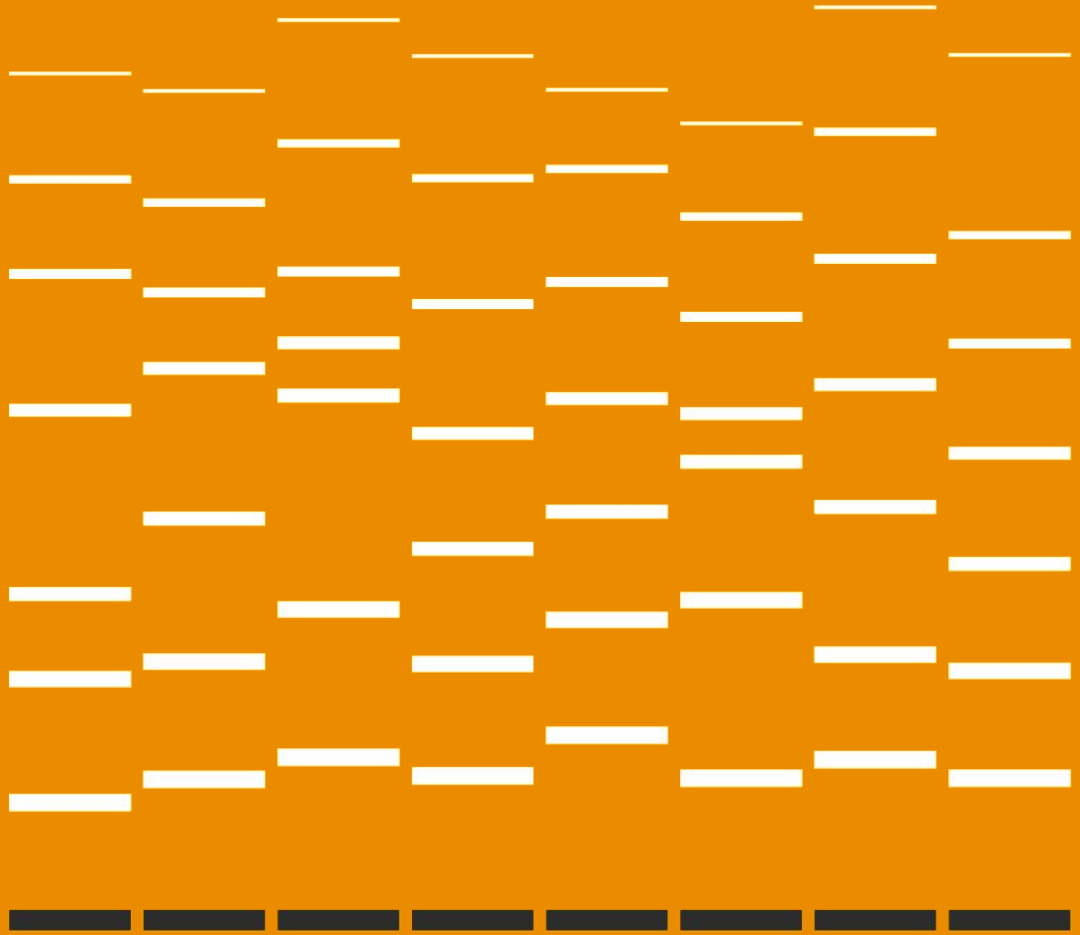
Professionisti, imprese e cybersecurity: rischi e opportunità

20 Febbraio 2024
ODEC, Milano

Nicola Monti, Partner Cyber PwC Italy
Giuseppe D'Agostino, Partner Cyber PwC Italy

pwc



Oggi con voi

Nicola Monti
Partner, PwC Italy
+39 3482504036
nicola.monti@pwc.com
linkedin.com/in/montinicola/

- Presidente PwC Business Services
- Cybersecurity Leader PwC Italy
- Membro PwC Global Cyber Leadership Team
- Dottore Commercialista
- Revisore Contabile
- Certification in Risk Management Assurance

Giuseppe D'Agostino
Partner, PwC Italy
+39 3476466747
giuseppe.dagostino@pwc.com
linkedin.com/in/gdagostino/

- Cybersecurity PwC Italy
- Ingegnere delle Telecomunicazioni (PoliMi)
- Assolombarda Cybersecurity Working Group
- Project Management Professional
- Certified Information Security Manager
- ISO 27001 Lead Auditor

Contenuti

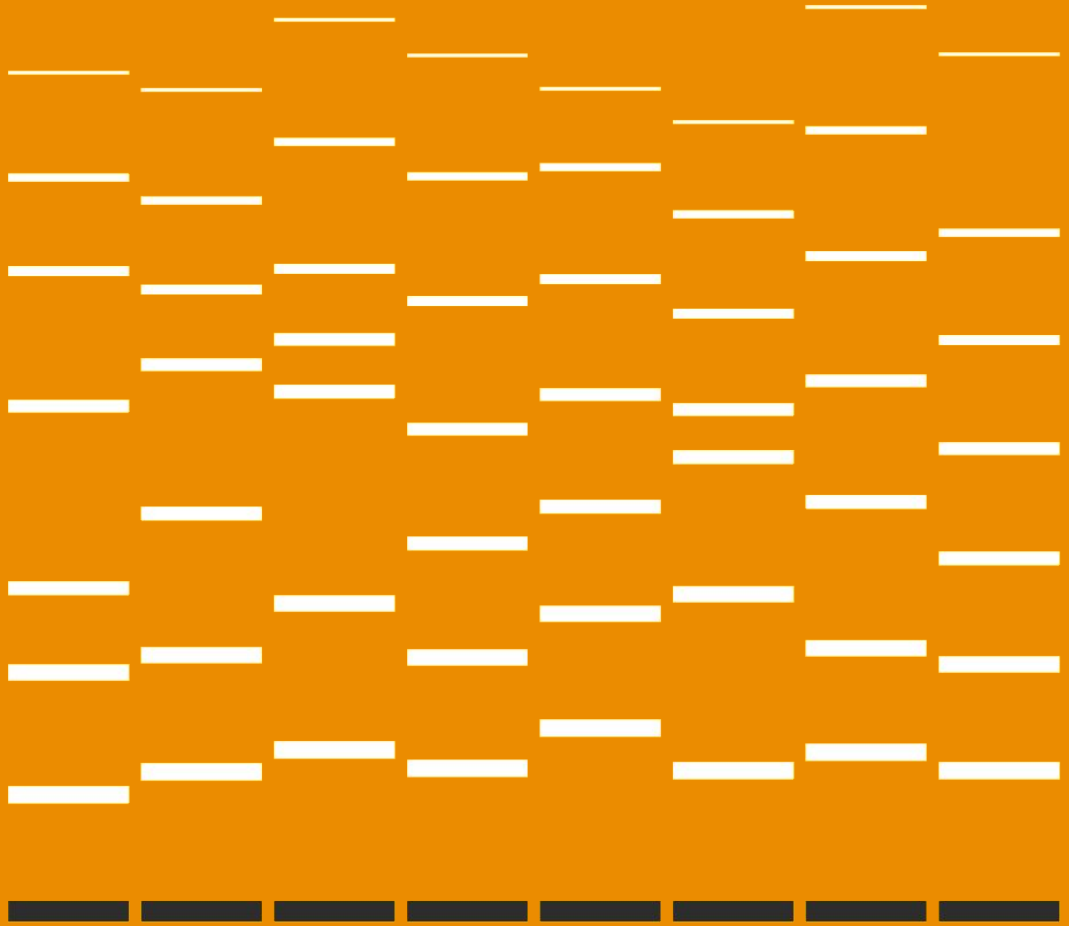
1. L’importanza del sistema di controllo interno anche in ambiente cibernetico
   a cura di Nicola Monti

2. Gli attacchi informatici: quali sono, come colpiscono; esempi di conseguenze dannose e presentazione Survey PwC
   a cura di Giuseppe D’Agostino

3. Conclusioni

1

L’importanza del sistema di controllo interno anche in ambiente cibernetico



Il “Codice della Crisi d’Impresa e dell’Insolvenza”

Il “Codice della Crisi d’Impresa e dell’Insolvenza” introdotto con il D.Lgs. 14/2019 e modificato, da ultimo, con il D. Lgs. n. 83/2022 il 15 luglio 2022, (attuativo della Direttiva UE 2019/1023 c.d. “Direttiva Insolvency”), ha l’obiettivo di favorire l’individuazione tempestiva dei segnali di crisi, al fine di tutelare il valore e **la continuità aziendale nell’interesse dei soggetti coinvolti e del sistema economico in generale**.

Il questo senso quindi: sono stati introdotti **nuovi doveri** per amministratori e **organi di controllo** in tema di **individuazione e valutazione** di **un adeguato assetto organizzativo, amministrativo e contabile** quale **strumento di prevenzione.**

Doveri del collegio sindacale (Art. 2403): Il collegio sindacale **vigila** sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione [2623, n. 3] ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile [2423, 2432] adottato dalla società e sul suo concreto funzionamento.

Responsabilità (Art. 2407, 2c.): Essi sono responsabili solidalmente con gli amministratori per i fatti o le omissioni di questi, quando il danno non si sarebbe prodotto se essi avessero vigilato in conformita' degli obblighi della loro carica.

Il CCII riserva un ruolo centrale all’organo amministrativo attraverso il novato art. 2086 c.c.

Art. 2086.

((Gestione dell'impresa))

L'imprenditore e' il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori.

((L'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuita' aziendale, nonche' di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuita' aziendale)).

Documento di Ricerca CNDCeEC: *Assetti organizzativi, amministrativi e contabili: profili civilistici e aziendalistici*

“”*Tralasciando gli aspetti correlati alla prevenzione della crisi e concentrandoci, ai fini di una corretta impostazione delle problematiche sottese, sulle previsioni che si riferiscono agli* ***assetti organizzativi, amministrativi e contabili****, ovvero sulle idonee misure, che ogni organizzazione imprenditoriale deve predisporre, è opportuno sin da subito evidenziare come* ***le richiamate disposizioni non ne forniscano una definizione****.*”

Il testo del documento subito di seguito però esplicita (pag.5):

“*Nell’ambito dell’attività di gestione, si tratterà di* ***approntare procedure*** *che possano* ***garantire*** *l’efficacia e l’efficienza della gestione dei rischi e del* ***sistema di controllo interno****, nonché la completezza, la tempestività e l’attendibilità dei flussi informativi tra le funzioni della società e tra queste e le funzioni di altre società del gruppo (se esistenti), nonché di individuare indici e parametri segnaletici che consentano di evidenziare segnali di allarme (al fine della emersione anticipata della crisi).*”

PRINCIPIO DI REVISIONE INTERNAZIONALE (ISA Italia) 315

- Appendice 3: La comprensione del sistema di controllo interno dell'impresa -

Componenti del sistema di controllo interno dell'impresa

1. **L'ambiente di controllo**: *L'ambiente di controllo include le attività di governance e di direzione nonché l'atteggiamento, la consapevolezza e le azioni dei responsabili delle attività di governance e della direzione riguardo al sistema di controllo interno ed alla sua importanza all'interno dell'impresa*.
2. **Il processo adottato dall'impresa per la valutazione del rischio**: ***Il processo adottato dall'impresa per la valutazione del rischio è un processo iterativo per l'identificazione e l'analisi dei rischi finalizzato al raggiungimento degli obiettivi dell'impresa e rappresenta la base con cui la direzione o i responsabili delle attività di governance determinano i rischi da gestire****.*
3. **Il processo adottato dall'impresa per monitorare il sistema di controllo interno**: *Il processo adottato dall'impresa per monitorare il sistema di controllo interno è un processo continuo per valutare l'efficacia del sistema di controllo interno dell'impresa e adottare tempestivamente le azioni correttive necessarie*.
4. **Il sistema informativo e la comunicazione**: *Il sistema informativo rilevante ai fini della redazione del bilancio è costituito da attività e direttive, registrazioni contabili e di supporto, configurate e stabilite al fine di rilevare, registrare ed elaborare le operazioni dell'impresa (...); elaborare e rendicontare le forzature sui sistemi o le elusioni dei controlli; (...)*.
5. **Le attività di controllo**: *(...) Tali controlli includono i controlli sulle elaborazioni delle informazioni e i controlli generali IT (...).*

Il processo adottato dall'impresa per la valutazione del rischio

I rischi rilevanti ai fini di un'informativa finanziaria attendibile includono eventi, operazioni o circostanze **esterni** ed interni che possono manifestarsi ed influenzare negativamente la capacità dell'impresa di rilevare, registrare, elaborare e riportare informazioni economico-finanziarie in modo coerente con le asserzioni della direzione nel bilancio. La direzione può avviare piani, programmi o azioni per fronteggiare rischi specifici o può decidere di accettare un rischio a causa dei costi o di altre considerazioni. I rischi possono emergere o modificarsi in seguito a circostanze quali:

- *Cambiamenti nell'ambiente operativo.* I cambiamenti nella regolamentazione, nell'ambiente economico o operativo possono modificare le pressioni concorrenziali e generare rischi completamente differenti.

- *Personale neoassunto o nuovo nella funzione*. Il personale neoassunto o nuovo nella funzione può focalizzare o comprendere il sistema di controllo interno dell'impresa in modo differente.

Il processo adottato dall'impresa per la valutazione del rischio
(continua)

- *Sistema informativo nuovo o aggiornato*. **Significativi e rapidi cambiamenti nel sistema informativo possono modificare il rischio relativo al sistema di controllo interno dell'impresa**.

- *Crescita rapida*. Un'espansione rapida e significativa delle attività operative può mettere a dura prova i controlli ed aumentare il rischio di un loro mancato funzionamento.

- *Nuova tecnologia*. **Incorporare nuove tecnologie nei processi di produzione o nel sistema informativo può modificare il rischio associato al sistema di controllo interno dell'impresa**.

- *Nuovi modelli di business, nuovi prodotti o nuove attività*. **Entrare in aree di attività od operazioni in cui l'impresa ha poca esperienza può introdurre nuovi rischi associati al sistema di controllo interno dell'impresa**.

Il processo adottato dall'impresa per la valutazione del rischio
(continua)

- *Ristrutturazioni aziendali*. Le ristrutturazioni possono essere accompagnate da riduzione di personale e da cambiamenti nella supervisione e separazione delle funzioni che possono modificare il rischio associato al sistema di controllo interno dell'impresa.
- *Incremento delle attività estere*. L'incremento o l'acquisizione di attività estere comporta nuovi e spesso peculiari rischi che possono influenzare il controllo interno, per esempio, rischi ulteriori o modificati derivanti da operazioni in valuta estera.
- *Nuovi pronunciamenti in materia contabile*. L'adozione di nuovi principi contabili o cambiamenti nei principi contabili possono influenzare i rischi di redazione del bilancio.

- *Utilizzo dell'IT*. Rischi connessi:

  o al **mantenimento dell'integrità dei dati** e delle **elaborazioni** delle informazioni;

  o ai rischi per la strategia aziendale dell'impresa che emergono se essa non è supportata in modo efficace dalla strategia IT dell'impresa; ovvero

  o a **cambiamenti** o **malfunzionamenti** nell'ambiente IT dell'impresa o all'avvicendamento del personale IT o a **mancati aggiornamenti necessari all'ambiente IT** o alla **mancata tempestività di tali aggiornamenti**.

Ambiente IT *PRINCIPIO DI REVISIONE INTERNAZIONALE (ISA Italia) 315*

Definizione: Le applicazioni IT e l'infrastruttura IT di supporto, così come i processi IT e il personale addetto a tali processi, che l'impresa utilizza a supporto delle proprie attività operative e per la realizzazione delle proprie strategie. Ai fini del presente principio di revisione:

i. Un'applicazione IT è un programma o una serie di programmi utilizzati nella rilevazione, registrazione, elaborazione e rendicontazione delle operazioni o delle informazioni. Le applicazioni IT includono data warehouse e report writers.

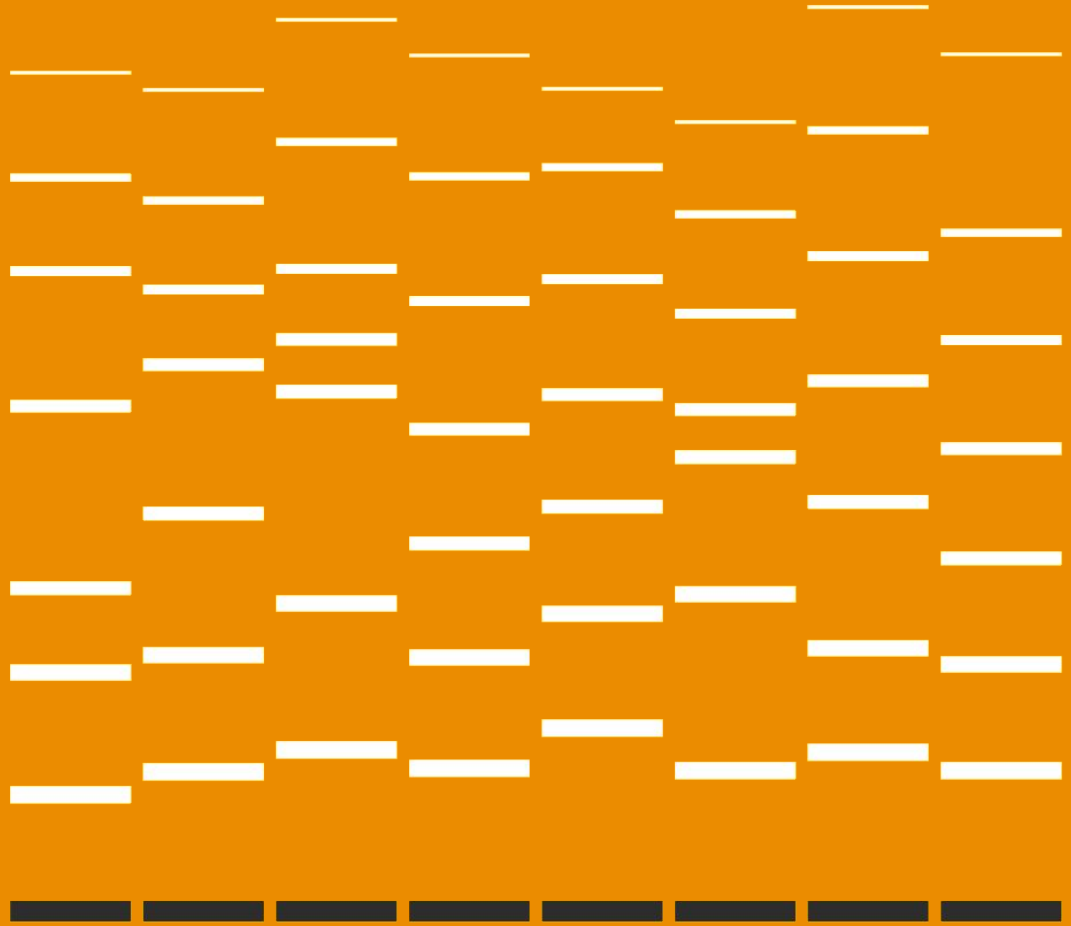
ii. L'**infrastruttura IT** include **la rete**, i **sistemi operativi** e i **database** con i relativi **hardware e software**.

iii. I processi IT sono i processi dell'impresa per gestire l'accesso all'ambiente IT, gestire i cambiamenti nei programmi o nell'ambiente IT e gestire le operazioni IT.

In sintesi: **la tecnologia è ormai pervasiva in ogni aspetto della gestione d'impresa e un'adeguata gestione degli aspetti di protezione della stessa è imprescindibile dal concetto di continuità aziendale.**

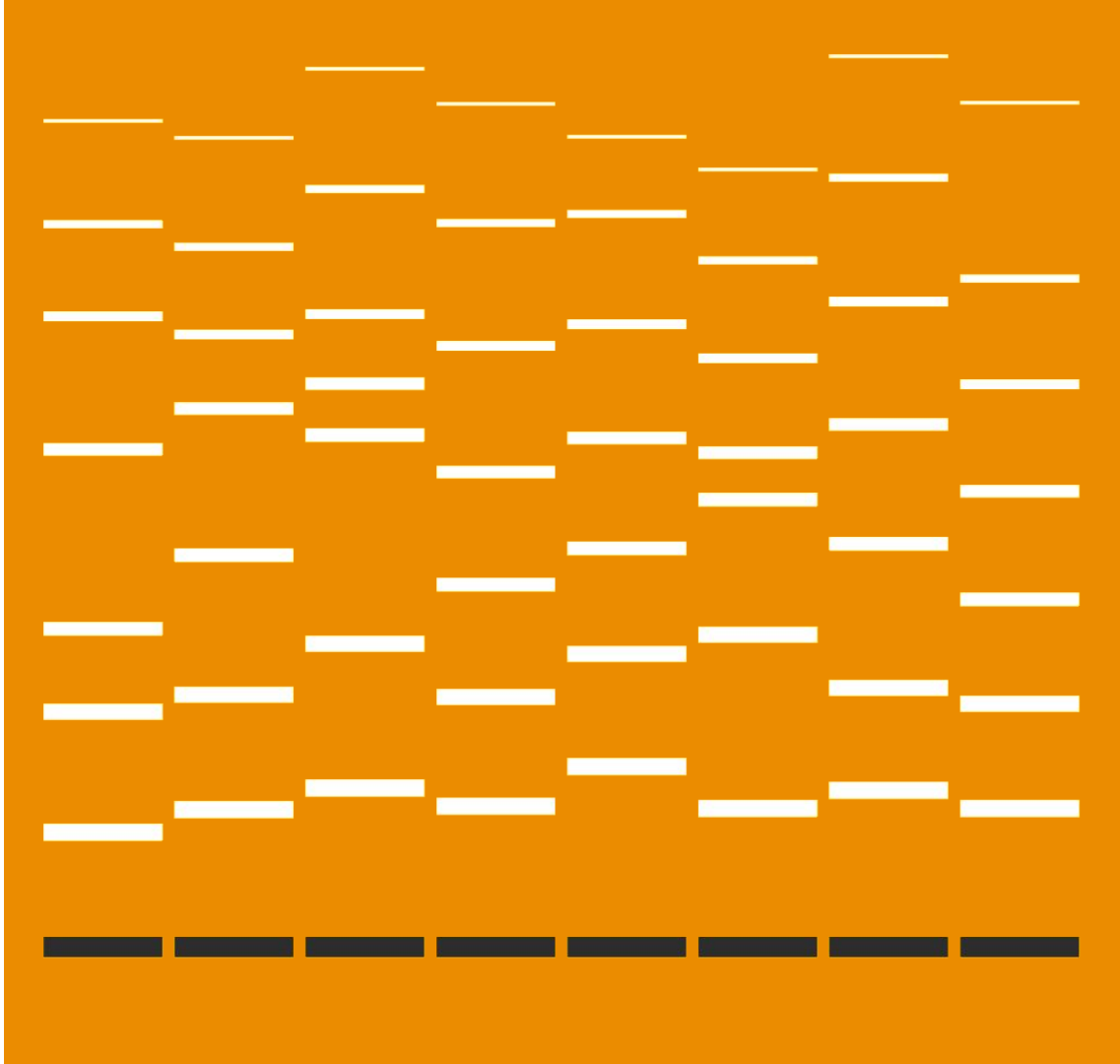
2

Gli attacchi informatici: quali sono, come colpiscono; esempi di conseguenze dannose e presentazione Survey PwC



2.1

Il contesto Cyber



A Dicembre 2023 una operazione dell'Interpol contro il cyber crime ha portato al sequestro di circa 300 milioni di dollari

*"Il sequestro di 300 milioni di dollari rappresenta una somma impressionante e illustra chiaramente l'**incentivo che sta dietro l'attuale crescita esplosiva** della criminalità organizzata transnazionale. Questo vasto accumulo di ricchezza illegale rappresenta una seria minaccia alla sicurezza globale e **indebolisce la stabilità economica delle nazioni in tutto il mondo**."*

Stephen Kavanagh, Direttore esecutivo dei servizi di polizia dell'INTERPOL

Il Cybercrime oggi è una questione globale che interessa privati, aziende e pubbliche amministrazioni

Crescono i costi

~$2T

Costo stimato del crimine informatico attuale, in crescita rispetto ai circa 400 miliardi di dollari nel 2015.

Impatti più seri

$265B

Costo stimato dei danni globali causati dai ransomware nel 2031, in crescita rispetto ai 20 miliardi di dollari nel 2021 a causa della maggiore frequenza e gravità degli attacchi che possono influire sulle operazioni.

Errore umano

82%

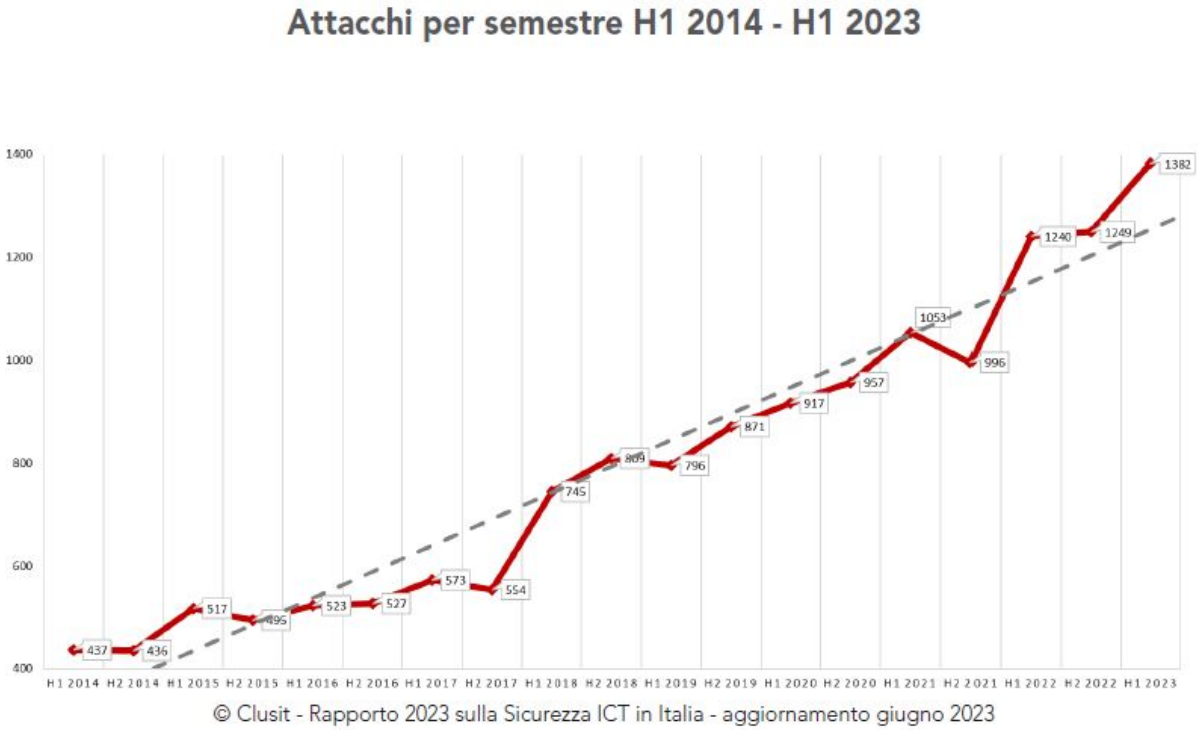
Degli attacchi informatici sono dovuti a errori umani e non vulnerabilità o malfunzionamenti tecnologici.

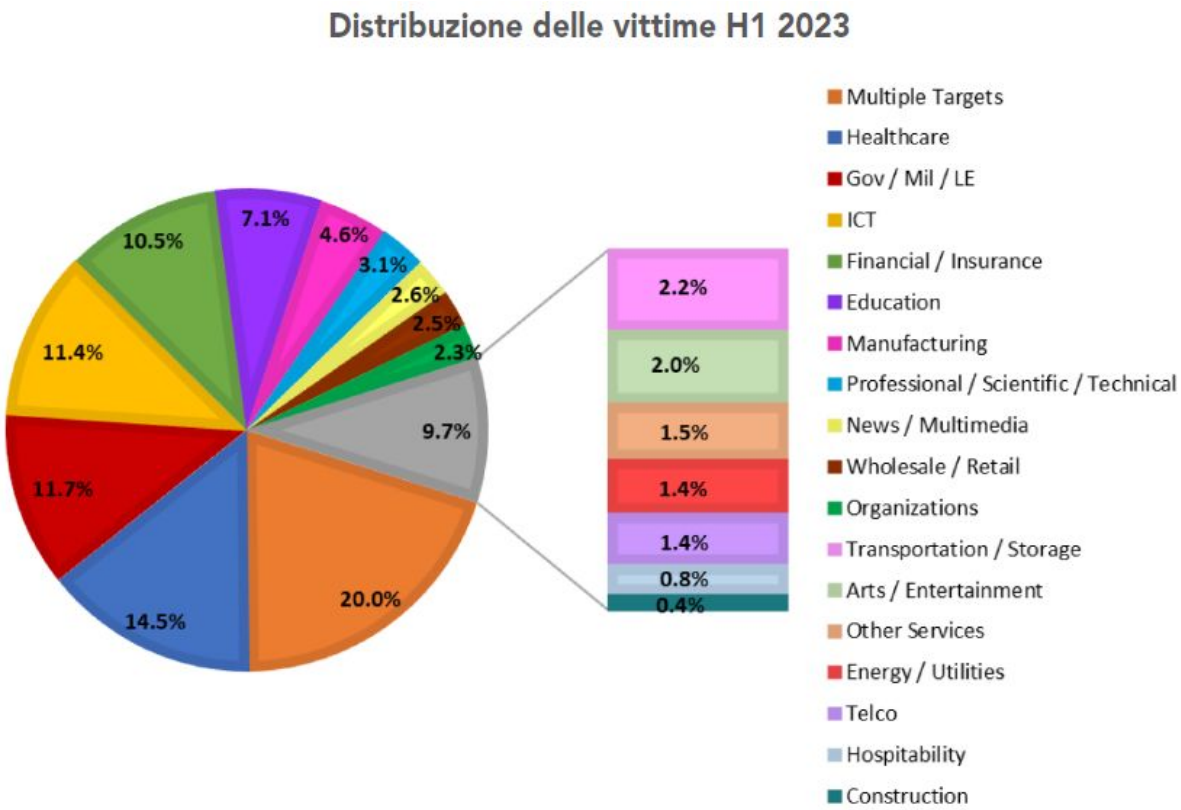
Gap di protezione

84%

Delle aziende non mitigano efficacemente i rischi informatici legati alle terze parti.

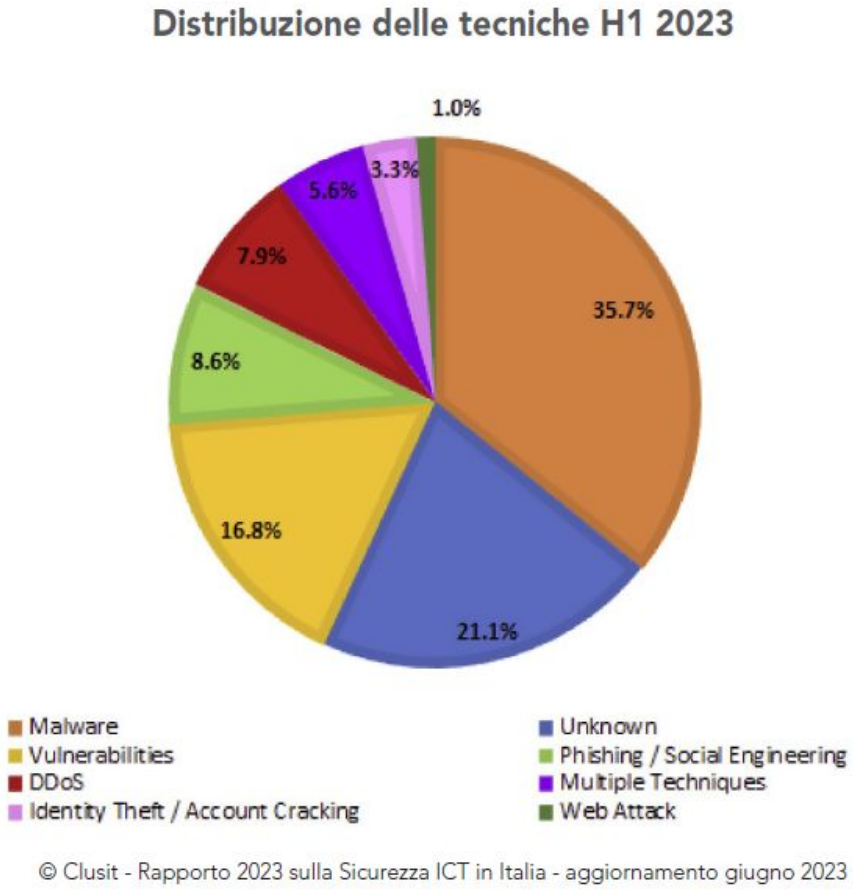
In Italia assistiamo a partire dal 2014 a una **crescita lineare** del numero di attacchi che sono **triplicati in 10 anni**





Le **vittime** in Italia appartengono a **tutti i settori industriali**, con un'incidenza molto alta nell'ultimo periodo di *sanità* e *settore pubblico*

Anche le **tecniche di attacco** sono molteplici, tra le principali l'utilizzo di **malware** e lo sfruttamento di **vulnerabilità dei sistemi**



Tattiche e tecniche di attacco più diffuse (1/3)

Phishing

Una **mail di Phishing** è creata in maniera tale da spingerti a fornire informazioni o cliccare su link/allegati che avviano malware sul tuo device.
Gli elementi principali del phishing sono: un'**entità** che viene **simulata**, un sito o un **contenuto malevolo** con il quale è richiesto di interagire e la richiesta di **disvelamento** delle proprie informazioni.

Spear Phishing

Mentre nel phishing i metodi possono consistere nell'inviare e-mail di massa ad individui casuali, lo **Spear Phishing** si concentra su **obiettivi specifici** e coinvolge **ricerche preliminari**. Viene in genere utilizzato nelle campagne di attacco mirate per accedere all'account o impersonare degli individui specifici.

Business E-mail Compromise (BEC)

Una **Business E-mail Compromise (BEC)** è un tipo di phishing mirato a frodi finanziarie in cui viene particolarmente sfruttato l'elemento fiducia per richiedere transazioni monetarie. Gli elementi principali sono: l'**impersonificazione** avanzata in modo studiato tramite l'uso di parole ed espressioni plausibili; la **fiducia**, poiché tramite la compromissione della mail di un contatto fidato, la vittima ritiene veritiero il mittente ed infine lo stress provocato dall'**urgenza** della richiesta che risulta sempre immediata.

Tattiche e tecniche di attacco più diffuse (2/3)

Vishing

Una **Vishing call** è una **chiamata** effettuata per spingerti a fornire informazioni o uploadare malware sul tuo device.

Smishing

Lo **Smishing** è la tecnica nella quale viene utilizzato un **sms** per spingerti a fornire informazioni o cliccare su link che avviano malware sul tuo device.

QRishing

Il **QRishing** avanza l'attacco tramite la **scannerizzazione dei QR code.**

Tattiche e tecniche di attacco più diffuse (3/3)

Brute-force

Il **Brute-force** è una tecnica per **individuare la password** attraverso l'utilizzo di tutte le combinazioni possibili di caratteri. Richiede molto tempo viste le numerose combinazioni da testare, che aumentano all'aumentare della lunghezza della password, tuttavia potenzialmente è in grado di scoprire qualsiasi password poiché effettua una ricerca esaustiva tra quelle possibili.

Attacco a dizionario

L'**attacco a dizionario** è una variante dell'attacco brute-force che consiste nel **testare** come password **combinazioni di parole comunemente utilizzate**. Ha successo quando la password da scoprire è corta e poco originale, ovvero composta da combinazioni di parole comuni (p.e. Iloveyou, etc.) o semplici (p.e. 12345, password; etc.).

Attacchi DDoS

Un **DDos «Distribute Denial of Services»** è un **attacco informatico** che cerca di **mettere in sovraccarico di richieste una macchina**, fino a rendere impossibile l'erogazione dei servizi richiesti. I cybercriminali sovraccaricano i siti web dell'organizzazione attaccata con traffico di tutti i tipi e creano una mail di phishing rivolta ai dipendenti per tentare di installare un programma malevolo con lo scopo di bloccare i sistemi.

Il Phishing consiste nell'inviare e-mail che contengono file malevoli o che inducono il destinatario a compiere azioni errate

1. L'attaccante individua la ***vittima***.

2. L'attaccante prepara il ***contenuto*** della mail e la invia alla vittima.

3. La vittima cade nella «trappola» ed ***esegue*** le azioni richieste.

Vittime più comuni

- C-levels e executive
- Legale
- Risk & Compliance
- R&D

Contenuti più comuni

- «Autorizzami un bonifico»
- «L'IBAN del fornitore è cambiato»
- Malware su Macro Office
- Link a Siti Web malevoli

Il **50%** delle volte* le vittime fanno click sui link di Phishing.

* Sorgente: Verizon Data Breach Investigation Report 2015

Le mail risultano anche il vettore d'attacco preferito dai frodatori per impersonificare figure aziendali apicali ai fini di estorsione nell'ambito della così detta *CEO Fraud*

Il frodatore dopo uno studio preventivo volto a scoprire iter e ruoli aziendali, passa all'attacco **impersonando una figura responsabile** d'azienda.

Il frodatore invia una falsa mail all'operatore contabile dell'azienda **richiedendo il versamento di un bonifico** ad un conto corrente indicato nel testo.

L'attaccante utilizza termini specifici per **mettere pressione** sulla vittima e instaurare un rapporto di confidenza che lo convinca che la transazione richiesta è autorizzata

L'operatore, **fidandosi dell'autenticità della richiesta**, procede al versamento della somma.

I target non sono solo i C-Level, ma anche tutti i dipendenti che hanno accesso a informazioni pregiate e possono eseguire transazioni di pagamento.

Il conto corrente è in realtà associato all'attaccante che così raggiunge il suo scopo.

Il Ransomware è una delle minacce più rilevanti per la maggior parte delle organizzazioni

Invio di mail di Phishing

Apertura allegato

Cifratura dei dati e richiesta riscatto

72 ore rimaste

Dopo 72 ore non sarà più possibile recuperare i file. «To pay or not to pay?»

Prima di rispondere ad una e-mail, è bene controllare una serie di aspetti

Fare attenzione allo **stile di scrittura** del messaggio (p.e. errori grammaticali e di ortografia).

Verificare **l'indirizzo e-mail** del mittente (p.e. non è interno all'azienda).

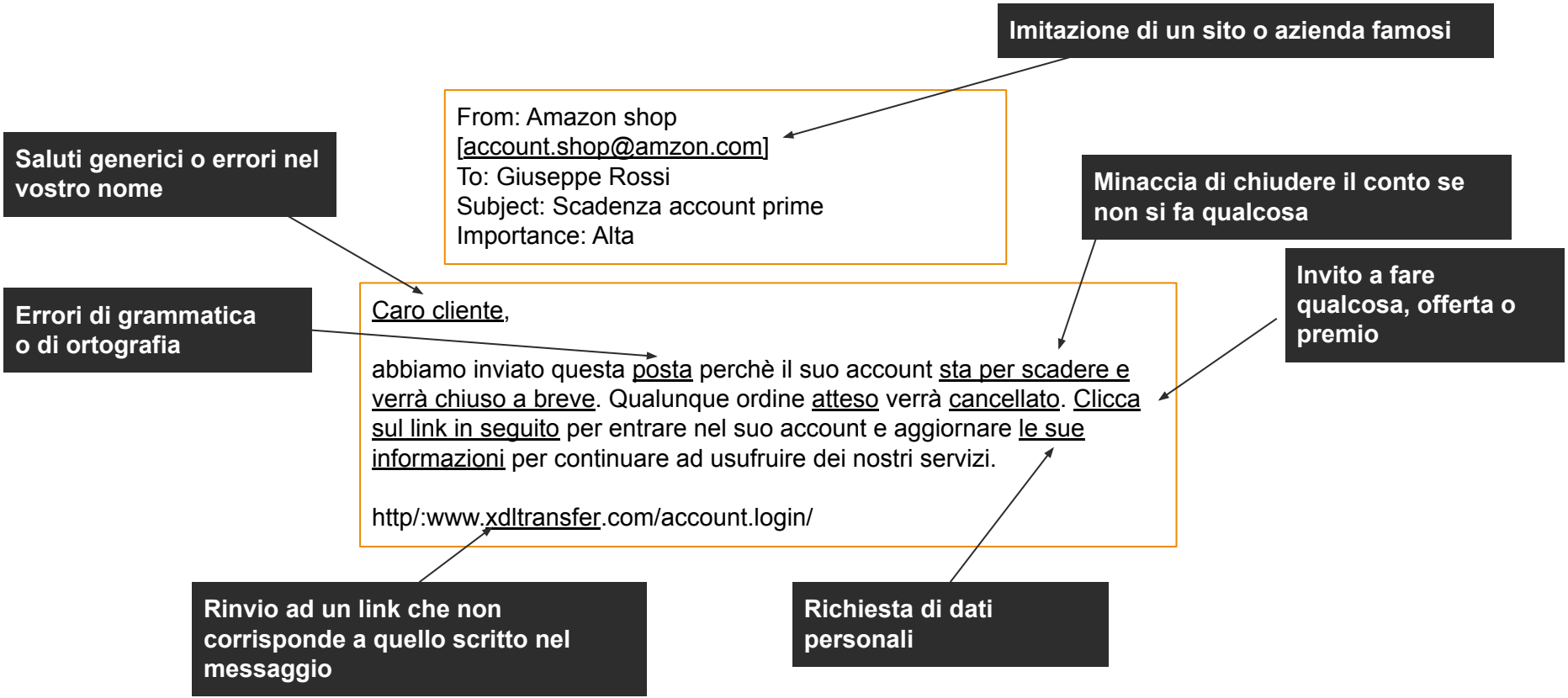
Verificare **l'autenticità** del messaggio (p.e. il provider è sconosciuto).

Investire in **tecnologie** Anti-Phishing.

Verificare **gli allegati** (p.e. allegati inaspettati e estensione dei file inusuale).

Interpretare i **punti di attenzione** (p.e. richiesta di inserimento urgente di informazioni o vincita di premi).

Come riconoscere una mail di phishing



La compromissione della password è spesso il primo tentativo di un attaccante per accedere ad un sistema

Password	Bruteforce speed		
	Fast Desktop PC	Fast GPU	Medium size botnet
Luglio	0 second	0 seconds	0 seconds
Lugl10	2 seconds	0 seconds	0 seconds
Luglio2022	4 seconds	1 seconds	0 seconds
Luglio2022!	4 minutes	20 seconds	5 seconds

È necessario proteggere le identità digitali attraverso password complesse e meccanismi di autenticazione a più fattori

Cosa devo evitare quando creo una password?

- Ricorda sempre che i cybercriminali usano tool sofisticati per poter decifrare le tue password, evita di utilizzare password troppo semplici
- Evita l'utilizzo di parole da dizionario (es. Luglio!21) e afferenti all'account (es. Instagram123!)
- Parole comuni o frasi comuni con la sostituzione di lettere e numeri (es. Acc3550S1cur0!)
- Non usare mai il termine password o derivazioni di esso (es. pwd2021!, p455w0rd!, ecc…)
- Sequenze di lettere o numeri adiacenti sulla tastiera (es. qwerty1234)
- Informazioni personali (es. nomi di familiari, date di compleanno o informazioni simili).
- informazioni pubbliche conosciute (es. città, squadre sportive, ecc …)

Cosa posso fare per rendere la mia password ancora più sicura

Utilizza parole o combinazioni di parole che siano difficili de identificare e ricondurre ad un significato. La password migliore? Robusta e facile da ricordare:

- scegli una password il più lunga possibile
- scegli 4 o meglio 6 parole non correlate tra loro e usa la tua immaginazione per ricordarle
- aggiungi lettere maiuscole, caratteri speciali e numeri

Abilita l'MFA (MultiFactor Authentication) sempre dove possibile. Se pensi che il tuo account sia stato compromesso, cambia immediatamente la password

Nel dark web è possibile trovare credenziali compromesse

SURFACE WEB
La parte accessibile del web che tutti conosciamo.

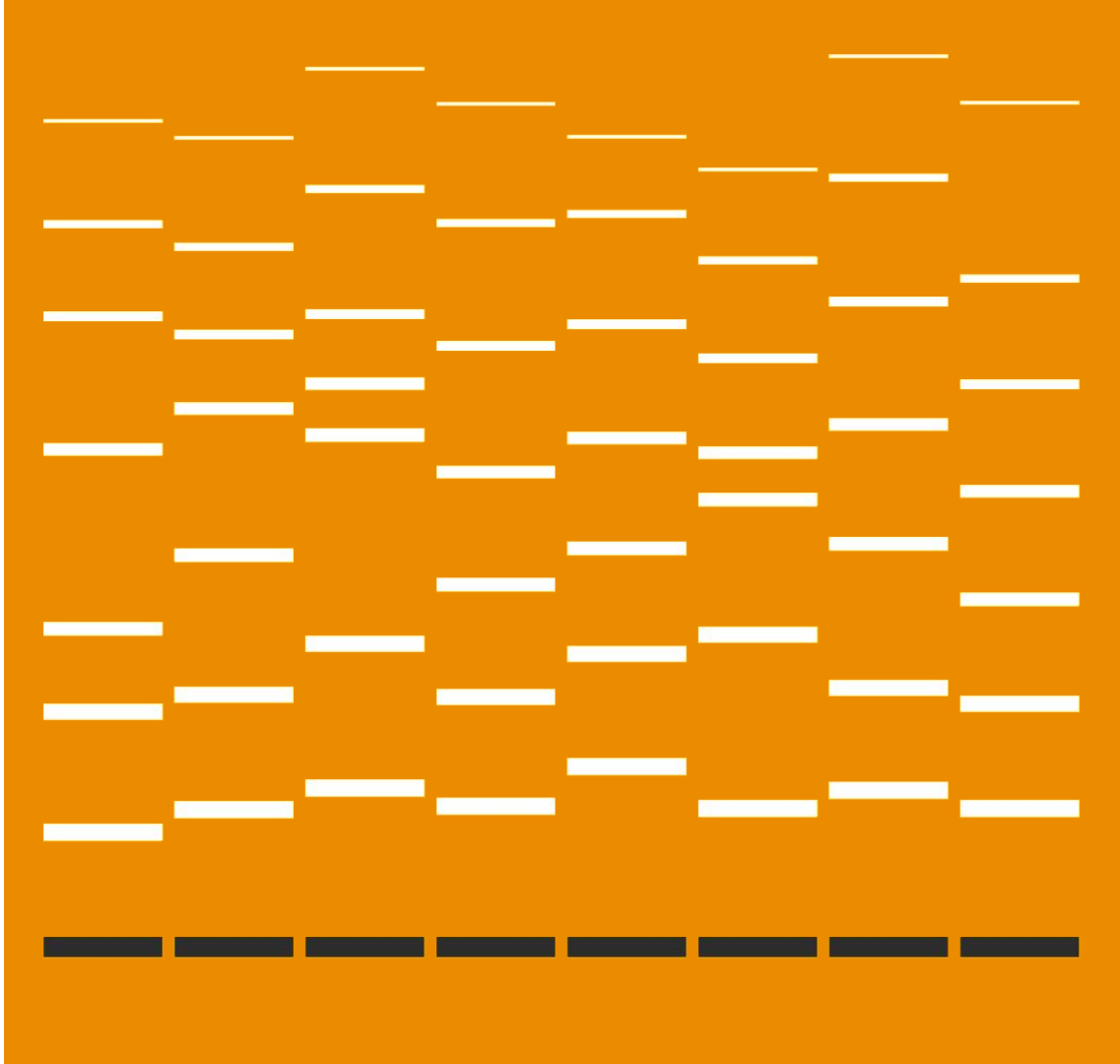
DEEP WEB
Accessibile ma non indirizzato dai motori di ricerca.

DARK WEB
Accessibile solo con particolari browser (es. Tor).

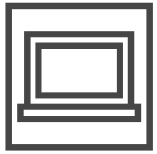
- Contatti
- Documenti d'identità
- Credenziali d'accesso, AaaS
- Documenti riservati
- Carte di credito
- Malware/ RaaS
- Botnet
- Hacking tool vari
- 0-day

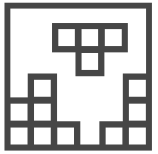
2.2

I rischi Cyber sul tavolo dei responsabili amministrativi



Gli attaccanti agiscono spinti da diverse motivazioni e adottando svariate tecniche



Chi?	Criminali	Hacktivisti	Stati / Nazioni	Insider
Perché?	**Per soldi**	**Per ideologia**	**Per segreti**	**Per vendetta / per vantaggio competitivo**
Come?	• Propagazione dei virus • Attacchi di ingegneria sociale • Furto di informazioni di valore	• Alterazione siti web per propaganda • Interruzione dei servizi web • Divulgazione di informazioni personali dei dipendenti	• Sottrazione di informazioni sensibili • Utilizzo di risorse «illimitate»	• Utilizzo di risorse interne come piattaforma di attacco • Divulgazione di informazioni riservate • Attacchi di ingegneria sociale
Impatti?	• Perdita di denaro • Danni di immagine • Interruzione del business	• Danni di immagine • Interruzione del business	• Perdita di competitività • Danni di immagine	• Perdita di clienti • Perdita di competitività • Danni di immagine • Interruzione del business

Normative in ambito Cybersecurity e Data Protection

Cybersecurity embedded in SEC e CONSOB a seguito dei recenti sviluppi rispetto agli attacchi Cyber

SEC e **Consob** hanno rappresentato l'esigenza di includere l'**informativa sulla cybersecurity** nella **rendicontazione periodica** obbligatoria **resa al mercato** e di **prevedere** all'interno dei **CdA** risorse con **competenze specifiche** in questo ambito.

Principali Normative di settore

Direttiva NIS/NIS2
Network & Information Security

eIDAS
Electronic IDentification Authentication and Signature

PSNC
Perimetro di sicurezza nazionale cibernetica

Decreto-legge 21 settembre 2019, n. 105

GDPR
General Data Protection Regulation

DORA
Digital Operational Resilience Act

PSD2
Payment Services Directive

Direttiva CER
Critical Entities Resilience

La Consob, in collaborazione con altre autorità finanziarie, sta inoltre lavorando a una proposta di **classificazione comune** degli **incidenti cibernetici** per stabilire principi e tassonomia condivisa, al fine di **armonizzare** le segnalazioni di incidenti da parte delle entità finanziarie.

Standard e best practice per proteggersi

Best practices

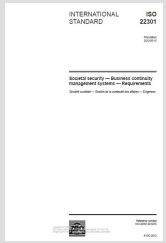
Misure Organizzative (alcuni esempi)

- IR Framework, Playbooks & Communications
- IR Retainer Subscription
- Cybersecurity Insurance
- Cyber Threat Modelling
- Ransomware Attack Simulation & Cyber Security Awareness

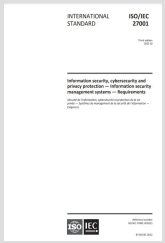
Misure Tecniche (alcuni esempi)

- Multi Factor Authentication
- Endpoint Detection & Response
- Secured and Encrypted Backup & Testing
- E-mail filtering

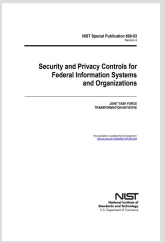
ISO 22301
Continuità Operativa



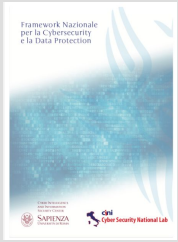
ISO 27001
Sicurezza delle Informazioni



NIST SP 800
Framework per la cybersecurity

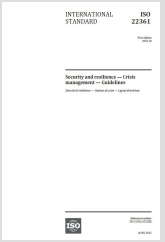


Framework Nazionale 2.0
Cybersecurity e Data Protection



GDPR
Data Protection

ISO 22361
Crisis Management



Trasferimento del rischio Cyber: le assicurazioni

Stimoli all'adozione di polizze cyber

- Numero crescente di incidenti informatici.
- Continua trasformazione digitale.
- Compliance a standard e normative.

Limiti all'adozione di polizze cyber

- Bassa consapevolezza del rischio (lato domanda e offerta, anche relativamente a sottoscrittori).
- Bassa fiducia nel mercato (practice di mercato non consolidata e offerta poco standardizzata).

Caratteristiche del mercato

- Coperture comuni: interruzione dell'attività, ripristino dei dati, estorsioni informatiche.
- Servizi ancillari (anche fornitori esterni): consulenza, legali, gestione delle crisi e prevenzione (corsi di formazione, test di penetrazione e scansione dei sistemi) – anche opzionali.

Principali sfide

- Prezzi percepiti alti da parte del cliente.
- Insufficiente livello di comprensione dei prodotti offerti.
- Mancanza di chiarezza sulle esigenze delle aziende, in particolare per le PMI.
- I singoli clienti non comprendono i vantaggi dell'assicurazione cyber a meno che non venga fornita assistenza IT.

GenAI: opportunità e rischi Cyber

69%

Più di due terzi (69%) affermano che utilizzeranno GenAI per cyber defence nei prossimi 12 mesi.

47%

Quasi la metà (47%) lo sta già utilizzando per il rilevamento e la mitigazione del rischio informatico.

21%

Un quinto (21%) sta già riscontrando vantaggi nei propri programmi grazie a GenAI, a pochi mesi dall'adozione.

Perdita di informazioni riservate

Misure di sicurezza dei dati non adeguate possono esporre pubblicamente i trade secret dell'azienda e altre informazioni proprietarie, nonché i dati dei propri clienti. La mancata revisione approfondita degli output della GenAI può comportare imprecisioni, violazioni di compliance e di contratti (inclusi copyright) e danni reputazionali alla reputazione.

Phishing and deepfakes factories

Misinformation and disinformation

Malware

Secondo la polizia di Hong Kong, un impiegato di una multinazionale è stato indotto con l'inganno a pagare **25 milioni di dollari a dei truffatori che utilizzavano la tecnologia deepfake** fingendo di essere il CFO in una videoconferenza.

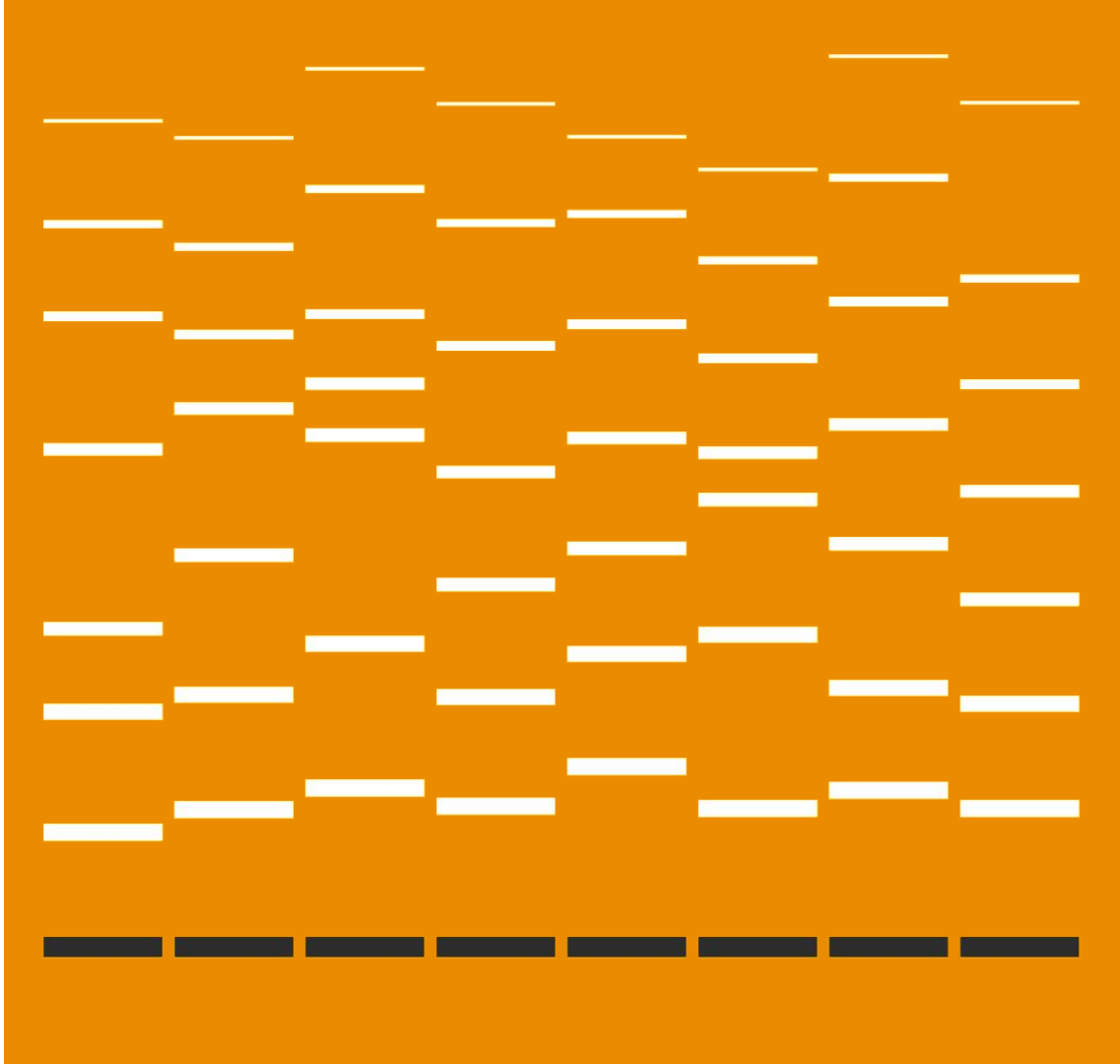
Il dipendente si è insospettito dopo aver ricevuto un messaggio che presumibilmente proveniva dal direttore finanziario della società con sede nel Regno Unito.

Poichè si parlava della necessità di effettuare una transazione segreta, il dipendente ha inizialmente sospettato che si trattasse di una email di phishing.

Tuttavia ha messo da parte i suoi dubbi iniziali dopo la videochiamata perché **le altre persone presenti avevano l'aspetto e il tono dei colleghi con cui aveva già collaborato**.

2.3

I risultati della PwC Digital Trust Insight Survey



2024 Global Digital Trust Insights: Il più longevo e più grande sondaggio del suo genere

3,876

La gamma più ampia di rispondenti esecutivi: dirigenti aziendali, tecnologici e di sicurezza inclusi CEO, Consiglio, CFO, CISO, CIO, CTO

71 paesi

W. Europa (32%), N. America (28%), Asia Pacifica (18%), America Latina (10%), E. Europa (5%), Africa (4%), Medio Oriente (3%)

67%

Aziende con ricavi di 1 miliardo e più

26° anno

Della relazione globale sulla sicurezza informatica di PwC

Accedi al rapporto completo su www.pwc.com/dti

Leggi una funzione speciale su Generative AI per la difesa cyber

Compila il nostro sondaggio "sempre attivo" per ottenere un rapporto di benchmarking DTI

Risultati chiave

1. **I rischi principali — rischi digitali e tecnologici, e rischi cyber — sono intrecciati**, richiedendo ai CISO e ai leader tecnologici di posizionarsi al centro dell'innovazione nelle loro organizzazioni.
2. **La proporzione di violazioni cibernetiche costose ($1m+) è aumentata** rispetto all'anno scorso.
3. **Cloud, cloud, cloud.** Minaccia più preoccupante (47%). Priorità massima per gli investimenti in cyber sicurezza (33%). Eppure mal gestito.
4. **Gli investimenti in sicurezza informatica sono una priorità.** I budget per la sicurezza informatica nel 2024 stanno aumentando e ad un ritmo superiore rispetto all'anno scorso.
5. **Molte aziende riportano attività per trasformare il cyber nei loro organizzazioni,** ma solo circa un quarto sta realizzando benefici.
6. **Semplificazione in corso.** Il passaggio a soluzioni tecnologiche integrate o suite è in aumento.
7. **DefenseGPT:** Le organizzazioni si stanno preparando a implementare strumenti AI generativi per la difesa cibernetica.
8. **Regolamento.** I leader aziendali e tecnologici vedono varie regolamentazioni come utili per garantire la crescita futura. Prevedono costi di conformità aggiuntivi e una significativa trasformazione aziendale.
9. Le **organizzazioni di maggior successo**, che mostrano una maggiore maturità nelle loro iniziative di sicurezza informatica, riportano un maggior numero di benefici e una minore incidenza di costose violazioni cibernetiche.

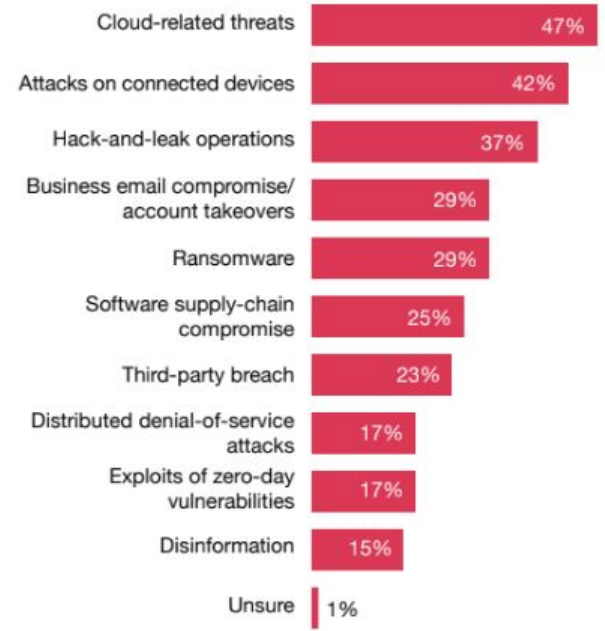
Le principali minacce informatiche nei prossimi 12 mesi

47%

sono maggiormente preoccupate per gli attacchi legati al cloud. Tra gli utenti di fornitori di cloud ibrido, il 54% è il più preoccupato.

Everything is connected, including cyber attacks

Top cyber threats over the next 12 months



Q3. Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three). Base: All respondents=3876
Source: PwC, 2024 Global Digital Trust Insights.

Le violazioni stanno diventando più costose

36%

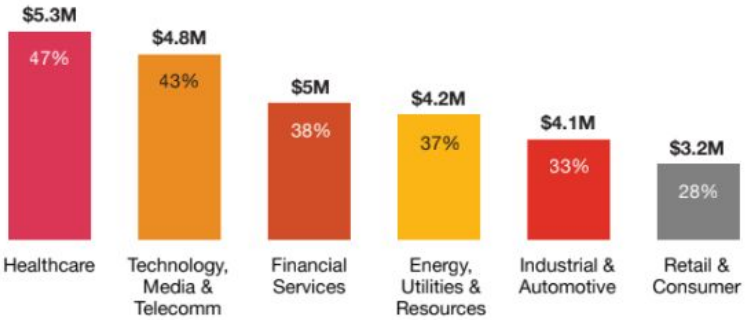
hanno subito una violazione dei dati che ha costato $1 milione o più, in aumento dal 27% dell'anno scorso.

Breaches are becoming more costly

Estimated costs to organisations' most damaging data breach in the past three years

Percentage who say they had a $1M+ breach: 2024 total = 36%, 2023 total = 27%

Average cost of breach in millions and percentage of most damaging breaches that cost $1 million or more, by sector



Q5. Thinking about the most damaging data breach you experienced in the past three years, please provide an estimate of the cost to your organisation. Base: Security and IT and CFO respondents= 1651
Source: PwC, 2024 Global Digital Trust Insights.

La semplificazione procede a ritmo sostenuto

49%

i leader aziendali stanno dando priorità agli investimenti in sicurezza informatica per la modernizzazione della tecnologia nei prossimi 12 mesi.

2024 cyber budgets aim to make the most of existing tools

Business leaders - Cybersecurity investment priorities over the next 12 months (Ranked top three)

Q14b. Which of the following investments are you prioritising when allocating your organisation's cyber budget in the next 12 months? (Ranked in top three). Base: Business respondents= 1925
Source: PwC, 2024 Global Digital Trust Insights.

Insoddisfazione per le capacità della tecnologia cyber

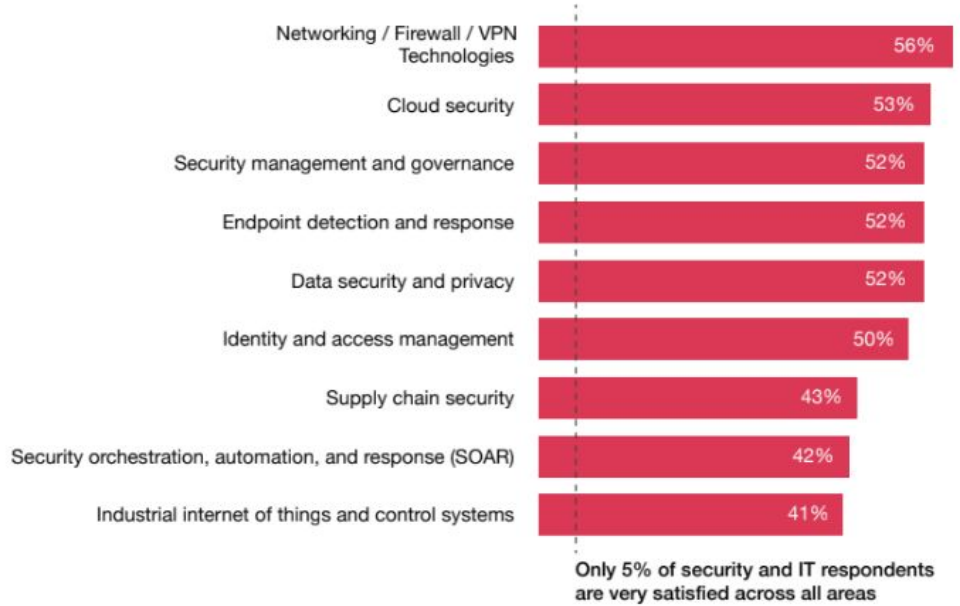
I rispondenti che hanno subito violazioni di dati costose

$1M

o più negli ultimi tre anni sono più propensi a riconoscere che hanno troppe soluzioni di sicurezza informatica e necessitano di integrazione.

Only half are satisfied with their cyber-tech capabilities

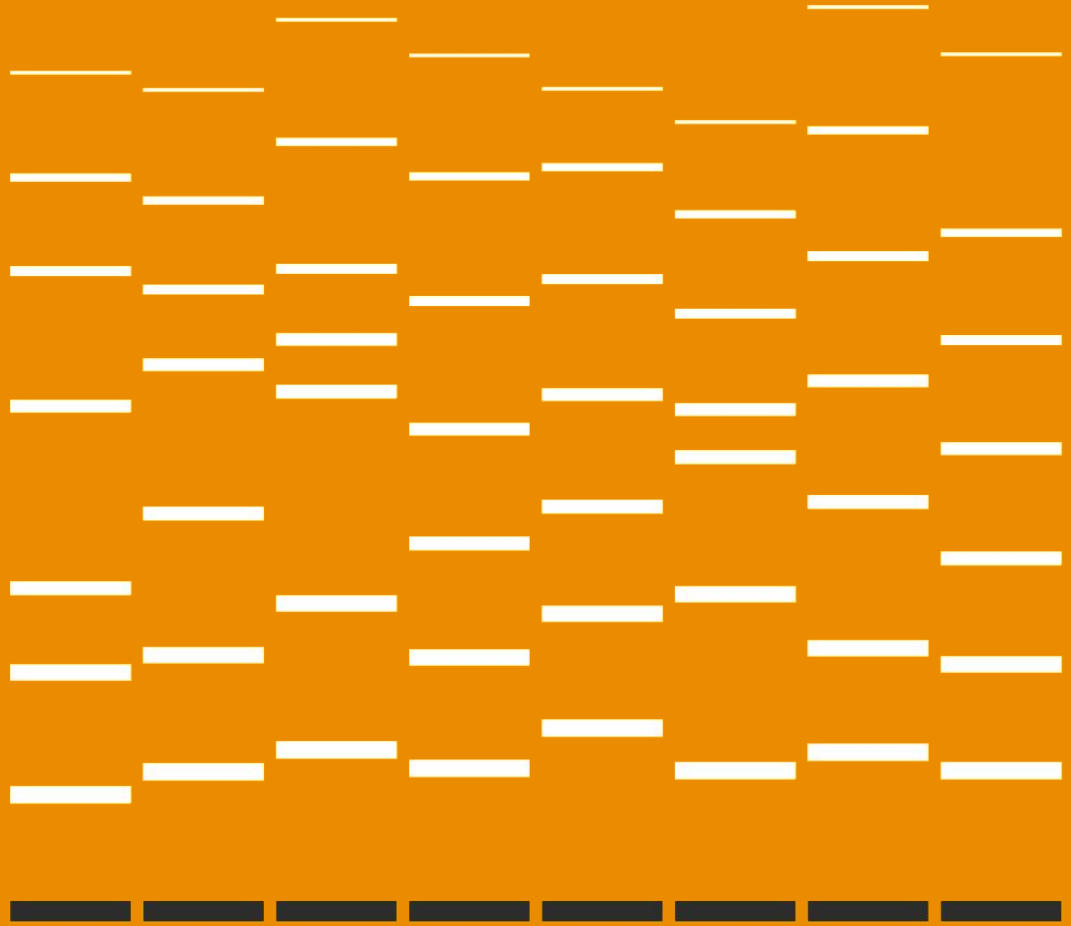
Organisation's technology capabilities in key cybersecurity areas



Q23. How satisfied are you with your organisation's technology capabilities in the following areas?
Base: Security and IT respondents=1517
Source: PwC, 2024 Global Digital Trust Insights.

3

Conclusioni



Agenzia Entrate

Divisione Contribuenti

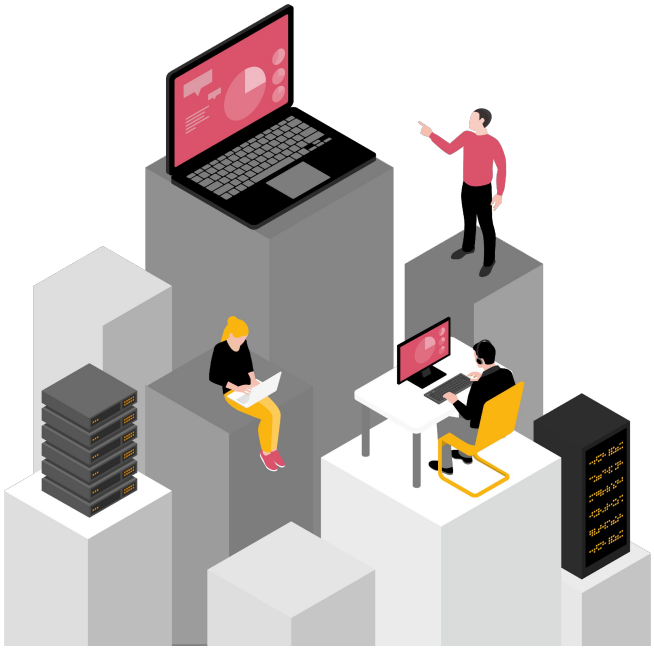
Direzione Centrale Grandi contribuenti e internazionale

Risposta n. 149/2023

OGGETTO: Principio di inerenza – Indeducibilità dei costi sostenuti per il pagamento in Bitcoin di un riscatto dati– Articolo 109, comma 5, del TUIR

To Do

- Il tema cyber è presente nell’agenda dell’imprenditore?
- È stato oggetto di discussione approfondita con gli organi di controllo dell’azienda (sindaci)?
- È stata assegnata una responsabilità specifica?
- Esiste una valutazione dei rischi cyber che includa aspetti organizzativi, di processo e tecnologici?
- Esiste un piano di implementazione delle misure di rimedio a copertura dei rischi?



Grazie!

Nicola Monti
Partner, PwC Italy
Cybersecurity & Privacy
39 3482504036
nicola.monti@pwc.com

Giuseppe D'Agostino
Partner, PwC Italy
Cybersecurity & Privacy
+39 3476466747
giuseppe.dagostino@pwc.com