, in cui l'organo di gestione dell'impresa assume un ruolo centrale nella definizione e nell'attuazione delle strategie di sicurezza informatica. Il regolamento richiede poi l'implementazione di un piano strutturato di gestione dei rischi ICT, che includa misure di prevenzione, rilevazione e risposta agli incidenti, nonché strategie di continuità operativa e *disaster recovery*. Un elemento innovativo del DORA è rappresentato dalla standardizzazione delle procedure di classificazione e segnalazione degli

incidenti informatici. Infatti, gli operatori sono chiamati a rilevare, registrare, categorizzare e comunicare gli eventi critici alle autorità competenti, secondo protocolli uniformi che facilitano la tempestività e l'efficacia degli interventi. Particolare attenzione è rivolta anche alla gestione dei rapporti con i fornitori terzi, n quanto il regolamento stabilisce precisi obblighi di *due diligence*, controllo contrattuale e documentazione, con l'obiettivo di garantire la sicurezza delle infrastrutture esternalizzate. Infine, il DORA promuove attivamente la condivisione di informazioni tra soggetti del settore attraverso meccanismi di cooperazione volontaria. L'idea è quella di potenziare la capacità collettiva del sistema finanziario europeo di prevenire, rilevare e contrastare le minacce cyber, attraverso lo scambio strutturato di dati e pratiche.

Il Regolamento DORA rappresenta, in conclusione, una pietra miliare nel percorso di rafforzamento della resilienza digitale in Europa. Coniugando obblighi stringenti, strumenti operativi e un approccio integrato alla gestione del rischio, esso costituisce un punto di riferimento essenziale per il futuro della sicurezza informatica nel settore finanziario dell'Unione. Alla luce della crescente attenzione normativa verso la sicurezza informatica, la Tabella 2 fornisce una sintesi strutturata dei principali riferimenti legislativi e standard internazionali attualmente rilevanti nella disciplina del cyber risk, evidenziandone l'ambito di applicazione e i principali contenuti.

Tabella 2 – Riferimenti normativi e standard sulla cybersecurity (*Fonte*: Elaborazione dell'autore)

Normativa / Standard	Fonte e Anno	Oggetto / Ambito	Principali contenuti e finalità
Direttiva NIS	Direttiva (UE) 2016/1148 – D.Lgs. 65/2018	Sicurezza delle reti e dei sistemi informativi	Impone obblighi a OSE e FSD per prevenzione, gestione e notifica degli incidenti informatici; promuove cooperazione tra Stati membri.
Direttiva NIS2	Direttiva (UE) 2022/2555	Rafforzamento e aggiornamento della NIS	Estende il campo d'applicazione a nuovi settori, rafforza requisiti di sicurezza, introduce vigilanza, enforcement e reporting armonizzati.
GDPR	Regolamento (UE) 2016/679	Protezione dei dati personali	Introdotti principi di privacy by design, accountability, DPIA, DPO; sanzioni fino al 4% del fatturato; misure tecniche e organizzative di sicurezza.
ISO/IEC 27001	ISO/IEC 27001:2013 e seguenti	Sistemi di gestione della sicurezza delle informazioni (ISMS)	Norma centrale della famiglia ISO 27k, basata sul ciclo PDCA; garantisce riservatezza, integrità e disponibilità delle informazioni.
ISO/IEC 27005	ISO/IEC 27005:2018	Risk management in ambito informatico	Linee guida per la valutazione e gestione del rischio cyber come parte dell'ISMS ISO 27001.
DORA	Regolamento (UE) 2022/2554	Resilienza operativa digitale nel settore finanziario	Quadro vincolante per la gestione del rischio ICT: governance, gestione dei fornitori, reporting incidenti, continuità operativa. Applicazione dal 17 gennaio 2025.

3.2 – *Il ruolo della cyber insurance nella gestione del rischio residuo*

Negli ultimi anni, la sicurezza informatica ha assunto un ruolo strategico non solo per la tutela degli *asset* tecnologici, ma anche come variabile critica nella governance e nel controllo di gestione delle organizzazioni pubbliche e private. L'impatto economico degli attacchi informatici – in termini di interruzione operativa, perdita di dati e danni reputazionali – ha reso evidente che la gestione del rischio informatico non può più essere considerata una voce accessoria nei bilanci aziendali, bensì un elemento strutturale delle politiche di investimento e allocazione delle risorse (Heidt *et al*., 2019). In Italia, diversi episodi – come gli attacchi che hanno interessato sistemi informativi regionali, aziende sanitarie locali e strutture ospedaliere – hanno generato significativi disagi per cittadini, dipendenti e pazienti, evidenziando l'esistenza di vulnerabilità sistemiche e l'insufficienza di strumenti di monitoraggio e risposta. Questi eventi mettono in luce la necessità di includere il rischio informatico all'interno dei sistemi di controllo direzionale, definendo indicatori di *performance* e strumenti di *reporting* specifici per la sicurezza digitale.

In un contesto dominato dalla digitalizzazione dei processi – dai social network agli *smart device*, dai sistemi di telelavoro all'automazione industriale – il *cyber risk* assume una rilevanza trasversale che coinvolge tutte le funzioni aziendali. Il controllo di gestione, in questo senso, è chiamato a integrare la *cybersecurity* nella pianificazione strategica e nella misurazione delle performance, promuovendo l'adozione di policy di prevenzione e sensibilizzazione interna. La letteratura manageriale (Damodaran & Amini, 2021) insiste sulla necessità di trattare la sicurezza informatica non come un costo, ma come un investimento in resilienza operativa e sostenibilità organizzativa.

Un'area critica riguarda il cosiddetto fattore umano. Molti attacchi, infatti, sfruttano vulnerabilità comportamentali, come l'apertura di *e-mail di phishing* o l'accesso inconsapevole a link malevoli. È proprio in questa dimensione che la formazione, il monitoraggio e l'analisi dei comportamenti diventano strumenti indispensabili per ridurre la superficie d'attacco. Le funzioni di controllo interno e *audit*, congiuntamente alla direzione ICT, dovrebbero sviluppare strumenti di analisi preventiva e valutazione *ex post* dei *cyber incident*.

Dal punto di vista economico-finanziario, la crescente esposizione al rischio digitale impone alle aziende di riconsiderare le proprie decisioni di *budget*, inserendo la *cybersecurity* tra le priorità di investimento pluriennale. L'adozione di soluzioni di sicurezza avanzate – come i sistemi SIEM, le piattaforme di *threat intelligence* o le architetture zero trust – non solo migliora la postura difensiva, ma rappresenta anche un elemento di valore per gli stakeholder e i partner di mercato. Inoltre, l'adeguamento agli standard internazionali (es. ISO/IEC 27001, NIS2, DORA) costituisce oggi un requisito di compliance imprescindibile, ma anche una leva per la creazione di valore a lungo termine. Pertanto oggi la sicurezza informatica non può più essere considerata una responsabilità esclusiva del reparto IT, ma deve rientrare a pieno titolo nella dimensione strategica del controllo di gestione, come leva di sostenibilità, competitività e continuità operativa.

Il Rapporto CLUSIT 2025 conferma la crescente pervasività e sofisticazione degli attacchi informatici, con implicazioni rilevanti anche per i sistemi di controllo di gestione. Nel 2024 si sono registrati 3.541 attacchi gravi a livello globale, con un incremento del 16% rispetto al 2023 e del 89% rispetto al 2020. Di questi, il 43% ha avuto impatti economici diretti, come interruzioni di servizio, furti di dati e danni reputazionali, rendendo evidente l'urgenza di integrare la gestione del rischio informatico nelle metriche di performance aziendale. In particolare, come

mostra la Figura 1 l'andamento crescente degli attacchi cyber gravi dal 2020 al 2024. Il numero è passato da 1.874 nel 2020 a 3.541 nel 2024, evidenziando non solo un *trend* quantitativamente rilevante ma anche un'accelerazione della minaccia, che supera in modo marcato la linea di crescita media stimata (linea tratteggiata). Questa dinamica conferma che le organizzazioni devono affrontare una nuova normalità caratterizzata da rischi informatici persistenti e strutturali.

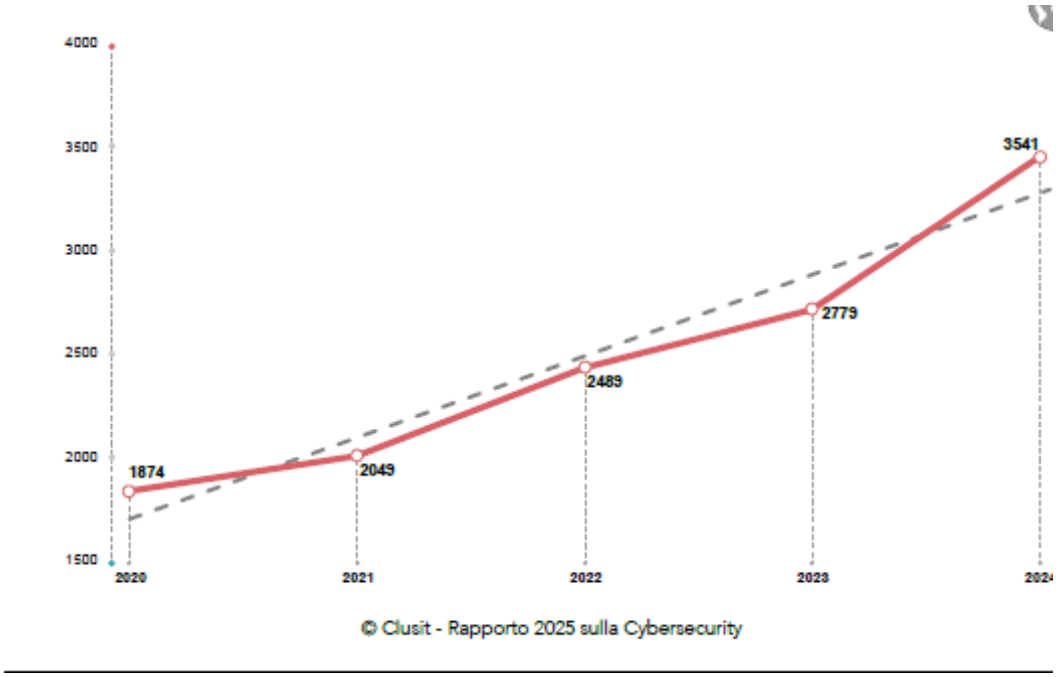

Fig. 1 – Andamento degli incidenti cyber nel periodo 2020-2024
(*Fonte*: Rapporto 2025 CLUSIT)

Il *cybercrime* si conferma il principale *driver* degli attacchi (77%), seguito da finalità di *hacktivism* (13%) ed *espionage/sabotage* (9%). In Italia, il settore più colpito è stato quello della sanità pubblica, seguito da pubblica amministrazione, istruzione, manifattura e finanza (CLUSIT, 2025). Questo dato richiama l'attenzione sul fatto che nessun settore può oggi considerarsi esente, rendendo necessario un approccio trasversale alla gestione dei rischi *cyber*. Dal punto di vista manageriale, la rilevanza crescente del rischio informatico impone una revisione dei tradizionali sistemi di controllo. I dati CLUSIT mostrano che oltre il 60% degli attacchi è reso possibile da vulnerabilità note ma non mitigate o da errori organizzativi e mancanza di consapevolezza interna. Questo evidenzia come il *cyber risk* non sia solo un problema tecnologico, ma soprattutto organizzativo e gestionale. Pertanto, gli strumenti del controllo di gestione – dalla *Balanced Scorecard al risk-adjusted performance management* – devono oggi includere anche indicatori di *cyber resilience*, continuità operativa, spesa in *cybersecurity* e capacità reattiva agli incidenti.

3.3 – *La gestione proattiva dell'esposizione al rischio: una nuova frontiera del controllo direzionale*

Nell'attuale scenario digitale, caratterizzato da minacce in costante evoluzione e superfici d'attacco sempre più estese e frammentate, la gestione proattiva dell'esposizione al rischio si

afferma come un elemento strategico da integrare nei sistemi di controllo direzionale. In questo quadro si afferma il principio della *cybersecurity by design*, secondo cui la sicurezza deve essere incorporata sin dalle fasi iniziali della progettazione di sistemi, processi e infrastrutture digitali, e non aggiunta successivamente come elemento correttivo (Macchia, 2019). Ciò implica che la sicurezza non è più un attributo esterno al ciclo di sviluppo o alle logiche decisionali, ma una componente strutturale delle scelte architetturali e organizzative (Katsumata *et al*., 2010).

Come evidenziato dal Rapporto CLUSIT 2025, una protezione efficace non può più basarsi su logiche reattive o su modelli che scansionano periodicamente la vulnerabilità dell'assetto aziendale. Al contrario, è necessario adottare un approccio continuo, dinamico e predittivo, fondato su analisi avanzate e su una visione integrata degli *asset* aziendali – tanto *on-premise* quanto *in cloud* – e delle loro interazioni.

La gestione dell'esposizione al rischio non si limita alla rilevazione degli incidenti, ma mira a prevenirli, anticipando le modalità di attacco potenzialmente adottabili da attori malevoli. In tale contesto, risulta cruciale implementare sistemi in grado di garantire:

a. una prioritizzazione intelligente delle vulnerabilità, fondata su dati aggiornati di *threat intelligence* e sulla probabilità concreta di sfruttamento;

b. una contestualizzazione del rischio, che non si fermi alla severità tecnica ma consideri la rilevanza strategica dell'*asset* esposto;

c. l'automazione delle misure correttive, per agire tempestivamente e ridurre i tempi di esposizione;

d. l'integrazione con le soluzioni di sicurezza di terze parti, favorendo un ecosistema informativo condiviso.

Dal punto di vista del controllo di gestione, ciò implica una ridefinizione dei tradizionali KPI legati alla sicurezza e alla resilienza. La misurazione della performance non può prescindere da indicatori come il tempo medio di rilevamento e risposta agli incidenti (MTTD/MTTR), il livello di rischio residuo per unità di business, la copertura delle vulnerabilità critiche e il grado di allineamento tra strategia di sicurezza e obiettivi operativi.

L'adozione di un modello proattivo consente, dunque, di ottimizzare l'allocazione delle risorse, concentrare gli investimenti sulle aree ad alto impatto e, soprattutto, rafforzare la capacità dell'organizzazione di resistere agli eventi critici, riducendo i costi potenziali e proteggendo la continuità operativa. In questa prospettiva, la *cybersecurity* diviene una variabile di governo aziendale, da presidiare in sede di *budgeting*, pianificazione strategica e *reporting* direzionale.

Il modello rappresentato nella Figura 2 si fonda su un insieme di concetti riconosciuti nella letteratura economico-aziendale, che giustificano l'integrazione tra gestione del rischio informatico e sistemi di controllo direzionale. In primo luogo, la gestione proattiva del rischio si collega direttamente alla teoria dell'Enterprise Risk Management (ERM), che prevede l'identificazione anticipata delle esposizioni al rischio come leva strategica per la creazione di valore (Beasley *et al*., 2005; Caserio, 2019). L'ERM si configura come un approccio integrato alla gestione dei rischi che attraversa trasversalmente tutte le unità organizzative, superando la visione frammentata del *risk management* tradizionale. Esso consente di connettere la valutazione dei rischi con le scelte di allocazione delle risorse, influenzando in modo diretto i processi di pianificazione strategica e controllo direzionale (Beasley, Branson, & Hancock, 2010; Kaplan & Mikes, 2012). Laddove l'organizzazione adotti un modello di ERM maturo, la gestione

del rischio informatico non si limita alla dimensione tecnica della difesa o alla mera conformità normativa, ma viene elevata a dimensione strategica, integrata nei processi di decisione, *budgeting* e *reporting* (Arena, Arnaboldi, & Azzone, 2010; Woods, 2009).

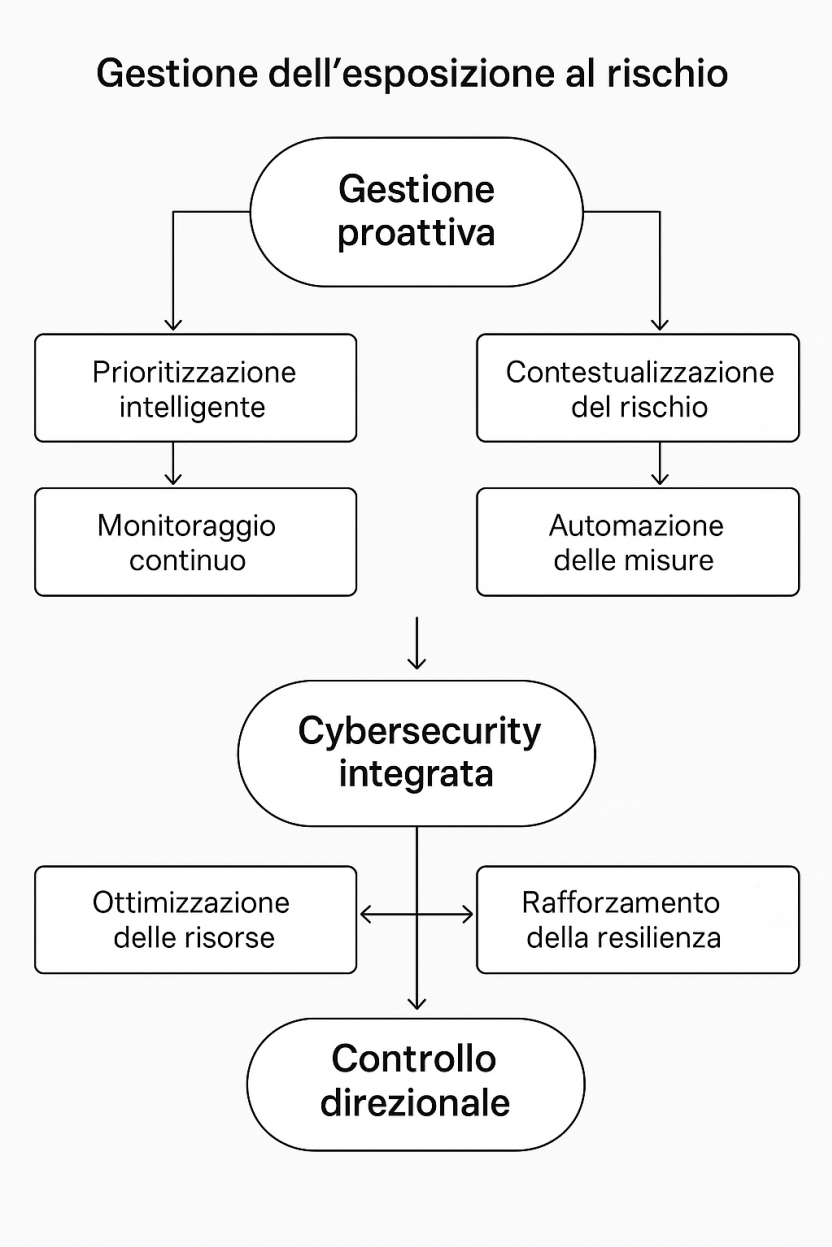

Fig. 2 – Modello proattivo di gestione del rischio informatico
(*Fonte*: Elaborazione dell'autore)

In questo senso, l'integrazione della *cybersecurity* in un sistema di *performance management* consente di migliorare sensibilmente la qualità delle decisioni, grazie a un'informazione più tempestiva, contestualizzata e strutturata rispetto ai potenziali impatti dei cyber risk su asset critici, processi chiave e obiettivi di business (Simons, 1995; Ferreira & Otley, 2009; Lee, 2021). Tale integrazione si traduce anche in una maggiore trasparenza informativa, che favorisce la diffusione di una cultura del rischio consapevole e partecipata, contribuendo a una *governance* più solida e responsabile (Frigo & Anderson, 2011; Power, 2009). Il bilanciamento tra metriche di *performance* e indicatori di rischio (Key Risk Indicators – KRI) permette di monitorare in tempo reale la coerenza tra le scelte operative e le priorità strategiche, promuovendo un allineamento

dinamico e continuo tra obiettivi aziendali e livelli accettabili di esposizione al rischio (Frigo & Anderson, 2011; COSO, 2017). In particolare, la *cybersecurity*, se correttamente integrata nel framework ERM, agisce come un moltiplicatore di resilienza organizzativa e di vantaggio competitivo, proteggendo le risorse, abilitando la trasformazione digitale e rafforzando la fiducia degli stakeholder. In linea con le più recenti evoluzioni concettuali (Mizrak, 2023; Lee, 2021), ciò implica la necessità di trattare il rischio informatico non più come un fattore esogeno e residuale, ma come una variabile endogena, gestibile attraverso strumenti di previsione, simulazione e controllo, pienamente inserita nel ciclo di creazione del valore.

La prioritizzazione delle minacce basata su modelli predittivi e su informazioni di *threat intelligenc*e risponde all'esigenza di razionalizzare l'allocazione delle risorse nei contesti organizzativi complessi (Kaplan & Mikes, 2012). In ambienti digitalizzati, caratterizzati da un'elevata eterogeneità infrastrutturale e da una crescente interconnessione tra processi critici, l'approccio predittivo consente di passare da una logica reattiva a una logica anticipatoria, fondata sull'analisi dinamica dei *pattern* di minaccia e sull'identificazione delle vulnerabilità più esposte a sfruttamento. L'utilizzo integrato di strumenti di *threat intelligence* – quali feed informativi, Indicatori di Compromissione (IoC), analisi comportamentali e fonti open-source – permette di arricchire il processo decisionale con dati contestualizzati e aggiornati, riducendo la dipendenza da valutazioni statiche e non più rappresentative del rischio effettivo. Quando queste informazioni vengono elaborate mediante modelli predittivi, ad esempio reti *bayesiane*, algoritmi di *machine learning* o simulazioni Monte Carlo, è possibile stimare la probabilità concreta di accadimento di un evento avverso e valutarne l'impatto potenziale sull'organizzazione.

Tale approccio consente di definire una scala dinamica delle priorità, in cui il rischio informatico non è misurato solo in termini di gravità tecnica, ma anche in relazione al valore degli asset coinvolti, alla loro criticità operativa e alla posizione che occupano nel disegno strategico dell'impresa. In altri termini, non tutte le minacce meritano la stessa attenzione, e non tutte le vulnerabilità devono essere gestite con lo stesso livello di urgenza: la *risk-based prioritization* orienta l'intervento là dove le conseguenze di un attacco sarebbero più rilevanti, sia in termini economici sia reputazionali (Mizrak, 2023; Lee, 2020). L'effetto sistemico di questa impostazione è duplice: da un lato, si ottiene un uso più efficiente delle risorse – umane, tecnologiche e finanziarie – evitando la dispersione di energie su minacce marginali; dall'altro, si crea un flusso informativo continuo tra la funzione *IT/cybersecurity* e i vertici aziendali, alimentando un processo di apprendimento organizzativo e di adattamento strategico alle minacce emergenti (Ferreira & Otley, 2009; Kure *et al*., 2018). Questo aspetto è cruciale in ambienti ad alta volatilità, in cui la comprensione del contesto e l'adattabilità delle risposte sono determinanti per il vantaggio competitivo. Da qui l'importanza di automatizzare le misure correttive, riducendo i tempi di reazione e integrando l'azione dei sistemi informativi di sicurezza con i cruscotti direzionali e gli strumenti di management control.

Nel cuore dello schema si colloca il concetto di *cybersecurity* integrata, che rappresenta il passaggio critico dal piano tecnico al livello strategico, riflettendo le raccomandazioni della letteratura sulla *cyber risk governance*: l'integrazione dei rischi digitali nei processi di pianificazione e controllo consente non solo di rafforzare la resilienza organizzativa, ma anche di migliorare l'accountability e la capacità adattiva dell'impresa. In questa prospettiva, recenti studi confermano che l'integrazione sistemica della gestione del rischio informatico nella

strategia aziendale promuove una maggiore resilienza e competitività, sottolineando il ruolo della cultura organizzativa e della leadership come fattori abilitanti (Mizrak, 2023).

Infine, i due *output* fondamentali – ottimizzazione delle risorse e rafforzamento della resilienza – sono coerenti con i principi del controllo direzionale orientato al rischio (*risk-based performance management*), secondo cui le risorse vanno allocate verso le aree a maggior impatto sistemico (Simons, 1995; Ferreira & Otley, 2009). Questo approccio implica l'abbandono di una logica distributiva rigida e lineare delle risorse, in favore di una logica selettiva e adattiva, capace di concentrare gli investimenti su quegli ambiti in cui una vulnerabilità o una disfunzione possono compromettere la continuità operativa, la reputazione aziendale o la creazione di valore a lungo termine.

L'ottimizzazione delle risorse in chiave *risk-based* richiede pertanto un'integrazione effettiva tra le funzioni di controllo di gestione e la governance dei sistemi informativi. Solo attraverso una visione integrata tra *IT governance* e controllo direzionale è possibile presidiare le aree critiche, anticipare scenari emergenti e proteggere la sostenibilità del valore nel tempo. Tale integrazione non è solo tecnica, ma strategica e culturale, in quanto essa presuppone che la sicurezza informatica sia considerata non come un costo, ma come una leva di performance e competitività, in grado di supportare i processi decisionali, la fiducia degli stakeholder e la resilienza organizzativa.

In questo senso, le conclusioni della letteratura convergono su alcuni punti essenziali: in primo luogo, emerge la necessità di sviluppare framework multilivello, capaci di combinare aspetti tecnologici, organizzativi e gestionali in un unico disegno di governo del rischio (Lee, 2021). In secondo luogo, si sottolinea l'importanza di integrare la sicurezza sin dalle prime fasi del ciclo di vita dei sistemi (*security by design*), per ridurre *ex ante* la superficie di attacco e favorire economie di apprendimento e scala nella gestione del rischio (Katsumata *et al*., 2010). Inoltre, è evidente l'insufficienza dei modelli tradizionali di *risk management* quando applicati a contesti cyber-fisici complessi, nei quali le interdipendenze tra asset digitali e infrastrutture critiche generano effetti a cascata non lineari e difficilmente prevedibili (Kure *et al*., 2018).

Infine, una componente fondamentale per la maturazione del controllo direzionale orientato al rischio è rappresentata dalla valutazione quantitativa dei rischi e dei ritorni sugli investimenti in sicurezza. In un contesto in cui le risorse sono per definizione limitate, la capacità di misurare l'efficacia e l'efficienza delle misure adottate – ad esempio tramite metriche di *cyber performance* o modelli di analisi costi-benefici – diventa un fattore abilitante per la legittimazione delle scelte strategiche e per la gestione del trade-off tra protezione e produttività (Lee, 2020). Tali strumenti permettono di passare da una logica difensiva e *compliance-oriented* a una prospettiva di valore, in cui la cybersecurity si configura come un vero e proprio capitale organizzativo, da misurare, governare e valorizzare nel tempo.

4 – Cyber insurance: uno strumento per la gestione del rischio informatico

Sebbene l'idea di assicurazione risalga al XIV secolo, il concetto di *cyber insurance* è emerso solo negli anni Duemila come risposta alle emergenti nuove minacce poste dalla digitalizzazione. A partire da quel periodo, le compagnie assicurative hanno introdotto le prime polizze specifiche per coprire i danni derivanti da incidenti informatici, contribuendo a rafforzare la capacità delle organizzazioni di far fronte alle conseguenze economiche, operative e reputazionali degli attacchi *cyber* (Bailey, 2014; Woods & Moore, 2020). L'assicurazione informatica è oggi riconosciuta come un meccanismo di trasferimento del rischio che, integrandosi con le misure

tecniche e organizzative di sicurezza, può incrementare la resilienza complessiva dell'impresa. In particolare, la sottoscrizione di una polizza *cyber* consente di mitigare i costi diretti e indiretti derivanti da attacchi come *ransomware*, *data breach*, frodi digitali e interruzioni di servizio (Franke, 2017). Tra le coperture generalmente offerte si annoverano il rimborso dei costi per il ripristino dei sistemi e dei dati, le spese legali, i risarcimenti a terzi, le consulenze tecniche post-incidente e, in alcuni casi, anche il pagamento del riscatto richiesto dai criminali informatici. Le polizze possono assumere forme generaliste (come estensioni di coperture D&O o property), oppure essere costruite *ad hoc*. Più nello specifico le soluzioni più evolute offrono, oltre alla compensazione finanziaria, anche pacchetti di servizi proattivi, tra cui *audit* di sicurezza, linee guida sulle *best practice*, accesso a strumenti di prevenzione e supporto nella gestione della crisi (MacColl *et al*., 2021).

Questo approccio integrato è particolarmente rilevante per le PMI, che spesso non dispongono di risorse interne dedicate alla *cybersecurity*. A differenza delle assicurazioni tradizionali, la *cyber insurance* presenta specificità legate all'intenzionalità e dinamicità del rischio, in quanto la probabilità di un incidente informatico non dipende solo da eventi aleatori, ma è influenzata direttamente dal comportamento degli attori malevoli. Ciò solleva questioni etiche ed economiche rilevanti. Alcuni autori hanno infatti criticato il ruolo ambiguo dell'assicurazione nella gestione dei *ransomware*: secondo Dudley (2019) e Jenkins e Ventham (2022), la disponibilità di coperture assicurative incentiverebbe i criminali a colpire aziende assicurate, nella convinzione che queste possano pagare più facilmente il riscatto. Al contrario, altri studiosi sottolineano che l'assicurazione rappresenta una risorsa cruciale per garantire continuità operativa, soprattutto nei settori critici (Jenkins & Ventham, 2022; Cluley, 2021). Un caso emblematico è stato quello di Sony, vittima nel 2011 di un grave attacco informatico che le causò danni stimati in 171 milioni di dollari. In quell'occasione, la compagnia assicurativa rifiutò la copertura, sostenendo che la polizza stipulata da Sony fosse limitata ai danni materiali e non contemplasse esplicitamente il rischio informatico. Questo episodio ha evidenziato l'importanza, per le imprese, di definire in modo chiaro i termini e l'estensione delle coperture assicurative (Bailey, 2014).

Oggi, il mercato globale della *cyber insurance* è in forte espansione, trainato dalla crescente digitalizzazione dei processi aziendali e dall'incremento, in termini sia quantitativi sia qualitativi, degli attacchi informatici. Secondo le proiezioni di Statista, il mercato globale dell'assicurazione contro i rischi cyber è destinato a raggiungere quasi 30 miliardi di dollari entro il 2027, partendo da circa 14 miliardi nel 2023 (Statista, 2024). Questa crescita segnala non solo una maggiore consapevolezza da parte delle imprese rispetto all'importanza della protezione informatica, ma anche l'evoluzione dell'assicurazione da strumento residuale a leva strutturale di resilienza organizzativa. La cyber insurance, pertanto, si configura come uno strumento complementare all'interno di una strategia articolata di gestione del rischio. Pur non essendo una soluzione definitiva, essa consente di assorbire parte del rischio residuo e contribuisce a rafforzare la sostenibilità economica delle imprese esposte a minacce digitali sempre più pervasive.

Detto ciò, è bene evidenziare anche che, seppur il mercato della *cyber insurance* è oggi un elemento essenziale, risulta essere comunque incompleto nell'ecosistema della gestione del rischio informatico. Sebbene si siano compiuti progressi notevoli in termini di diffusione, personalizzazione e consapevolezza, permangono criticità rilevanti legate alla standardizzazione delle coperture, all'asimmetria informativa tra assicuratori e assicurati e, soprattutto,

alla mancanza di dati storici attendibili per la corretta modellazione attuariale del rischio (Biener, Eling, & Wirfs, 2015; Eling & Schnell, 2016). In questo contesto, la cooperazione tra settore pubblico e privato risulta fondamentale. I governi, le autorità di vigilanza, le compagnie assicurative e le imprese devono agire in sinergia per creare un sistema di condivisione delle informazioni sugli incidenti informatici, promuovere la trasparenza contrattuale e facilitare la diffusione di prodotti assicurativi più accessibili anche alle PMI e agli studi professionali (ENISA, 2020). Solo così sarà possibile colmare il cosiddetto cyber insurance gap, che oggi rappresenta uno dei principali ostacoli alla costruzione di un tessuto economico realmente resiliente (OECD, 2017). In ultima analisi, la *cyber insurance* non può essere considerata una soluzione isolata, ma deve essere integrata in una più ampia strategia di gestione del rischio che combini prevenzione, rilevazione, risposta e recupero (Woods & Simpson, 2017). Se adeguatamente valorizzata, essa potrà svolgere un ruolo chiave nel rafforzare la continuità operativa.

5 – Discussione

Alla luce di quanto detto fin ora, diventa necessaria una visione integrata della *cybersecurity* nel governo d'impresa, evidenziando come la gestione del rischio informatico non debba più essere relegata a una funzione tecnica o settoriale, ma debba assumere un ruolo strategico trasversale, pienamente incorporato nei meccanismi di controllo direzionale. Le trasformazioni indotte dalla digitalizzazione e dalla crescente pervasività delle minacce informatiche impongono una revisione profonda del ruolo del controllo manageriale, che oggi deve includere indicatori, metriche e processi capaci di rappresentare e mitigare l'esposizione al rischio *cyber* (Simons, 1995; Ferreira & Otley, 2009).

In particolare, l'integrazione della cybersecurity nei sistemi informativi aziendali e nel *risk-based performance management* consente alle imprese di ottenere una visione olistica dei propri *asset* critici, migliorando l'allocazione delle risorse e la tempestività decisionale. Inoltre, le *best practice* internazionali, come quelle contenute nello standard ISO/IEC 27001, insieme alle disposizioni normative come il GDPR, la NIS2 e il DORA, agiscono come catalizzatori di questa evoluzione, spingendo verso un approccio multilivello che combina compliance, gestione proattiva e rendicontazione strutturata (Katsumata *et al*., 2010; Lee, 2021). Uno degli aspetti più innovativi che emerge dal presente contributo è il ruolo della "*cybersecurity by design*" come leva di legittimazione strategica e non solo di tutela operativa.

La sicurezza, in questa prospettiva, diventa parte integrante del valore d'impresa, contribuendo a rafforzare la fiducia degli stakeholder e la reputazione aziendale. Tale trasformazione culturale richiede che le decisioni in materia di sicurezza informatica siano rese visibili e tracciabili attraverso processi di *budgeting, reporting* e pianificazione, in modo da integrarsi pienamente nel ciclo di controllo di gestione. L'adozione di coperture assicurative *cyber*, poi, arricchisce

la strategia di gestione del rischio, fornendo un supporto finanziario concreto in caso di incidente e contribuendo al tempo stesso alla diffusione di pratiche virtuose nella prevenzione di attacchi informatici. Come discusso, tali polizze possono essere strutturate per includere non solo indennizzi economici ma anche supporti operativi e tecnici (Bailey, 2014; Woods & Moore, 2020), configurandosi come strumenti chiave nel disegno di una governance più adattiva e *data-driven*.

In definitiva, emerge un cambiamento paradigmatico, in quanto la *cybersecurity* non è più un "costo da sostenere", ma un investimento strategico che può generare vantaggio competitivo, migliorare la qualità del controllo direzionale e rafforzare la capacità dell'organizzazione di fronteggiare eventi imprevisti. Solo adottando una logica integrata – che unisca framework normativi, strumenti assicurativi e modelli di performance management – sarà possibile costruire imprese realmente resilienti in un contesto digitale ad alta volatilità.

6 – Conclusioni

La crescente digitalizzazione dei processi economici e organizzativi, unitamente alla proliferazione di minacce informatiche sempre più sofisticate, ha reso il rischio informatico una delle variabili critiche della governance aziendale contemporanea. Come evidenziato nel presente contributo, il *cyber risk* non può più essere relegato a una dimensione tecnica della sola funzione IT, ma va integrato nei processi strategici, decisionali e di controllo direzionale dell'impresa.

L'approccio proattivo alla gestione dell'esposizione informatica, supportato da modelli di ERM, framework normativi e strumenti predittivi di *threat intelligence*, consente di anticipare gli scenari di rischio, ottimizzare le risorse e rafforzare la resilienza organizzativa. In tale ottica, il controllo direzionale si configura come un ambito privilegiato per la connessione tra performance e sicurezza, favorendo la costruzione di un sistema informativo integrato, in grado di guidare le scelte di allocazione e monitorare gli impatti dei *cyber risk* sugli obiettivi di business.

Infine, l'emergere di una logica di "cybersecurity by design" che non si limita alla sola introduzione di requisiti tecnici sin dalle prime fasi del ciclo di vita dei sistemi informativi, ma implica una vera e propria trasformazione culturale dell'organizzazione. La sicurezza non è più un'esigenza accessoria da soddisfare *ex post*, bensì è un principio fondante che deve permeare all'intero processo decisionale, influenzando la progettazione dei processi, la definizione dei ruoli organizzativi e la gestione dei dati e delle relazioni con l'ambiente esterno. Tale cambiamento presuppone una maturazione del "*cyber risk awareness*" a tutti i livelli aziendali includendo i vertici direzionali, i responsabili delle funzioni operative e il personale amministrativo. Il rischio informatico deve essere considerato parte integrante del profilo di rischio dell'impresa e governato con strumenti coerenti con il suo impatto potenziale sulla continuità operativa, sulla reputazione aziendale e sulla compliance normativa.

In questo quadro, la sicurezza informatica si configura come leva di valore e legittimazione strategica. Da un lato, consente all'impresa di rispondere efficacemente alle pressioni esterne – normative, competitive e reputazionali – rafforzando la propria accountability e il proprio posizionamento nei confronti di clienti, investitori e istituzioni. Dall'altro, agisce come fattore abilitante della trasformazione digitale sicura, rendendo possibile l'adozione di tecnologie innovative senza compromettere l'integrità e la disponibilità degli *asset* critici.

La fiducia degli stakeholder, in particolare, è oggi fortemente correlata alla percezione della capacità di un'organizzazione di proteggere i dati, gestire le crisi e assicurare la *business continuity*. In tal senso, la cybersecurity diventa un requisito abilitante per la reputazione aziendale, oltre che una garanzia per la qualità e l'affidabilità dei servizi erogati. Studi recenti (es. Mizrak, 2023; Lee, 2021) mostrano che le imprese che adottano un approccio strutturato alla sicurezza informatica, incorporandola nei propri modelli di business, presentano anche migliori performance in termini di resilienza, sostenibilità e capacità di attrarre investimenti.

In un contesto competitivo, volatile e interconnesso, la capacità di gestire il rischio informatico in modo sistemico e trasversale costituisce dunque un vantaggio competitivo durevole. Non si tratta solo di proteggere ciò che si ha, ma di abilitare ciò che si vuole essere: un'organizzazione reattiva, trasparente, affidabile e capace di trasformare la gestione del rischio in una leva strategica per innovare, crescere e differenziarsi.

7 – Bibliografia

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. Accounting, Organizations and Society, *35*(7), 659–675.

Bailey, D. (2014). Cyber insurance and the law of unintended consequences. Journal of Law and Cyber Warfare, *3*(1), 1–18.

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). Developing key risk indicators to strengthen enterprise risk management. *ERM Initiative at North Carolina State University and the Committee of Sponsoring Organizations of the Treadway Commission, Raleigh, NC*.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*(6), 521–531.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance - Issues and Practice, 40*(1), 131–158.

Böhme, R., Christin, N., Edelman, B., Moore, T., & Moore, T. (2018). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 27, 100–109.

Bon, A., Akkermans, H., & Gordijn, J. (2016). Developing ICT services in a low-resource development context. Complex Systems. I*nformatics and Modeling Quarterly,* (9), 84-109.

Brunetti, G. (2012). Il Controllo di Gestione nell'Ottica della Creazione di Valore–Proposta di un percorso di lettura. *Economia Aziendale Online-,* (1), 1-2.

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2022). The changing nature of cyber risk: Evidence from remote work and digital acceleration. *Journal of Management Information Systems, 39*(1), 5–35.

Caserio, C. (2019). Integrated information systems and information systems quality: Prospects for analysis and emerging trends. *Economia Aziendale Online,10*(2), 293-320.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks (Technical Note CMU/SEI-2010-TN-028). Software Engineering Institute, Carnegie Mellon University. In https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9397

Cheng, L., Liu, F., Yao, D., & Hu, H. (2021). Risks and countermeasures for AI-powered cybersecurity attacks. *IEEE Security & Privacy, 19*(4), 63–72.

Cluley, G. (2021). *Cyber insurance: Paying ransoms could make things worse*. Retrieved from https://grahamcluley.com

Clusit. (2025). *Rapporto Clusit 2025 sulla sicurezza ICT in Italia*. Associazione Italiana per la Sicurezza Informatica.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2016). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546.

CRO Forum. (2014). Cyber resilience: The cyber risk challenge and the role of insurance. In https://www.thecroforum.org/cyber-resilience/

CRO Forum. (2016). Conceptualizing and modeling cyber risk,
In https://www.thecroforum.org/conceptualizing-and-modeling-cyber-risk/

CrowdStrike. (2025). Threat intelligence and exposure management. Retrieved from https://www.crowdstrike.com/en-us/global-threat-report/

Damodaran, A., & Amini, M. (2021). "Cybersecurity Strategy in the Age of Digital Risk." *Journal of Management Accounting Research*, *33*(1), 45–68.

Denzin, N. K. (1978). *The research act: A theoretical introduction to sociological methods* (2nd ed.). New York: McGraw-Hill.

Direttiva (UE) 2022/2555 (NIS2)
In https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666.

Dudley, R. (2019). Why cyber insurance is worsening the ransomware crisis. Cybersecurity Review, (8), 45–49.

Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys*, *44*(2), 1–42.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance, 17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

ENISA. (2020). Cyber Insurance: Recent Advances, Good Practices and Challenges. European Union Agency for Cybersecurity.

ENISA. (2023). *Cybersecurity Threat Landscape 2023*. European Union Agency for Cybersecurity, in https://www.enisa.europa.eu/publications

Ferreira, A., & Otley, D. (2009). The design and use of performance management systems: An extended framework for analysis. *Management Accounting Research, 20*(4), 263–282.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security, 68*, 130–144.

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance, 22*(3), 81–88.

Gazzola P, Pavione E, Amelio S., Magrì J (2020). Smart Industry e Sviluppo Sostenibile, Imprese Intelligenti e SDGs 2030. *Economia Aziendale Online, 11*(1), 41-53.

Geneva Association. (2016). *Cyber risk: Risk management principles for the insurance industry*. Retrieved from https://www.genevaassociation.org/research-topics/cyber-risk

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, *19*(2), 1–7.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the cybersecurity investment decision-making process: A multiple-case study of financial organizations. *Information & Management*, *56*(7), 103151.

Huang, Y., Pearce, P., Kannan, S., & Paxson, V. (2019). Understanding email fraud: A large-scale analysis of scam campaigns. *Proceedings of the 28th USENIX Security Symposium*, 3031–3048.

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Wiley-Interscience.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.

Jenkins, R., & Ventham, M. (2022). The paradox of cyber insurance: Risk reduction or risk amplification? Journal of Risk Research, *25*(7), 891–905.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, *90*(6), 48–60.

Katsumata, S., Kawamura, T., & Takanashi, K. (2010). *Security by design: Toward secure software and systems development*. *Journal of Information Processing*, *18*, 142–153.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 3–24.

Kumar, N., Goudar, R. H., & Kumar, M. (2020). Detection and mitigation of application layer DDoS attacks: A review. *Computer Science Review*, 37, 100267.

Lee, A. (2021). Cybersecurity and risk management in the digital era: Emerging frameworks and governance challenges. *Journal of Cybersecurity, 7*(1), taab007.

Livrieri, L. N., & Greco, A. (2025). La gestione proattiva dell'esposizione al rischio per ottimizzare la sicurezza aziendale. In *Rapporto Clusit 2025 sulla sicurezza ICT in Italia*. 336–341.

MacColl, B., Hurley, L., & Pereira, R. (2021). Global Cyber Insurance Market Trends 2021–2027. *Market Research Future*.

Macchia, S. (2019). A review on Management Accounting Change. What's next?. *Economia Aziendale Online-, 10*(1), 107-134.

Mauceri, F. (2016). *Cyber risk: il rischio informatico e le coperture assicurative*. AssiNews, in https://www.assinews.it/07/2016/cyber-risk-rischio-informatico-le-coperture-assicurative/660024235/

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108.

NIST. (2012). *Guide for conducting risk assessments (SP 800-30 Rev. 1)*. National Institute of Standards and Technology.

OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management. Organisation for Economic Co-operation and Development.

Osservatorio Fintech & Insurtech della School of Management del Politecnico di Milano. (2023, 2 gennaio). *Fintech e Insurtech in avanzata*. AssiNews – Il Quotidiano Assicurativo. In https://www.assinews.it/01/2023/fintech-e-insurtech-in-avanzata/660102183.

Provasi, R., & Guizzetti, C. (2019). L'evoluzione dei sistemi di controllo aziendale: dal controllo di gestione al controllo sulla governance. *Economia Aziendale Online-*, *10*(2), 257-271.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6–7), 849–855.

Regolamento (UE) 2022/2554 (Digital Operational Resilience Act – DORA). In https://eur-lex.europa.eu/eli/reg/2022/2554/oj?locale=it.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management*. Springer. https://doi.org/10.1007/978-3-319-23570-7

Rifkin, J. (2019). *Un green new deal globale*. Edizioni Mondadori.

Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.

Statista. (2024). *Cyber insurance market size worldwide from 2020 to 2027*. Retrieved July 7, 2025. In https://www.statista.com/statistics/1127572/global-cyber-insurance-market-size/.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii.

Woods, D., & Moore, T. (2020). Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy, 18*(1), 21–27. https://doi.org/10.1109/MSEC.2019.2948777

Woods, D., & Simpson, A. (2017). Cybersecurity insurance: Modeling and measuring risk posture. *Proceedings of the 2nd International Workshop on Software Assurance*, 29–36.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research, 20*(1), 69–81.

World Economic Forum. (2012). Partnering for cyber resilience: Risk and responsibility in a hyperconnected world.
In https://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*, *15*(4), 2046–2069.

Zhou, Y., Huang, Y., Wang, H., & Huang, H. (2007). Pharming attack and its countermeasures. *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering*, 500–504.