La trasformazione digitale ed i «nuovi» rischi ad essa associata: come gestirli?

Lazise, 17 Maggio 2023

Relatori

Loredana Bombaci
Unit Director - Credit Solutions
Commercial Risk Solutions
| M:+39 331 6835093
Loredana.bombaci@aon.it

Riccardo Aggio
Unit Director – Cyber & Intangible Assets
Specialty Financial Lines
M: +39 3397203677
Riccardo.aggio@aon.it

Giovanni Vannone
Head of Cyber Solutions Southern Europe
Aon M&A and Transaction Solutions
M: +39 366 6742024
Giovanni.vannone@aon.it

AON

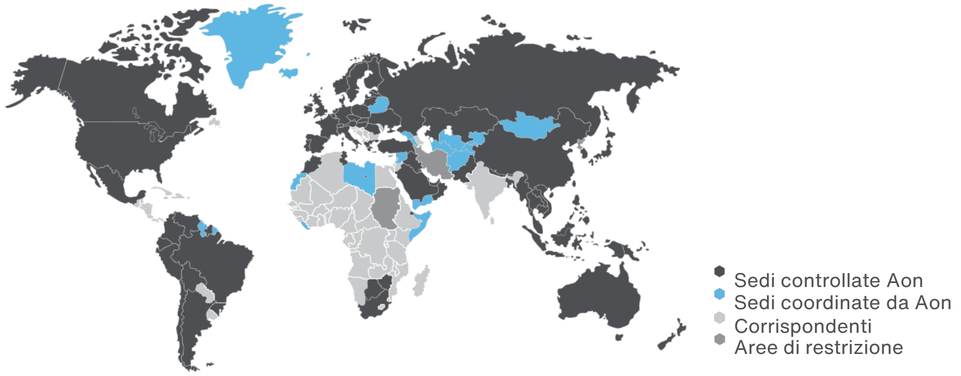
Aon Credit Solutions: nel mondo e in Italia

57 Nazioni In cui siamo presenti con uffici strutturati per la gestione del credito

Più di 100 Uffici

Grazie al nostro network altamente qualificato possiamo offrire ai nostril Clienti un supporto internazionale

500 Credit specialist



€ 100ML Premi intermediati in Italia

8 Uffici
In Italia

50 Credit specialist

PolicyManager – Cosa è?

Solution overview, at a glance:

- E’ una piattaforma Web, cloud based;
- Nata in partnership con Visma Onguard;
- Implementazione facile e veloce;
- Elevati standard di sicurezza;
- Multilingue;
- Zero costi di start up con l’Assicuratore;
- Avvisi in tempo reale;
- Reportistica semplificata;
- Analisi del rischio credito

Rischio Cyber: Cos’è

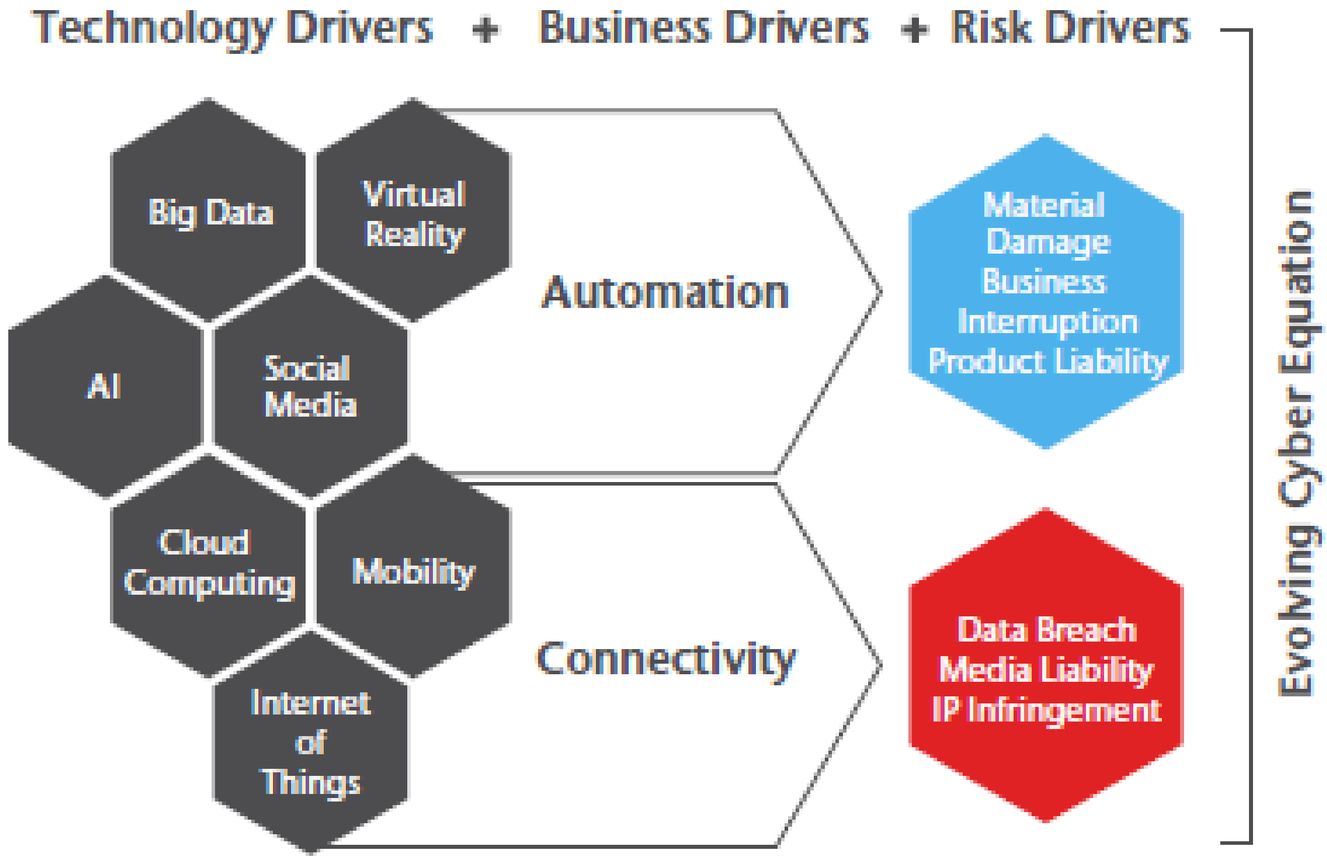
Rischio Cyber: un rischio atipico, dinamico e complesso

- Il Rischio Cyber è una **funzione di probabilità di accadimento e impatto di Business** di una minaccia cyber
- I target sono **sia gli asset materiali dell'Azienda, che quelli immateriali** (dati propri o di terzi detenuti o gestiti).
- **La trasformazione digitale crea un fattore moltiplicativo**, sia sulla probabilità di accadimento, sia sull'impatto

Il rischio Cyber è dinamico

Tema di Business, non solo IT

Non esiste il Rischio ZERO



Evoluzione della Minaccia Cyber

- **Frequenza e impatto**
  un attacco ogni 11 secondi, phishing +600% YOY, danni medi 3M€ ma sul lungo termine fino a 5-10x
- **Target**
  tutti i settori (PA, utilities, healthcare, retail, industria e manufatturiero, finanziario, …)
- **Tipologia di Attaccanti**
  vere e proprie «aziende», specializzate e altamente organizzate, con metodi e strumenti innovativi e dinamici
- **Evoluzione Tecnologica**
  Tecniche di attacco sofisticate ed in continua evoluzione, che fanno leva sulla evoluzione tecnologica portata dalla trasformazione digitale

- Il rischio cyber ha assunto caratteristiche peculiari: **alta probabilità ed elevato impatto**
- **Impossibile impedire** qualsiasi tipo di attacco, ma possibile invece:
  - Renderlo meno conveniente
  - Essere preparati a rispondere bene
  - Aver predisposto una mitigazione degli impatti (polizza, sistemi di protezione di dati e asset, etc.)
- **Necessario supporto specialistico** da parte di esperti di cyber risk management, non solo tecnici o specialisti IT

AON

Il Rischio *percepito* dalle aziende

Aon Global Risk Management Survey 2021

2.300+
Partecipanti

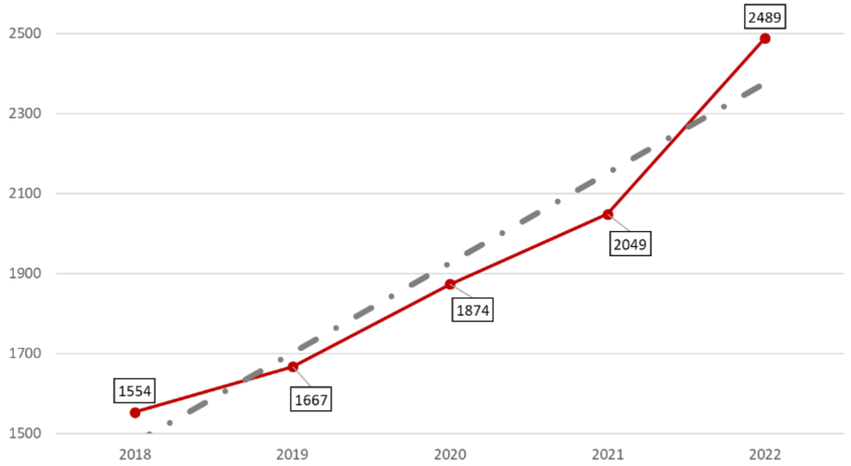
60
Paesi / Territori Nazionali

16
Industry

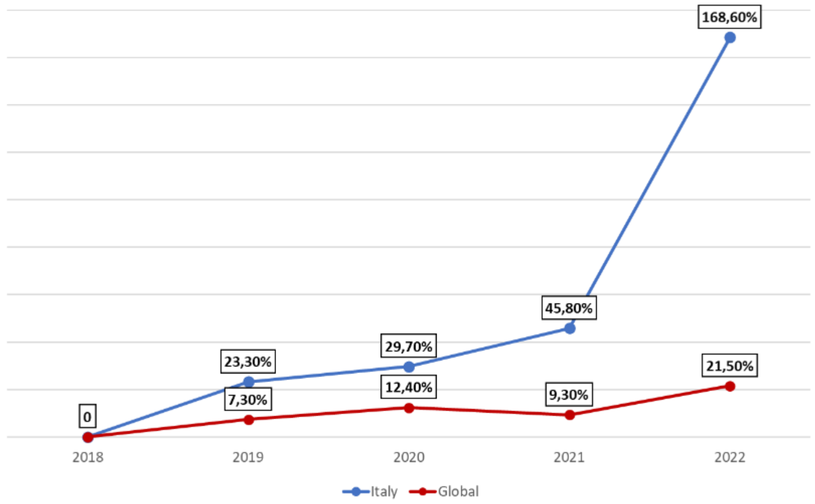
Source: AON Global Risk Management Survey 2021

Incidenti Cyber in costante crescita

Major incidents a livello globale ‘18-’22



Incremento Incidenti Italia vs Global ‘18-’22



Source: Clusit 2023

Principali Attacchi Cyber nel 2022

DATA	VITTIMA	SETTORE	LOCAZIONE	TIPOLOGIA	ATTORI
28/01/2022	Ministero della Giustizia	PA	Francia	Data Breach	Lockbit
03/02/2022	Swissport	Trasporto	Svizzera	Ransomware	BlackCat
08/02/2022	Artic Building Services	Edilizia	UK	Ransomware	ALPHV
27/02/2022	Bridgestone Americas	Manufacturing	Giappone	Ransomware	Lockbit
05/03/2022	NVIDIA	Tecnologia	USA	Ransomware	Lapsus$
12/04/2022	Panasonic	Manufacturing	Canada	Ransomware	Conti
26/04/2022	Coca-Cola Company	Food and Beverage	USA	Ransomware	Stormus
08/05/2022	ACGO	Manufacturing	USA	Ransomware	BlackMatter
18/05/2022	Vivalia	Healthcare	Lussemburgo	Ransomware	Lockbit
02/06/2022	The De Montfort School	Formazione	UK	Ransomware	Vice Society
15/06/2022	Novelty Group	Manufacturing	France	Ransomware	Vice Society
27/06/2022	Ministry of Agriculture	PA	Indonesia	Ransomware	Vice Society
04/07/2022	Vectalia Group	Trasporto	Spain	Ransomware	Vice Society
14/07/2022	Bandai Namco	Gaming	Japan	Ransomware	ALPHV
02/09/2022	TAP Air Portugal	Trasporti	Portugal	Ransomware	Ragnar Locker
1/11/2022	Genesys Aerosystems	Manufacturing	USA	Ransomware	BlackBasta
23/11/2022	Continental	Manufacturing	Germany	Ransomware	LockBit
11/11/2022	Medibank	Finance	Australia	Ransomware	Revil
13/11/2022	Wilken Software Group	IT	Germany	Ransomware	BlackBasta
8/11/2022	Silverstone	Sports	UK	Ransomware	Royal ransomware
28/11/2022	Ikea	Retail	Svezia	Ransomware	ViceSociety
05/12/2022	André Mignot	Healthcare	Francia	Ransomware	Sconosciuto
23/12/2022	The Guardian	Media	UK	Ransomware	Sconosciuto

Rischio Cyber: Come gestirlo

Domande Fondamentali per le Aziende

- **Come posso essere attaccato?**

  (non «se» posso essere attaccato)

- **Quanto sono vulnerabile?**

- **Quali danni subirei e per quale valore?**

- **Come mitigare il rischio, ottimizzando i costi?**
  - Interventi interni – quali?
  - Trasferimento in polizza – quale e cosa copre?

- **In caso di incidente sono preparato?**

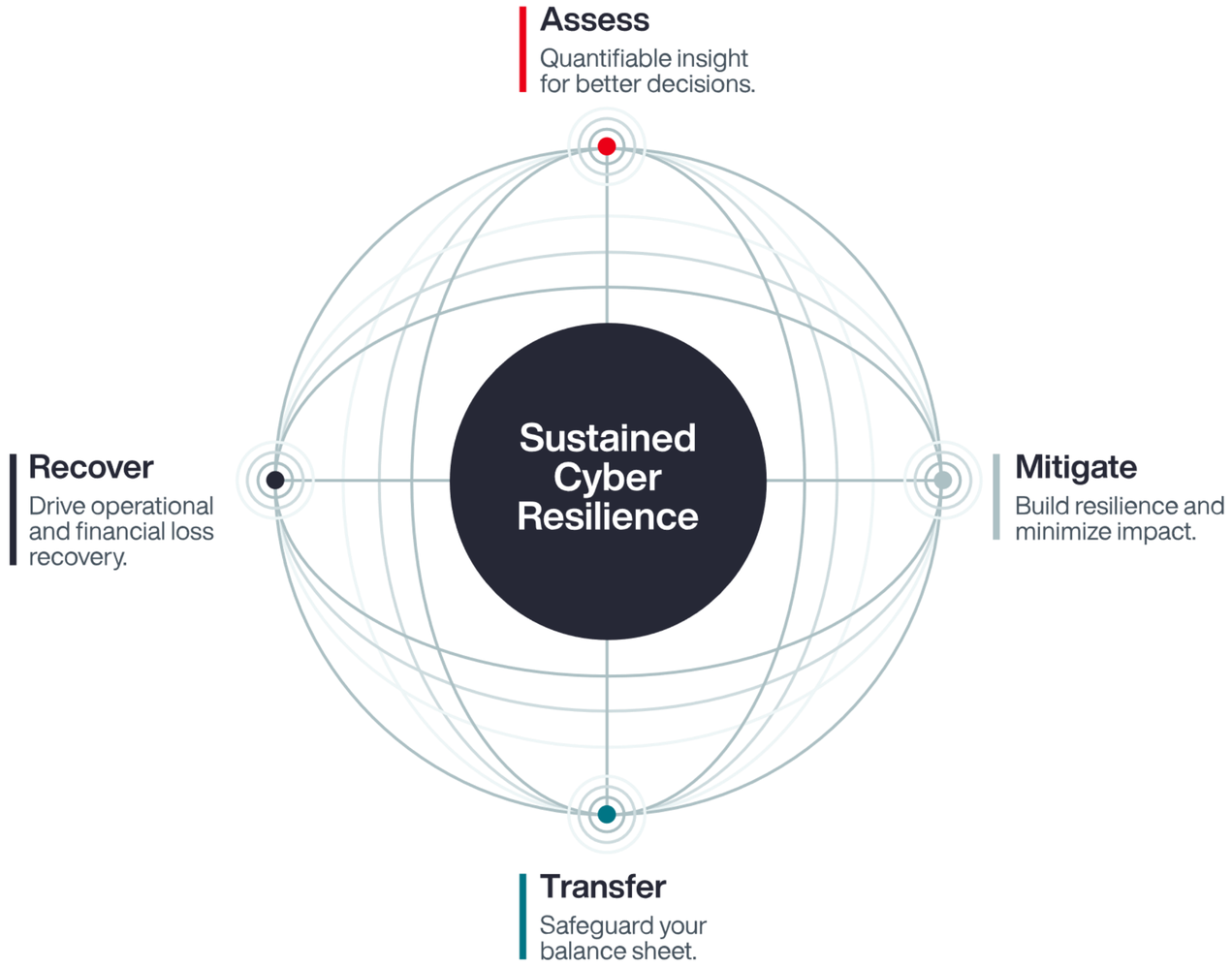
Analisi

Mitigazione

Risposta

Essenziale un approccio PREVENTIVO ed INTEGRATO

L’approccio integrato – Cyber Loop



Gestire il Rischio Cyber

Analisi «Assess»

Cyber Risk Assessment
- Scenari di crimine
- Esposizione tecnica
- Impatti economici
- Strategie di mitigazione

Cyber Quotient Evaluation +
- Check-up analitico sicurezza
- Priorità di intervento e rischi
- Analisi OSINT e scansione sistemi esterni

VA / PT
- Analisi reti / applicativi
- Mappatura vulnerabilità
- Penetration Test applicativi, web, infrastrutturali, IoT, HW
- White phishing

Prevenzione «Mitigate»

Ingegneria della sicurezza
- Governance e Organizzazione
- Infrastrutture cyber security
- Riprogettazione sistemi
- Piani di Incident Response

Temporary staff / BPO
- Risk manager / virtual CISO
- Tecnici cyber security

Formazione
- Awareness dipendenti
- Tecnica avanzata, Blue Team
- Test di Incident Response

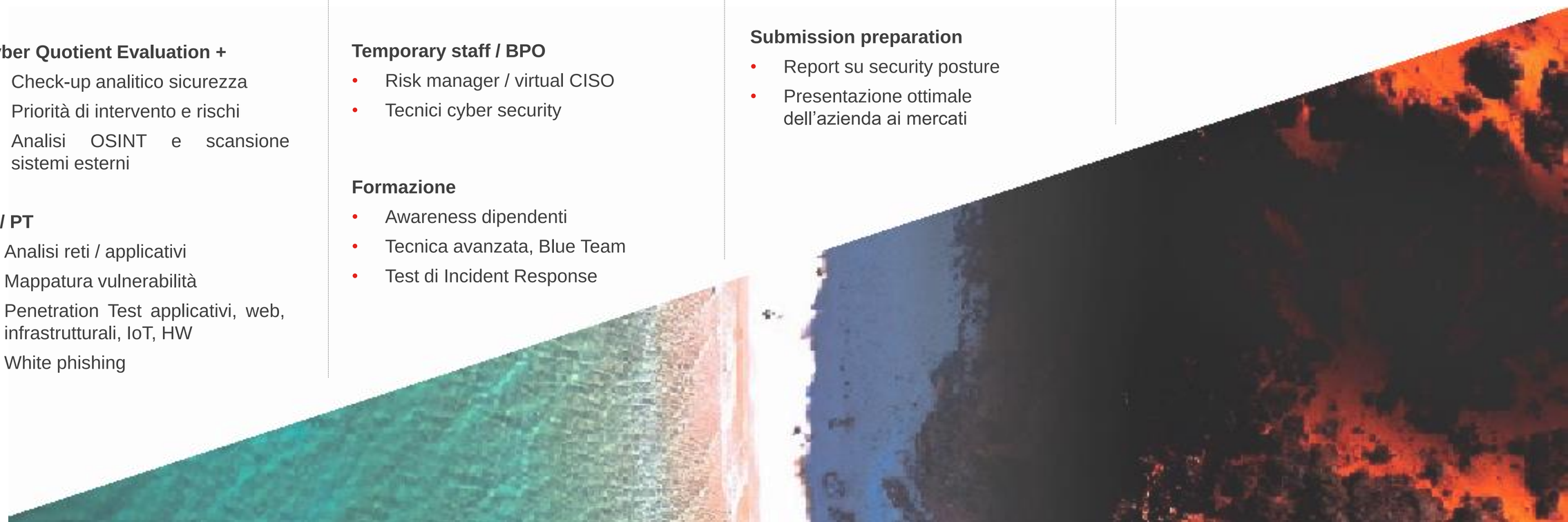
Trasferimento «Transfer»

Coperture Cyber, IT, BI, D&O
- Diagnostico efficacia / costi
- Disegno personalizzato
- Piazzamento e gestione

Submission preparation
- Report su security posture
- Presentazione ottimale dell'azienda ai mercati

Risposta «Recover»

Incident Response
- Investigazione forense
- Supporto tecnico al ripristino
- Gestione claim e perizia
- Comunicazioni e obblighi



Cyber Incident Response

5 aree di intervento

- **Investigazione**: in cui viene svolta l'analisi forense e gli approfondimenti tecnici necessari a perimetrare l'attacco ed i suoi obiettivi, le sue origini, dinamiche e conseguenze, nonché a valutare la presenza di eventuali infiltrazioni malevole pregresse o ancora in corso, quali malware, APT.
- **Ripristino**: in cui, prima di recuperare i sistemi da backup, vengono messe in atto le necessarie misure per rimuovere i vettori d'attacco identificati (es. malware e backdoor) e contenere l'impatto dell'incidente, bloccando ad es. le connessioni di rete utilizzate, gli account compromessi, terminando l'esecuzione dei processi e rimuovendo i file e i meccanismi di persistenza associati al malware, oltre che effettuando installazione di patch, modifica delle password e rafforzamento della rete sicurezza perimetrale.
- **Gestione del Claim**, in cui, laddove ci sia una polizza, gestione dell'incidente nei rapporti con la compagnia assicuratrice, garantendo la migliore risposta delle coperture in essere.
- **Quantificazione**, in cui si supporta l'azienda nella stima degli impatti economico patrimoniali dell'attacco, tenendo conto degli effetti di Business Interruption (mancati ricavi e opportunità commerciali), da degrado di efficienza dei processi di business, da extra lavorazioni IT, sia interne che con supporti esterni, da attività stesse di risposta tecnica, attività legali / privacy, di comunicazione, rivalse da terze parti etc.
- **Comunicazione**, in cui si gestiscono le notifiche a terze parti potenzialmente coinvolte, la denuncia alle autorità competenti (incluso il Garante della Privacy), agli azionisti, i fornitori, clienti e dipendenti.

AON

Aon – Il player globale nella gestione del rischio cyber

Analizzare ed affrontare preventivamente il cyber risk è una scelta ormai imprescindibile: fortunatamente, sono disponibili **soluzioni e metodologie** per trattare in modo approfondito i vari aspetti del problema ed apportare drastici miglioramenti alla **capacità di prevenzione e di risposta**.

Individuare e ingegnerizzare, tra di esse, l'insieme di interventi più efficace e mirato per una specifica realtà aziendale è un compito complesso, per il quale è necessaria una solida **esperienza trasversale** nei settori della cybersecurity, della modellizzazione del rischio e del suo trasferimento al mercato.

Aree di gestione rischio cyber

Trasferimento assicurativo: con molte decine di operatori nel mondo che offrono coperture cyber, il mercato ha sviluppato un'ampia capacità ed una proposta dettagliata e flessibile per le diverse casistiche di incidente.

Analisi e prevenzione: esistono standard procedurali particolarmente solidi e riconosciuti (ISO27001, NIST, AGID, etc.) e numerose soluzioni tecnologiche per lo sbarramento, il riconoscimento e la neutralizzazione di eventuali minacce.

Risposta ad incidenti: vi sono operatori specializzati nel supportare la gestione sia sul fronte del pronto ripristino delle infrastrutture e servizi, che per ottemperare ad obblighi normativi (es. GDPR) e relazioni con terze parti.

Aon

Il partner di riferimento sul cyber risk
con un team dedicato di oltre **700 specialisti**
da settori high-tech, militari, finanziari, accademici
e dalla integrazione di *Stroz Friedberg* e *Gotham*.

L'unico cyber leader presente sull'intero ciclo

STROZ FRIEDBERG an Aon company GOTHAM DIGITAL SCIENCE A STROZ FRIEDBERG COMPANY

N.1 al mondo nelle soluzioni di copertura assicurativa cyber
Con migliaia di polizze intermediate e un vasto network internazionale di compagnie, Aon ottimizza e personalizza coperture cyber di ogni complessità e dimensione.

600+ progetti tecnici di cyber risk analysis e cyber defense
Da anni tra gli operatori più evoluti ed esperti sul mercato per il disegno di strategie di gestione del rischio cyber, con approfonditi assessment tecnico-economici, ingegnerizzazione di piani di intervento organizzativo, tecnologico e formativo.

1100+ claims e incidenti cyber gestiti
Leader riconosciuti a livello internazionale (*Forrester, IDC, Forbes*), i nostri team di *Cyber Incident Response* gestiscono le più complesse investigazioni forensi, il ripristino dei sistemi e l'intera pratica di sinistro con l'assicuratore, in modo integrato ed efficace.

AON

Cyber Insurance
2023

Prepared by Aon's Cyber Specialty
Proprietary & Confidential

Mercato Assicurativo Cyber

Caratteristiche & Andamento

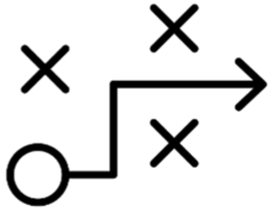
I pilastri chiave della polizza cyber

Prevenzione

- Pre-breach assessment
- Accesso a consulenti preapprovati
- Informazioni sulla Cybersecurity

Assistenza

- Investigatori forensi
- Servizi legali
- Assistenza notifiche
- Monitoraggio del credito
- Servizi di call center
- Gestione delle crisi/relazioni pubbliche



Operations

- Costi per porre fine alla minaccia estorsiva e per far ripartire l'operatività
- Perdita di profitto
- Costi per ricreare e/o ripristinare i dati
- Indennizzo trasferimento fondi seguito attacco informatico

RCT

- Costi legali e danni derivanti da richieste di risarcimento derivanti da trasmissione di virus e divulgazione di dati

La polizza cyber: le garanzie «First Party»

- **Interruzione dell'attività per violazione della sicurezza** – Copertura per la perdita di profitto causata da una violazione della sicurezza della rete, così come le spese extra associate. È normalmente applicata una franchigia economica ed una temporale.
- **Interruzione dell'attività da guasto del sistema** – Espande l'attivazione della copertura per l'interruzione dell'attività allo spegnimento improvviso del sistema IT o all'errore del dipendente.
- **Interruzione dell'attività da violazione della sicurezza o guasto del sistema del fornitore** – Copertura per l'assicurato per la perdita di profitto causata da una violazione della sicurezza di rete e/o dal guasto del sistema IT di un'azienda da cui l'assicurato dipende. Anche per questa garanzia è normalmente applicata una franchigia economica ed una temporale.
- **Cyber extortion** – Copertura per le spese sostenute per contrastare una minaccia di cyber estorsione. Possibile indennizzo anche del riscatto previo assenso della compagnia di assicurazione.
- **Costi di recupero dati** – Copertura per i costi sostenuti per ripristinare, recuperare o ricreare beni immateriali, non fisici (software o dati) che siano stati danneggiati, distrutti o cancellati a causa di una violazione della sicurezza della rete.
- **Spese di incident response** – Copertura dei costi per rispondere a un incidente di sicurezza o di violazione dei dati. Sono incluse le spese di esperti IT e consulenti legali, di gestione della crisi, informatica forense, pubbliche relazioni, e i costi di notifica ai soggetti i cui dati sono stati violati.

La polizza cyber: le garanzie «Third Party»

- **Responsabilità per la privacy** – Copertura per i costi di difesa e le richieste di risarcimento danni subiti da terzi per qualsiasi mancanza di protezione di informazioni riservate, che sia dovuta o meno a un fallimento della sicurezza della rete. La copertura può includere: violazioni involontarie della politica sulla privacy dell'assicurato, azioni di dipendenti disonesti e presunta raccolta illecita di informazioni riservate.
- **Responsabilità per la sicurezza della rete** – Copertura per i costi di difesa e i danni subiti da terzi derivanti da una violazione della sicurezza di rete, compresa la responsabilità causata da furto o divulgazione di informazioni riservate, accesso non autorizzato, uso non autorizzato, attacco denial of service o trasmissione di un virus informatico.
- **Responsabilità derivante dai media** – Copertura per i costi di difesa e i danni subiti da terzi per lesioni derivanti dalla pubblicazione di contenuti come calunnia, diffamazione, violazione del copyright, violazione del marchio o violazione privacy. La portata dei media coperti è variabile e può andare dal solo sito web dell'assicurato a tutti i contenuti in qualsiasi mezzo.
- **Multe e penalità PCI** – Copertura per una multa o una penalità contrattuale da parte di un'associazione di carte di pagamento (ad es. MasterCard, Visa, American Express) o di una banca che elabora transazioni con carte di pagamento (cioè una "Banca acquirente") in relazione alla non conformità di un assicurato con gli standard di sicurezza dei dati PCI.
- **Privacy Regulatory Multe e Sanzioni** – Copertura per i costi di difesa per i procedimenti intentati da un'agenzia governativa in relazione a una mancata protezione delle informazioni private e/o a una mancata sicurezza della rete. La copertura include multe e sanzioni laddove assicurabili per legge. I danni compensativi, cioè gli importi che l'assicurato è tenuto a depositare in un fondo di risarcimento per i consumatori, possono essere coperti.

Andamento del mercato cyber in Italia: forecast 2023

Il mercato cyber è in continua evoluzione, ma sta mostrando trend positivi...

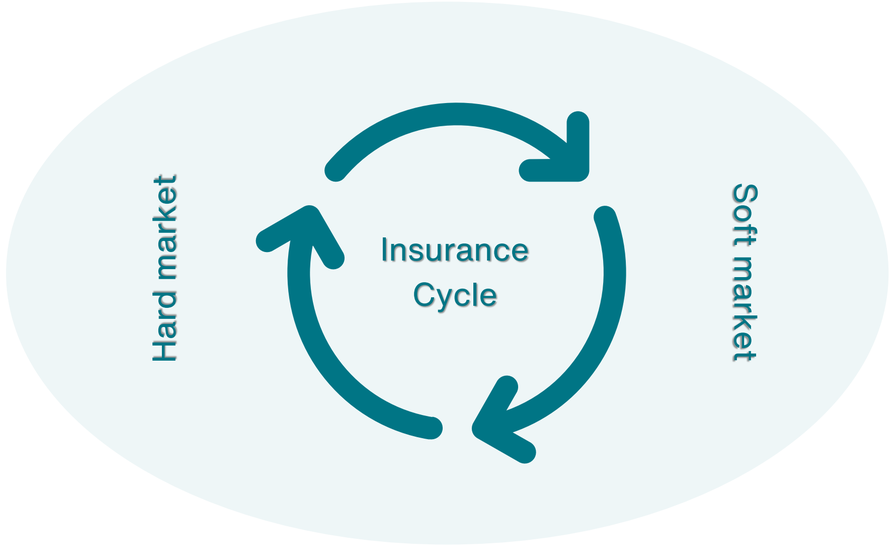
Premi: verso la stabilizzazione ma si continuano a registrare aumenti	
Capacità: ancora in leggera contrazione, ma si segnalano aperture dal mercato	
Processo sottoscrittivo: rigoroso, ma stabile	
Franchigie: in assestamento dopo un periodo di aumenti significativi	
Limiti: ancora importanti restrizioni di copertura con l'introduzione di nuovi sottolimiti	
Sinistri: calo della sinistrosità, ma peggioramento della severità degli impatti	

Il rischio cyber: i temi chiavi del 2022 – 2023 (1/2)

1 La fase di «hard market» perdura, ma è in lieve miglioramento

A causa del sempre elevato numero di attacchi hacker, nel 2022 il mercato assicurativo Cyber è stato ancora caratterizzato dal generale inasprimento delle condizioni offerte, sebbene i peggioramenti di copertura previsti dalle compagnie assicurative soprattutto nel Q3 – Q4 2022 sono risultati meno drastici del 2021.

Per il 2023 si intravedono e sono da molti annunciati segnali di stabilizzazione in termini di tassi di premio applicati, capacità offerta e processo sottoscrittivo.



2 Rigore nella sottoscrizione

Gli assicuratori continuano a richiedere l'uso di soluzioni di info e network-security e misure di continuità aziendale volti, da un lato, a migliorare la postura di sicurezza dell'assicurato e, dall'altro, a mitigare le conseguenze finanziarie e non degli attacchi e incidenti informatici.

Adottati ormai da molte compagnie requisiti minimi di assicurabilità (ad es. MFA).

L'opinione è che siano stati fissati standard in grado di garantire la sostenibilità del mercato.

Il rischio cyber: i temi chiavi del 2022 – 2023 (2/2)

3 Capacità & Premi

Nei mesi scorsi molti assicuratori hanno ridotto la capacità offerta per singolo player e singolo rischio che spesso non supera i 5M per sinistro e anno.

Allo stesso tempo, viene registrata maggiore concorrenza e capacità sui layer in eccesso.

Il miglioramento dei loss ratio e l'aumento della concorrenza rendono ragionevole pensare che nel 2023 i tassi di premio saranno più competitivi rispetto ai 24 mesi precedenti.

4 Limitazioni di Copertura

Gli assicuratori continuano a vagliare attentamente la copertura offerta per le infrastrutture critiche.

Tra gli aspetti maggiormente attenzionati e fonti di limitazioni di copertura si segnalano: 1) esclusioni relative alla guerra, 2) limitazioni territoriali, 3) rischio sistemico e 4) coperture accessorie come quella relativa al trasferimento di fondi.

Particolarmente attenzionata continua ad essere anche la copertura offerta per l'attacco ransomware

Il rigore nella sottoscrizione: gli aspetti più attenzionati

Token Based Multi-factor Authentication (MFA)

Vulnerability Scanning & Patch Management

Endpoint Protection & Response (EDR)

E-mail Filtering & Security (DMARC/DKIM)

Social Engineering Exercises & Awareness Training

Identity, Access, and Privileged Access Management

Network Segmentation: Secure RDP, VPN, OT/IT

Disaster Recovery Testing, BCP, & Backups

Incident Response Plan (Written & Tested)

Inoltre, molti assicuratori conducono nella fase assuntiva scansioni di vulnerabilità non invasive sugli assicurati per segnalare in modo proattivo eventuali vulnerabilità riscontrate. Queste scansioni sono alla ricerca di problemi relativi a RPC (Remote Procedure Call), VNC (Virtual Network Computing), SMB (Server Message Block) e RDP (Remote Desktop).

Timeline

Incontro / Call iniziale

1

4 settimane circa per la raccolta delle informazioni tramite compilazione appositi questionari oppure cd. Road Show

2

Presentazione del rischio al mercato assicurativo

4 settimane circa per la valutazione del rischio da parte degli Assicuratori ed eventuali richieste di approfondimento e/o compilazione di ulteriori questionari specifici

3

Ricezione dei riscontri dal mercato.

Valutazione delle proposte ricevute

4

Scelta del miglior player e invio dell'ordine fermo

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better—to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business

aon.com

Important notice

This presentation was prepared for the exclusive use and benefit of the addressee to whom it is directed and solely for purposes of facilitating a general discussion regarding Aon plc and/or its subsidiaries ("Aon") and certain of its products and services. This presentation is for discussion purposes only and is incomplete without reference to, and should be viewed solely in conjunction with, the accompanying oral briefing provided by Aon. This presentation contains confidential information and neither this presentation nor any of its contents may be copied or disclosed, in whole or in part, or used for any other purpose without the prior written consent of Aon.

In preparing this presentation, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which has been provided to, or reviewed by, us. While this presentation has been prepared in good faith, no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by Aon or by its officers, employees or agents in relation to the adequacy, accuracy, completeness or reasonableness of this presentation or any other information (whether written or oral) supplied or otherwise made available in connection with it. All and any such responsibility and liability is expressly disclaimed. The information contained in this presentation is subject to change and no responsibility or liability is assumed for updating this presentation or any additional information provided herewith, or for correcting any inaccuracies in this presentation or such information which may become apparent.

This presentation does not constitute a commitment by any Aon entity to arrange or place insurance or to underwrite any risks or provide any other services.