



POLIZZA CYBER

**LE PRINCIPALI GARANZIE PER
L'INDUSTRIA DELLA GOMMA**

**Michele Lavaggi
Cyber Leader AIG**

Un webinar a cura di



**L'INDUSTRIA
DELLA GOMMA**

mercoledì 28 aprile 2021



What's Inside CyberEdge:
Copertura modulare



What's Inside CyberEdge:
Strumenti e Servizi gratuiti



What's Inside CyberEdge:
Servizi di AIG Risk Consulting



What's Inside CyberEdge:
Servizi di Fornitori selezionati

Una soluzione olistica

Copertura modulare

Le società stanno sempre di più mettendo i dati e le reti al centro dei loro affari e possono subire pesanti perdite economiche in caso di incidenti di cyber sicurezza. CyberEdge è una polizza modulare flessibile che permette di scegliere le coperture che meglio rispondono alle proprie esigenze.

Qui di seguito alcuni esempi di moduli disponibili:



Pronto intervento



Gestione di Eventi



Responsabilità civile sicurezza e privacy



Violazione della rete



Violazione della rete OSP



Guasto del Sistema



Incidente ai Dati Elettronici



RC per attività Multimediali



Attacchi informatici a scopo estorsivo



Hacking telefonico



Trasferimento fraudolento di fondi

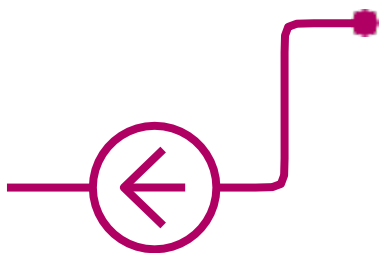


Buono omaggio



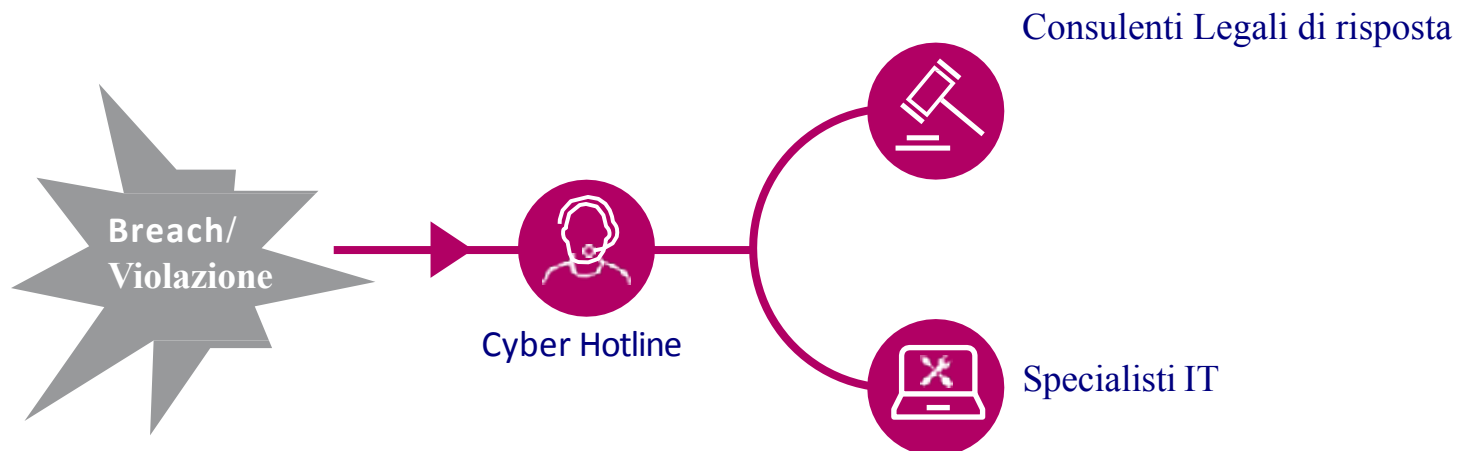
Ricompensa per segnalazione di atti criminali

Copertura Modulare

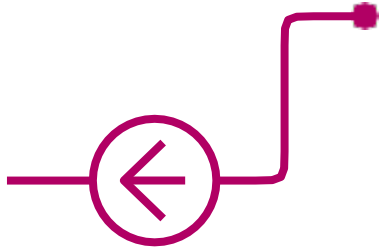


Pronto Intervento

Quando si sospetta un violazione della sicurezza informatica molte società non hanno la capacità di diagnosticare la problematica e rispondere rapidamente. La copertura **Pronto Intervento** offre l'accesso, in emergenza, ad un team di consulenti legali di risposta e specialisti IT che possono offrire supporto critico ed una risposta coordinata. Questa copertura è offerta senza franchigia nei limiti temporali precisati in polizza*.



Copertura Modulare



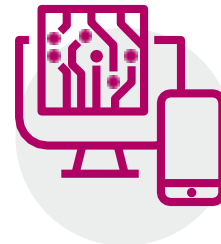
Gestione di Eventi

Dopo un attacco informatico, le società necessitano di una serie di servizi per rimettere sui binari i loro affari. La copertura **Gestione di Eventi** di CyberEdge indennizza i servizi Legali, IT e PR, nonché servizi di Monitoraggio Creditizio e dell'Identità Digitale (ID) in aggiunta al ripristino dei Dati e i costi di Notifica dell'avvenuta violazione.



Legali /PR

Risposta coordinata ai
danni reputazionali



Forensica tecnica

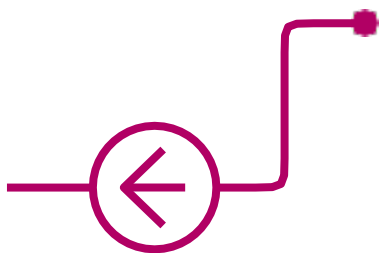
Dati impattati
Ripristino dei Dati



Clienti

Notifica Monitoraggio
Creditizio &
dell'Identità Digitale

Copertura Modulare



Responsabilità civile sicurezza e privacy

La copertura **Responsabilità civile sicurezza e privacy** risponde alle richieste di risarcimento di terze parti derivanti da una falla nella sicurezza della rete. Include i costi di difesa e il risarcimento dei danni derivanti da una violazione di informazioni confidenziali nonché i costi di difesa in cui si incorra durante un'investigazione di un Ente Regolatore o PCI (incluse le eventuali penalità).

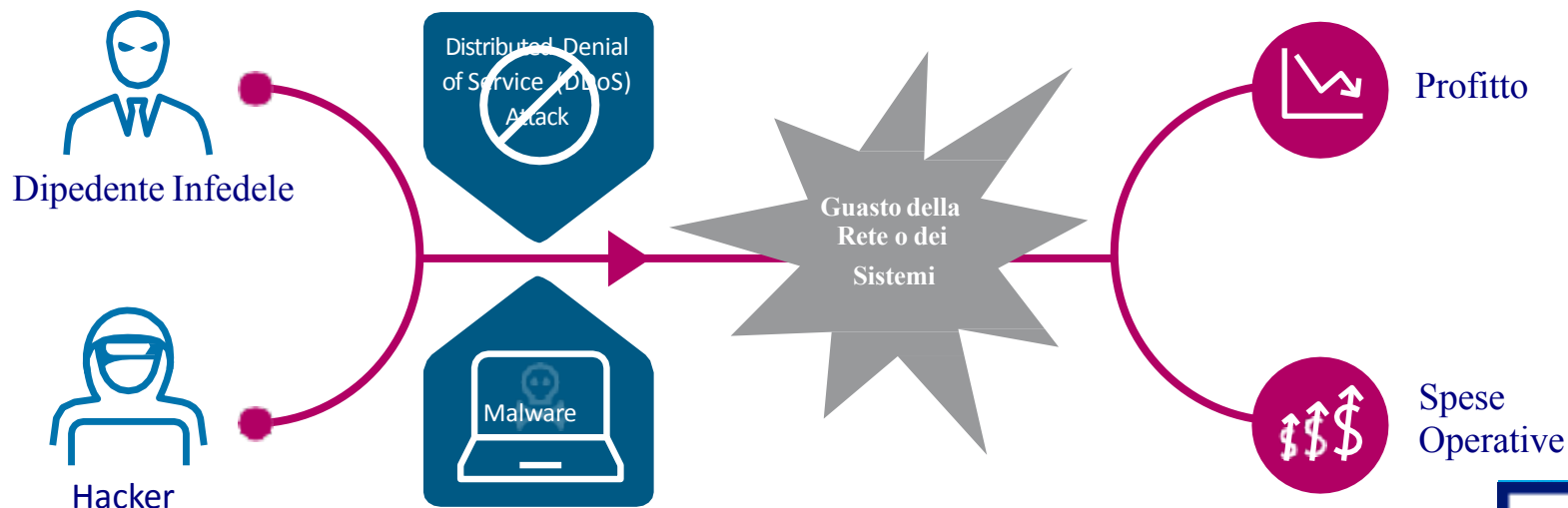


Copertura Modulare

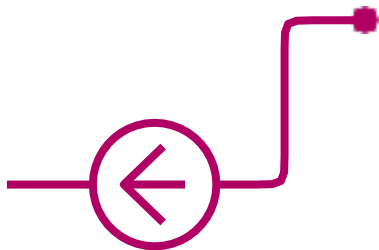


Interruzione della rete: Violazione della Rete

Quasi tutti gli affari che presuppongono relazioni con i consumatori oggi dipendono pesantemente dal web per le vendite dirette o le relazioni con i clienti, ed anche le industrie tradizionali, quali la manifatturiera e i trasporti, richiedono la connettività della rete per operare efficientemente. La copertura **Violazione della rete** copre la perdita di profitto e le spese di mitigazione quando le attività aziendali siano interrotte o sospese a causa di un incidente di sicurezza informatica

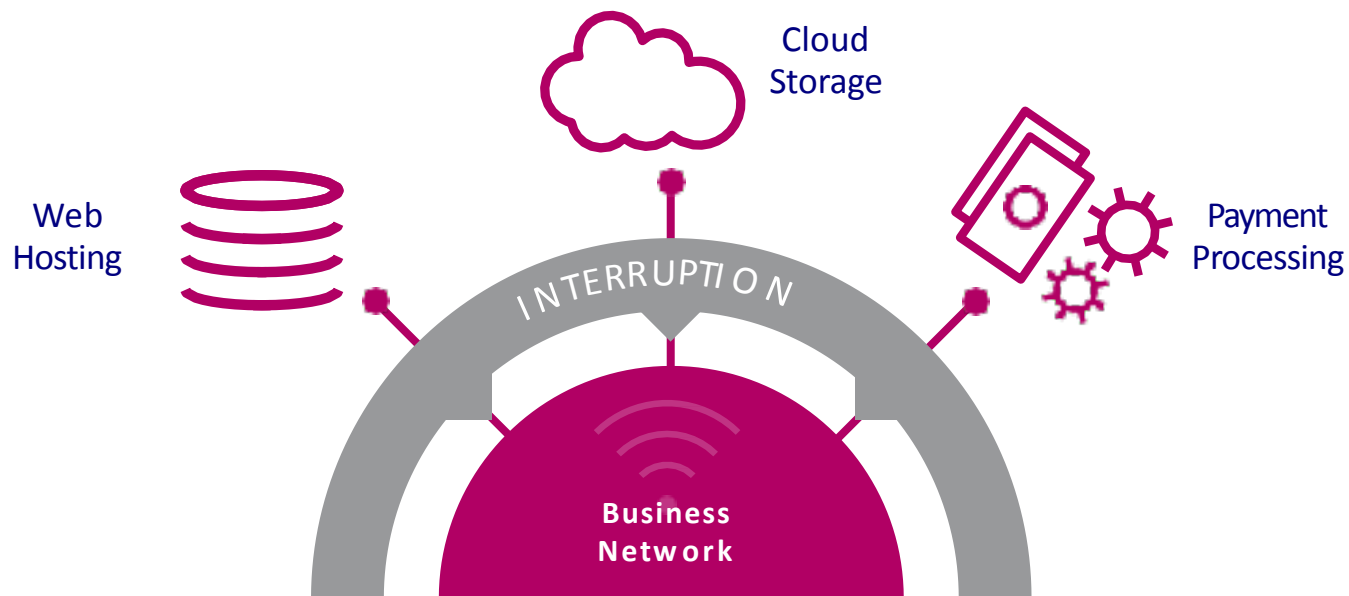


Copertura Modulare

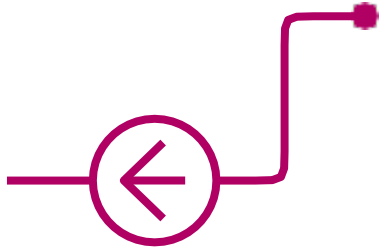


Interruzione della rete: Violazione della Sicurezza OSP

I Fornitori Esterni di Servizi (Outsourced Service Providers - OSP) gestiscono per le Società un'ampia serie di importanti servizi quali web hosting, processamento dei pagamenti, raccolta e conservazione dei dati. La garanzia **Violazione della Sicurezza OSP** estende la copertura alla perdita di profitto subita dalla cliente, e i costi di mitigazione, derivante da un guasto alla rete o i sistemi dell'OSP.

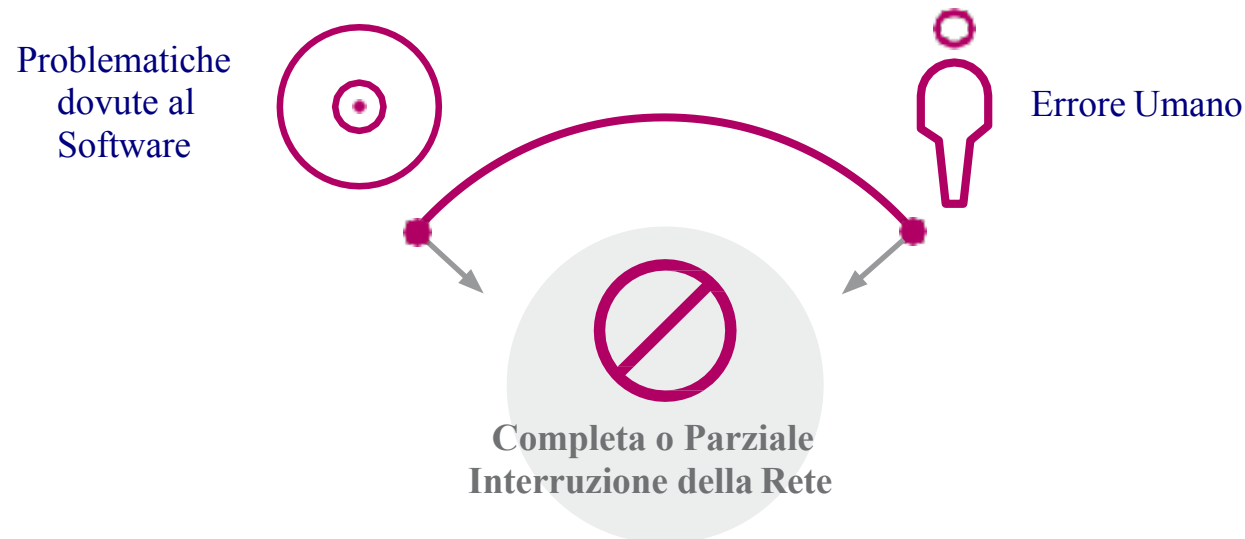


Copertura Modulare



Interruzione della rete: Guasto del sistema

Non tutti i guasti ai sistemi sono attribuibili ad una falla nella sicurezza informatica: interruzioni non intenzionali e non pianificate possono portare a subire perdite per **Interruzione della rete**. La garanzia **Guasto del sistema** del CyberEdge estende la copertura **Interruzione della rete** alle perdite e i costi di mitigazione derivanti da guasto dei sistemi interno non dovuto a una violazione della sicurezza informatica

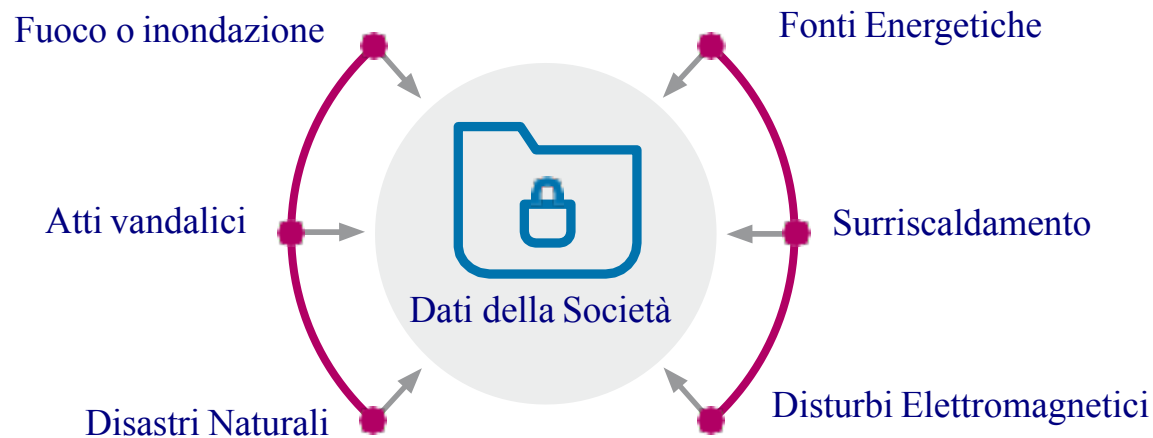


Copertura Modulare

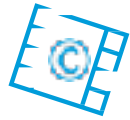
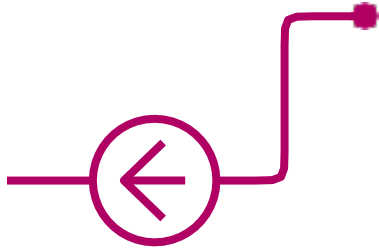
10001101
00110100
10001101
00110101

Incidente ai Dati Elettronici

Un incidente di cyber sicurezza non è l'unico motivo per il quale i dati possono andare perduti o corrotti. Le fonti energetiche, disastri naturali, surriscaldamento e atti vandalici (fisici), possono portare all'inaccessibilità dei dati. L'estensione **Incidente ai Dati elettronici** semplicemente aggiunge un altro evento assicurato alla sezione **Gestione di Eventi** del **CyberEdge** per coprire i danni accidentali o la distruzione dei sistemi informatici di una società

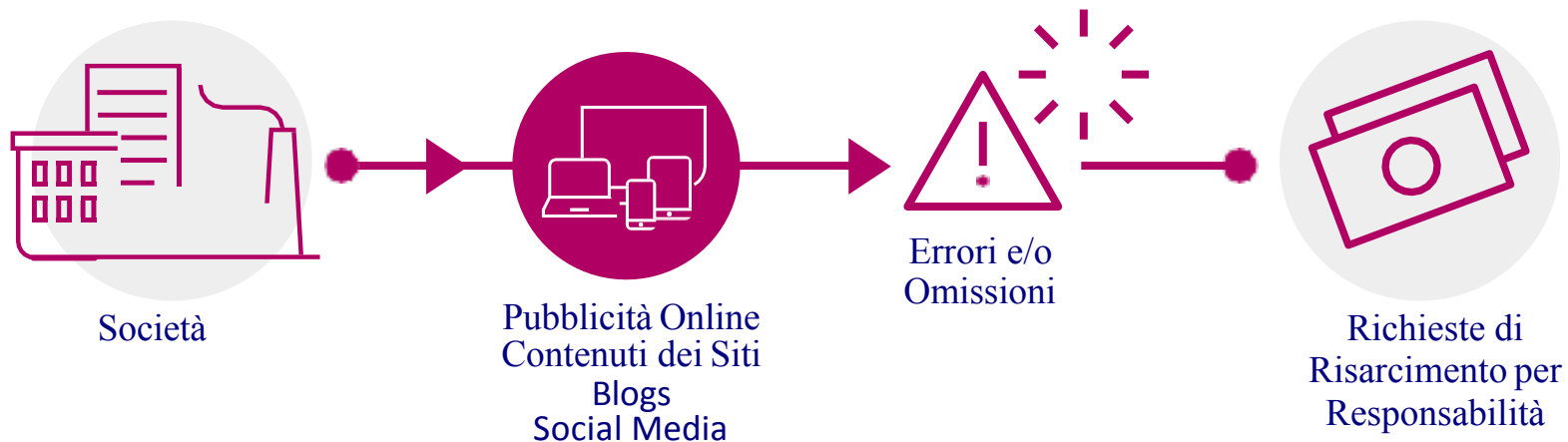


Copertura Modulare

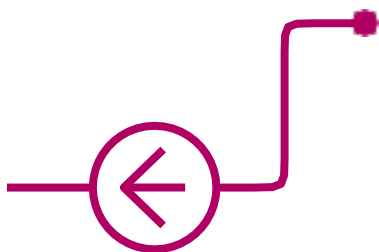


Responsabilità Civile per attività multimediali

In un contesto digitale in continua evoluzione, è oggi più facile che mai per le società incorrere inavvertitamente in violazioni di marchi, appropriazione indebita di materiale creativo o inadeguata verifica dei fatti. La copertura **Responsabilità civile per attività multimediali** copre i danni ed i costi di difesa in relazione ad una violazione della proprietà intellettuale altrui, o negligenza in connessione con contenuti elettronici.

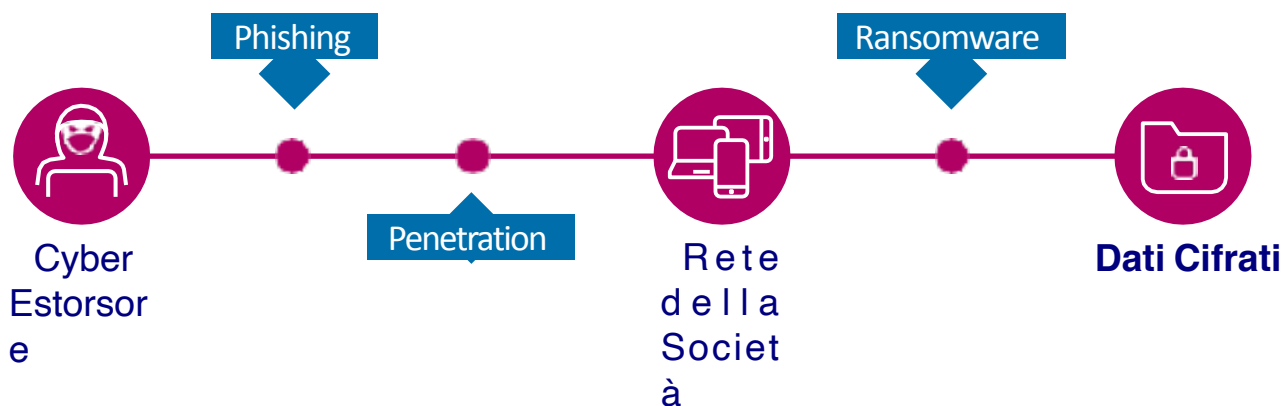


Copertura Modulare

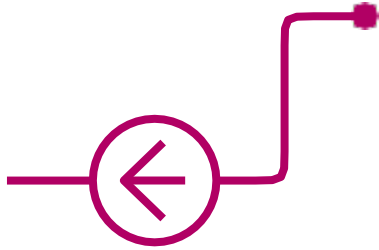


Attacchi Informatici a scopo estorsivo*

Gli imprenditori possono essere vittime di criminali informatici che usano ransomware per cifrare i loro dati fintanto che questi non paghino per ricevere una chiave di sblocco. La copertura **Attacchi informatici a scopo estorsivo** copre le perdite risultanti da una minaccia di estorsione ed include le somme pagate dall'assicurato a titolo di riscatto per fare cessare un'estorsione oltre l'indennizzo degli onorari dovuti a consulenti specializzati in estorsioni informatiche.

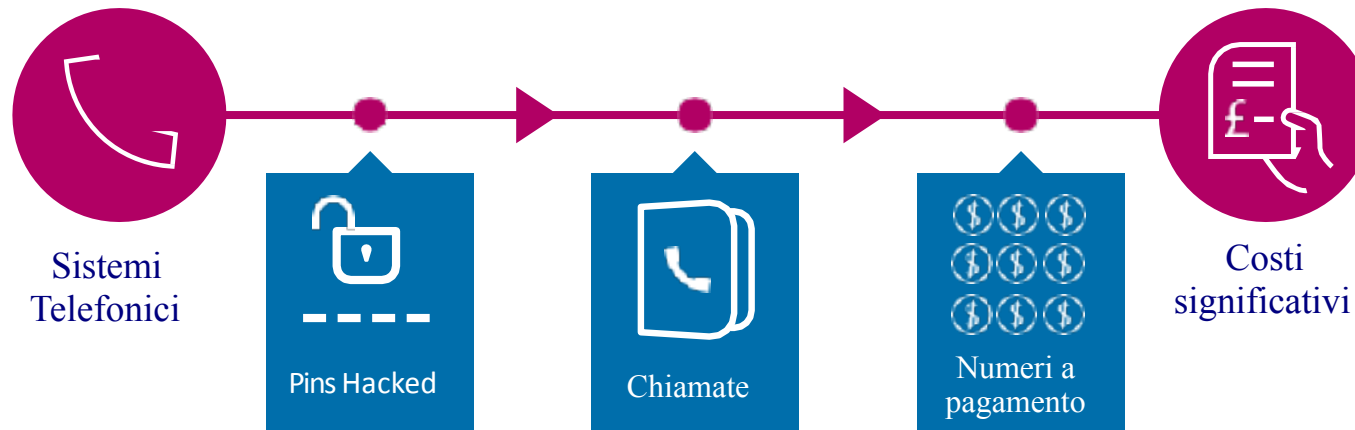


Copertura Modulare

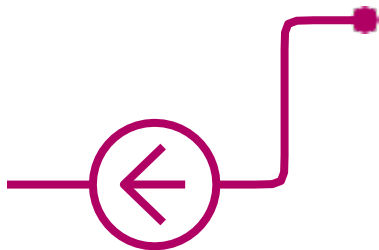


Hacking telefonico

Oltre l'hacking online, gli imprenditori possono anche sperimentare l'hacking dei sistemi telefonici. Si fa riferimento a una frode perpetrata sul PBX (Private Branch Exchange - Rete Telefonica Interna), che si verifica quando un truffatore prende di mira un sistema telefonico per fare chiamate a numeri a pagamento. L'estensione **Hacking telefonico** copre i costi derivanti da accesso e uso non autorizzato ai sistemi telefonici sia nell'ipotesi che esso sia iniziato dentro ovvero fuori i locali dell'impresa.

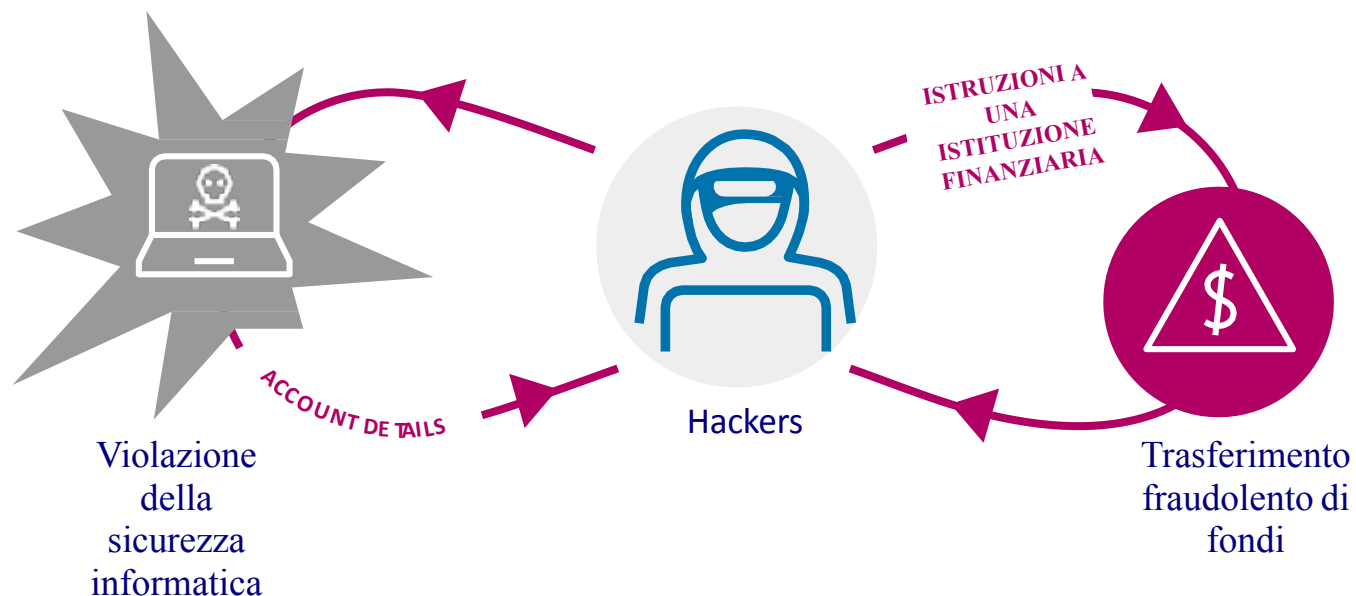


Copertura Modulare

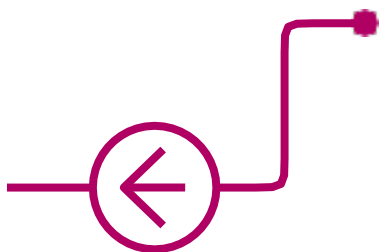


Trasferimento Fraudolento di fondi

Il trasferimento fraudolento di fondi è una forma di **computer crime** con cui i criminali usano informazioni ottenute tramite una violazione della sicurezza informatica per trasferire fraudolentemente fondi da un conto corrente aperto presso un'Istituzione Finanziaria. La copertura **trasferimento fraudolento di fondi** di CyberEdge copre le perdite finanziarie, direttamente derivanti dal trasferimento di fondi, subite a causa di una violazione della sicurezza informatica



Copertura Modulare



Buono omaggio

Un incidente informatico può impattare negativamente le relazioni fra i clienti e una società: buoni omaggio, rimborsi e/o sconti, possono essere uno strumento per invertire il feeling negativo. La copertura **Buono omaggio** di CyberEdge è uno strumento flessibile da offrire ai clienti in alternativa alla garanzia **Monitoraggio Creditizio e dell'Identità Digitale** ogni qual volta vi sia stata una violazione di informazioni confidenziali o le persone fisiche non abbiano potuto accedere a servizi a causa di un'interruzione.



La copertura **Buono omaggio** può essere attivata in due modi:

1. Dalla sezione **Gestione degli eventi**, in quanto i dati di persone fisiche siano stati compromessi; questa offre la flessibilità di scegliere fra il Monitoraggio creditizio e dell'Identità Digitale ovvero il Buono Omaggio
2. Dalla sezione **Interruzione della rete**, in quanto le persone fisiche non siano state in grado di accedere a servizi a causa di un'interruzione

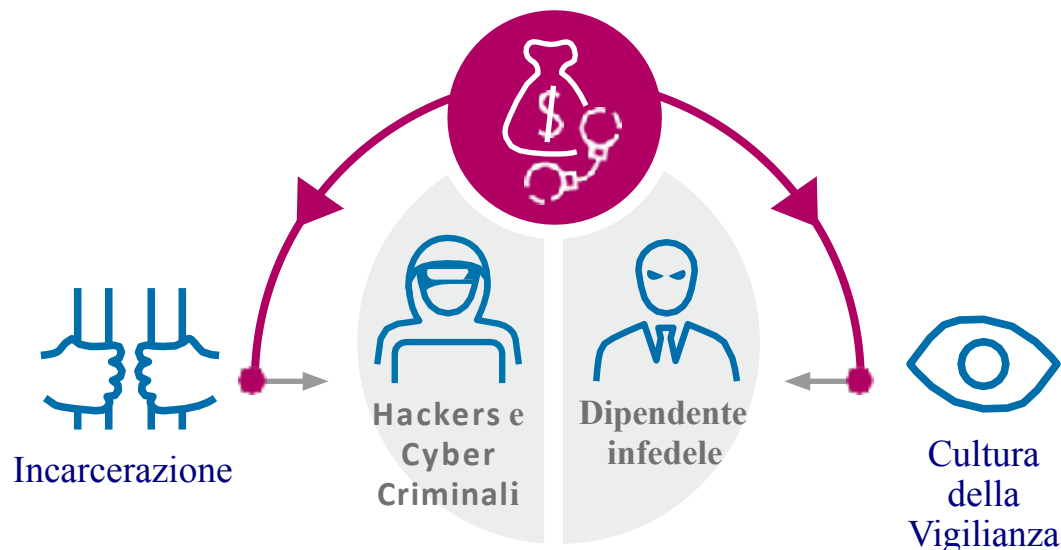
Copertura Modulare



Ricompensa per segnalazione di atti criminali

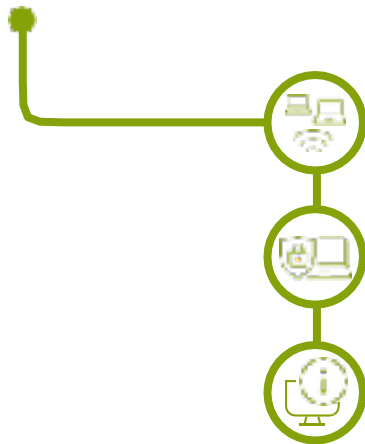
La copertura **ricompensa per segnalazione di atti criminali** mette a disposizione un fondo da elargire a quanti abbiano fornito informazioni che consentano di arrestare ed incarcerare persone fisiche che abbiano commesso o stiano tentando di commettere atti illegali oggetto di copertura ai sensi della polizza CybeEdge. Questa copertura opera non solo per hackers o criminali informatici ma anche per i dipendenti infedeli, così da premiare i collaboratori che segnalino e riportino comportamenti sospetti

Ricompensa per segnalazione dei criminali



Strumenti e Servizi gratuiti

CyberEdge include una serie di **strumenti e servizi di prevenzione** che aiutano a ridurre la probabilità di un cyber-attack e ad aggiungere una barriera addizionale al programma di cybersecurity approntato dalla società. Contraenti qualificati hanno accesso ai seguenti strumenti e servizi gratuiti:



Scan di Vulnerabilità dell'Infrastruttura*

Proactive Shunning e Servizi formativi* Portale

di Informazione sulla Cyber sicurezza*

Strumenti e Servizi gratuiti

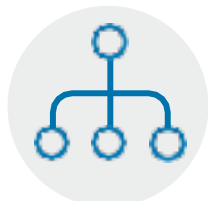


Scan di vulnerabilità dell'Infrastruttura*

Esperti effettuano da remoto uno scan delle infrastrutture esposte sulla rete per identificare vulnerabilità che offrano potenziali exploit ai cyber criminali. Il servizio di scanning individua e prioritizza i rischi nascosti e fornisce una visione dettagliata dello stato di vulnerabilità di una società così che la stessa possa meglio tracciarle, comprenderle e annotarle sulla sua postura di sicurezza .



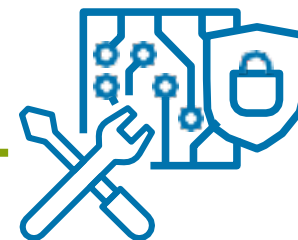
Scan



Web Infrastructure



Identificazione
Vulnerabilità



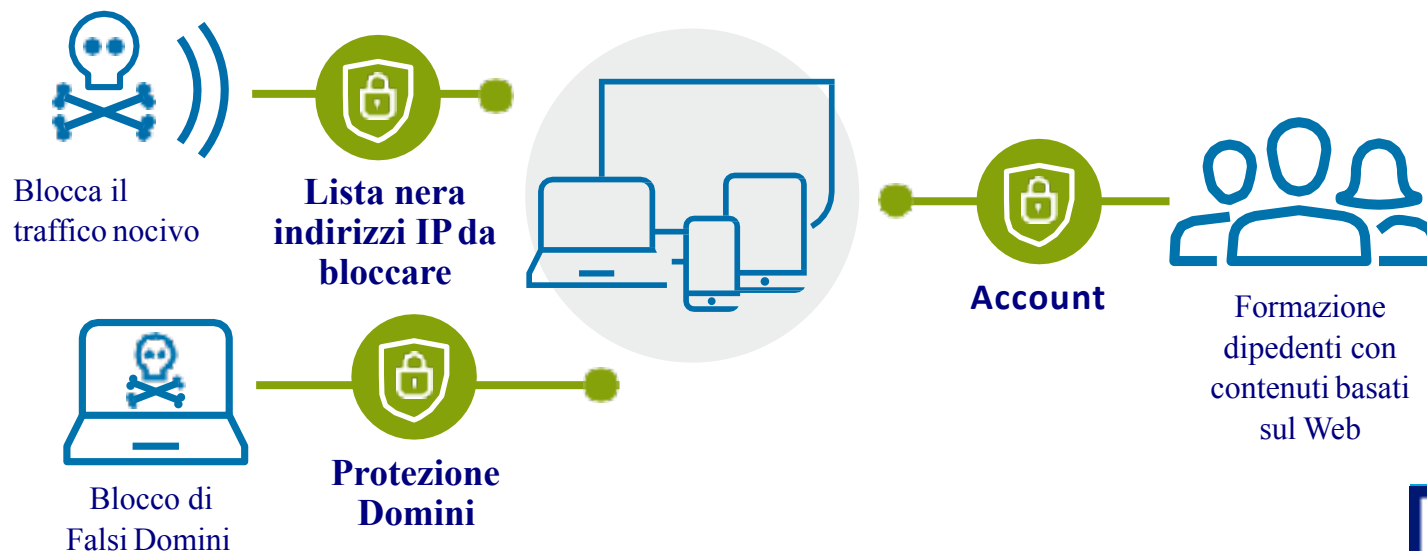
Prioritizzare
interventi di
bonifica

Strumenti e Servizi gratuiti

Proactive Shunning e Servizi Formativi*

Prima di portare un attacco, i criminali spesso effettuano ricognizioni per confermare che un indirizzo IP sia un obiettivo praticabile. Lo **shunning** impedisce che queste comunicazioni raggiungano una rete, riducendo il rischio di un attacco. Se una rete è già compromessa, lo **shunning** può anche impedire che una comunicazione raggiunga il server del criminale, di fatto disarmando il malware.

Servizi formativi con contenuti disponibili sul web sono messi a disposizione per ridurre proattivamente il più grande singolo rischio di sicurezza informatica di qualsiasi società: l'**errore umano**.

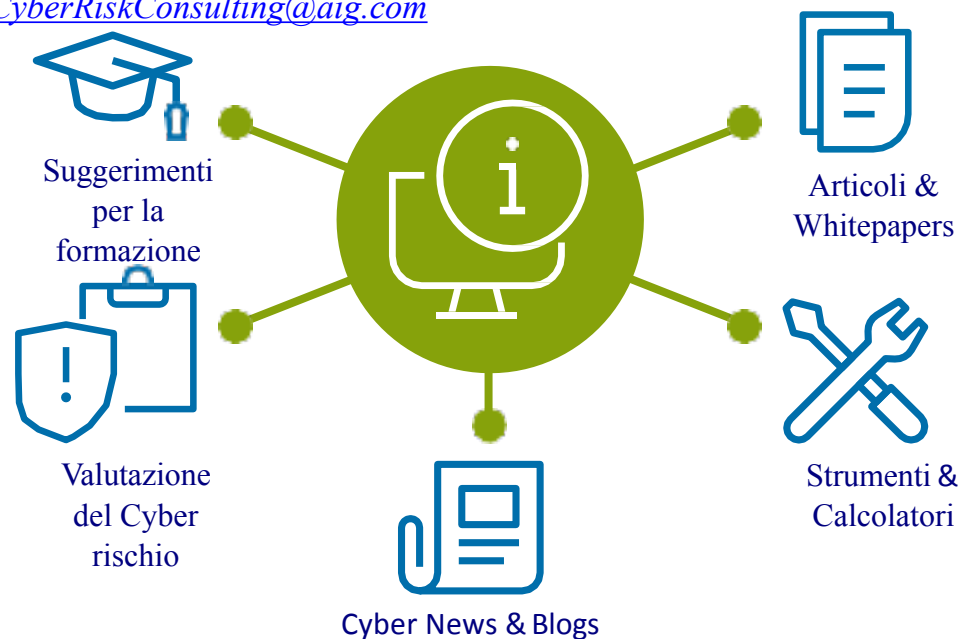


Strumenti e Servizi gratuiti

Portale di Informazione sulla Cyber sicurezza*

Il **portale di informazione sulla Cyber sicurezza** offre accesso online a un hub centralizzato di educazione e tecnica di sicurezza informatica che può aiutare nella prevenzione di una violazione. I contenuti del Portale includono suggerimenti per la formazione, notizie e articoli sul mondo cyber, valutazioni del cyber rischio ed una varietà di strumenti di valore e calcolatori.

Visita il sito dedicato www.aig.com/CyberRiskConsulting e completa il form di contatto o scrivi un'email a CyberRiskConsulting@aig.com



Servizi di AIG Risk Consulting

Un team di consulenti di AIG sui rischi informatici, combinando oltre 50 anni di esperienza nella sicurezza IT, può aiutare i nostri clienti ad anticipare i loro rischi informatici. Il nostro team lavora direttamente con gli assicurati CyberEdge per fornire dettagliate esperienze tecniche e servizi di consulenza.

Tutti gli assicurati CyberEdge hanno la possibilità di accedere ai seguenti servizi a prezzi di favore:



Revisione della Cyber Difesa



Sistemi esposti su Internet
Workshop di simulazione di un incidente



Sintesi esecutiva delle minacce



Studio di Ingegneria Informatica

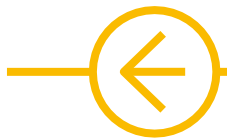


Servizi di AIG Risk Consulting



Revisione delle Cyber Difesa

Il servizio di revisione della cyber difesa di AIG analizza persone, processi e strumenti del cliente che descrivono il loro programma di sicurezza informatica ed identifica i punti di forza e debolezza. I consulenti portano avanti una ricognizione passiva e attiva della vulnerabilità testando i sistemi dei clienti per identificare informazioni che gli attaccanti potrebbero sfruttare.



Ricognizione
passiva



Identificazione
dei punti di
forza e
debolezza

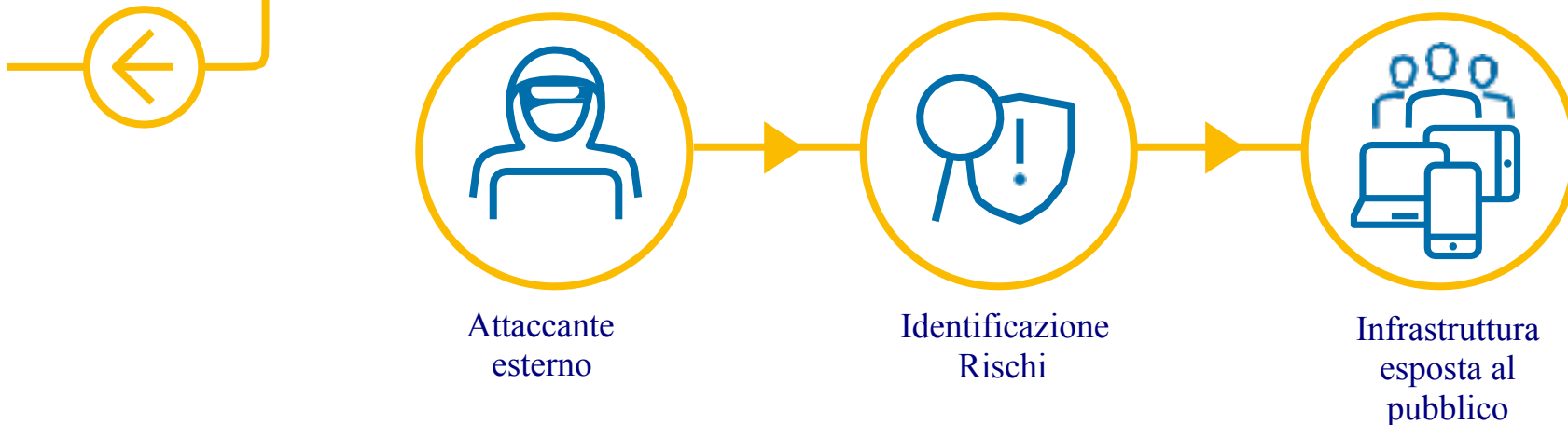


Test attivo della
vulnerabilità

Servizi di AIG Risk Consulting

Sistemi esposti su Internet

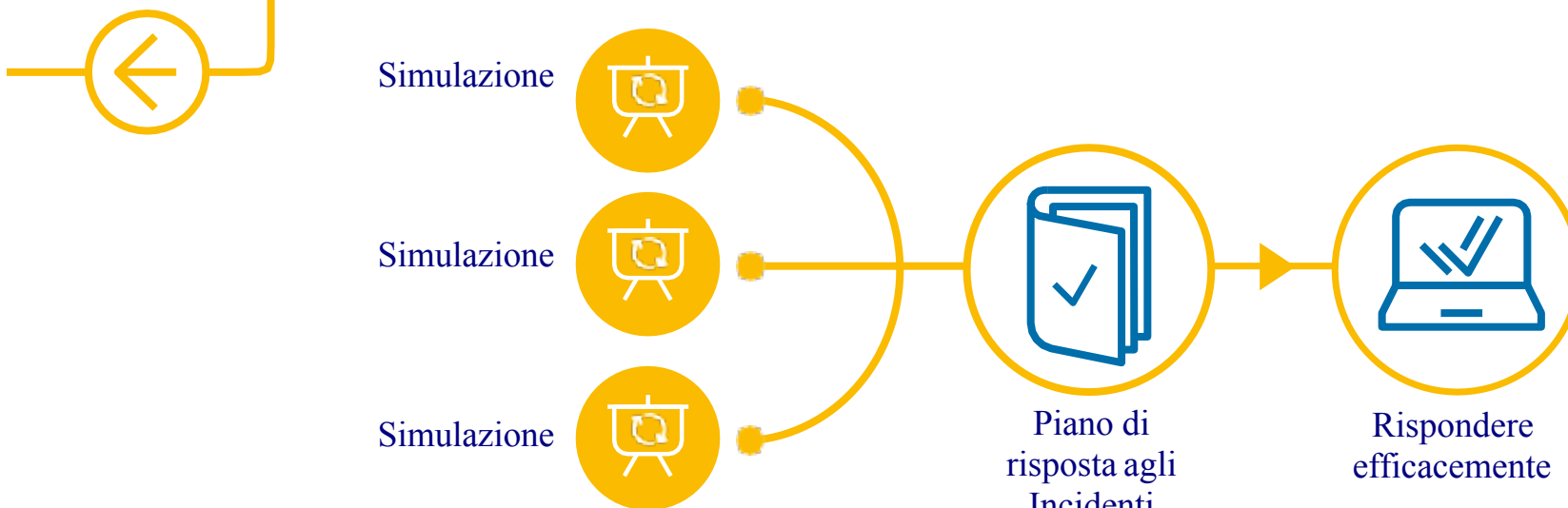
Questo servizio è pensato per aiutare i clienti a identificare i rischi e l'esposizione della loro infrastruttura esposta su internet dalla prospettiva esterna di un attaccante. I consulenti conducono una ricognizione passiva e attiva delle vulnerabilità testando i sistemi del cliente per identificare informazioni che gli attaccanti potrebbero sfruttare.



Servizi di AIG Risk Consulting

Workshop di Simulazione di un incidente

Il nostro workshop di simulazione di un incidente è pensato per aiutare i clienti a perfezionare il loro piano di risposta agli incidenti in modo che la loro organizzazione risponda efficacemente qualora occorra un incidente e per aiutare i clienti a utilizzare al meglio i benefici di CyberEdge. Il cliente ed il consulente di AIG identificano insieme e simulano 2 incidenti adattandoli all'organizzazione del Cliente.

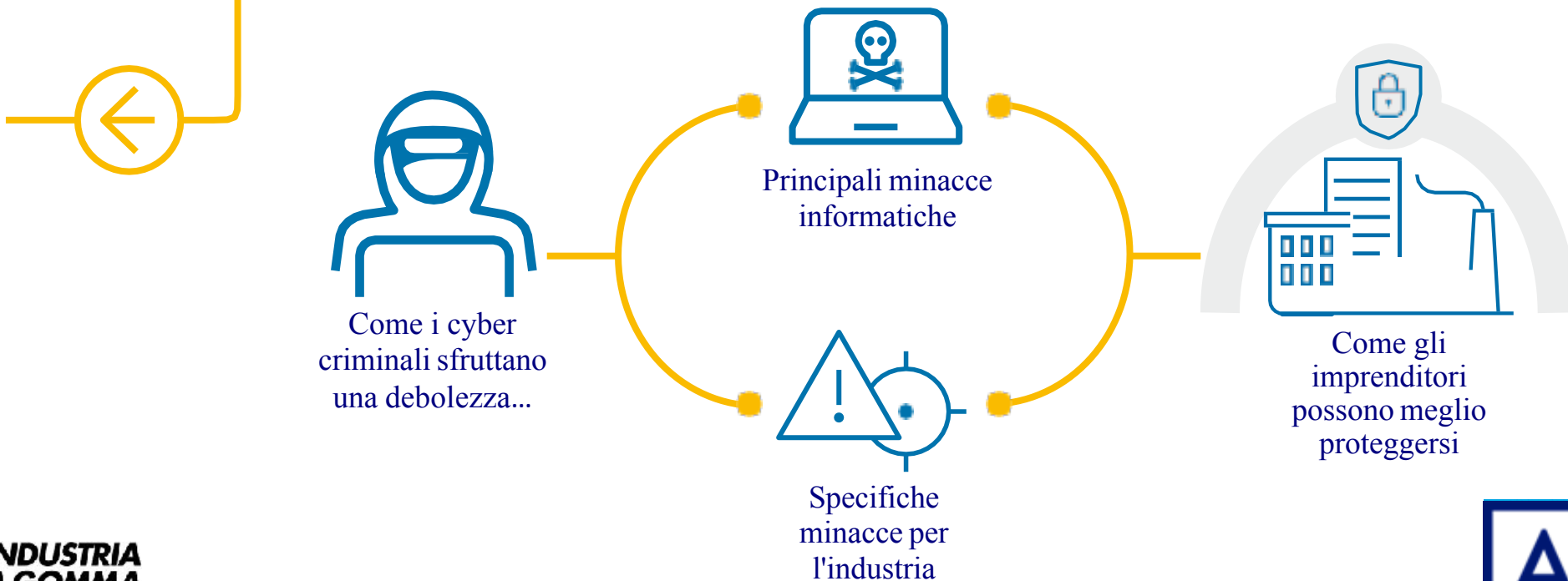


Servizi di AIG Risk Consulting



Sintesi delle minacce per gli Amministratori

Questo workshop è pensato per aiutare gli Amministratori dei nostri clienti a comprendere meglio il panorama delle principali minacce, con specifico riferimento alla loro industria oltre ai metodi attualmente utilizzati dagli attaccanti così che i clienti possano difendere meglio i loro interessi.

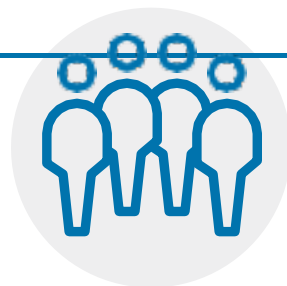


Servizi di AIG Risk Consulting

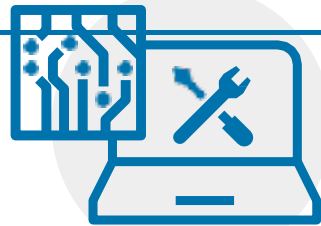
Studio di Ingegneria Informatica

Il nostro Studio di ingegneria informatica analizza persone, processi e strumenti che proteggono i sistemi critici e i controlli industriali del cliente nel loro ambiente. I consulenti rivedranno l'architettura di sicurezza e i processi relativi ai controlli industriali, intervisteranno lo staff per discutere su cosa funziona (e cosa no) e rivedranno registri e altri elementi.

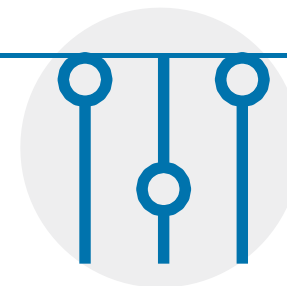
Processi



Persone



Sistemi Critici
&
Controlli Industriali



Controlli

Servizi di Fornitori selezionati

Abbiamo fatto accordi con esperti in rischi informatici per offrire ai nostri clienti servizi aggiuntivi da aggiungere alla loro linea difensiva. Questi servizi sono stati specificamente selezionati sulla base di 20 anni di esperienza e con il fine specifico di rafforzare la maturità in ambito di sicurezza informatica di una società. Tutti i clienti di CyberEdge hanno la possibilità di accedere ai seguenti servizi a prezzi di favore:



Dark Net Intelligence



Cybersecurity Maturity Assessment



Security Ratings



Vendor Security Ratings



Security Awareness Training



SecureDNS



Portfolio Analysis

Servizi di Fornitori Selezionati

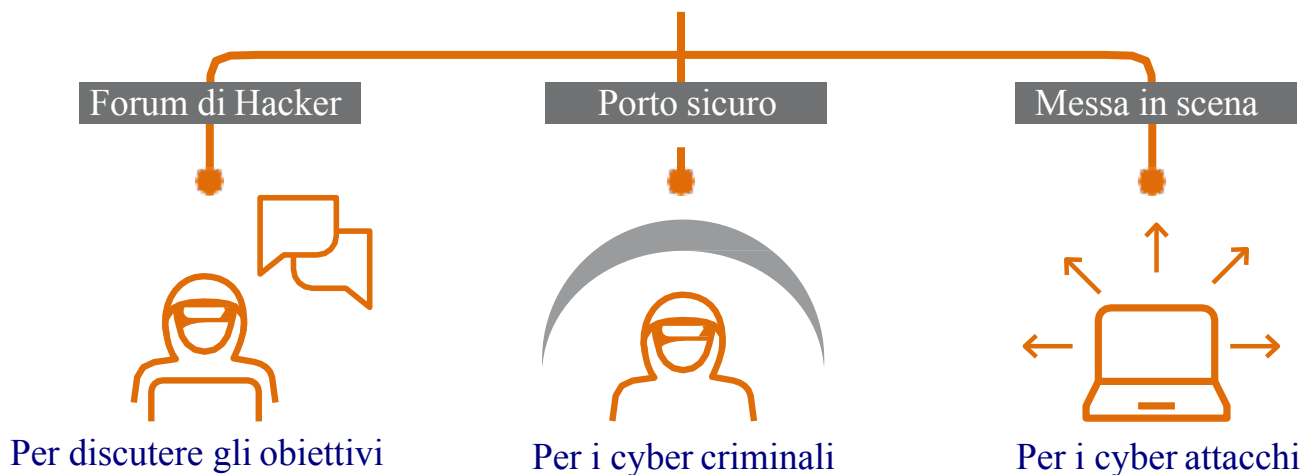


Dark Net Intelligence

Powered by K2-Intelligence

K2 Intelligence lavora con i clienti per tenerli informati sulle più recenti conversazioni che li riguardano effettuate sulla "dark net" (la rete oscura), il mercato nero ed i forum degli hackers. K2 Intelligence monitora la dark net usando motori di ricerca (crawler) e sofisticati strumenti di raccolta dei dati umani per aiutare le società ad adottare un approccio proattivo con riguardo alla gestione dei rischi di cyber sicurezza.

La Rete Oscura



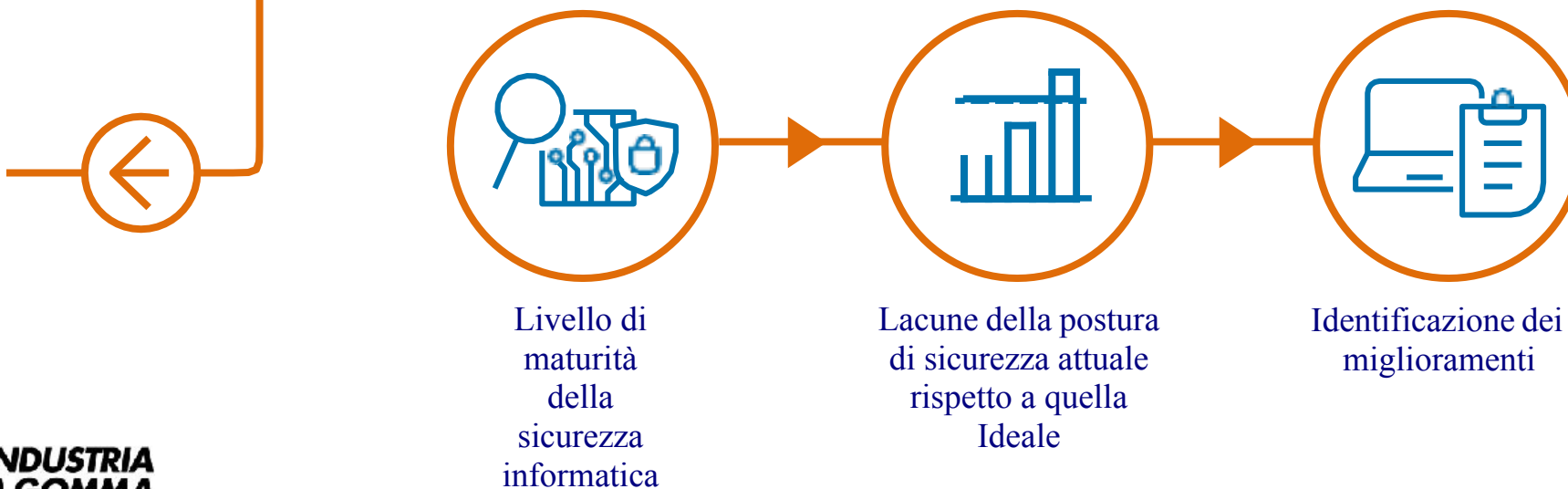
Servizi di Fornitori Selezionati



Cybersecurity Maturity Assessment

Powered by RSA

Tutti gli acquirenti di una polizza CyberEdge ricevono l'accesso per sei mesi alla piattaforma Governace, Risk and Compliance (GRC) di RSA una soluzione per la valutazione dei rischi di sicurezza informatica. Questo è uno strumento che sfrutta la struttura del National Institutes of Standard Technology per valutare la sicurezza informatica e aiuta a identificare le aree di miglioramento. Questo è uno strumento per grandi gruppi o società che gestiscono infrastrutture critiche (come generazione di energia, telecomunicazioni, salute pubblica).



Servizi di Fornitori Selezionati

Security Ratings

★★★ Powered by BitSight Technologies

Bitsight genera giudizi sulla sicurezza delle organizzazioni misurando e monitorando la loro rete e quella dei loro fornitori. I giudizi sono generati senza intrusioni attraverso la continua misurazione da parte di BitSight di dati osservabili dall'esterno. Gli assicurati qualificati* di CyberEdge potranno ricevere un report gratuito di BitSight per misurare le loro prestazione di sicurezza.



Servizi di Fornitori Selezionati

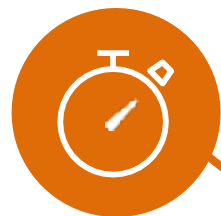


Vendor Security Ratings



Powered by Security Scorecard

I rischi di sicurezza legati a partner, fornitori e venditori sono una grande area che molti tendono a ignorare. Il Vendor Security Ratings fornisce un report che consente alle organizzazioni di misurare e monitorare la sicurezza della propria rete e di quella dei loro fornitori esterni. Questo consente alle organizzazioni di tenere sotto controllo l'ecosistema delle terze parti e prioritizzare gli interventi sui fornitori più rischiosi. Una demo o una prova sono disponibili su richiesta.



Ridurre il tempo di integrazione dei fornitori



Prioritizzare la valutazione dei fornitori



Risolvere le problematiche di sicurezza delle terze parti

Servizi di Fornitori Selezionati



Security Awareness Training

Powered by Wombat Security

Formazione sulla sicurezza per i dipendenti che include esercitazioni sul phishing e simulazioni. Una metodologia unica nel suo genere per la Valutazione, Educazione, Rinforzo e Misurazione della formazione che combina le quattro componenti chiave dei programmi di consapevolezza e formazione per una sicurezza informatica di successo. Una demo o una prova sono disponibili su richiesta.

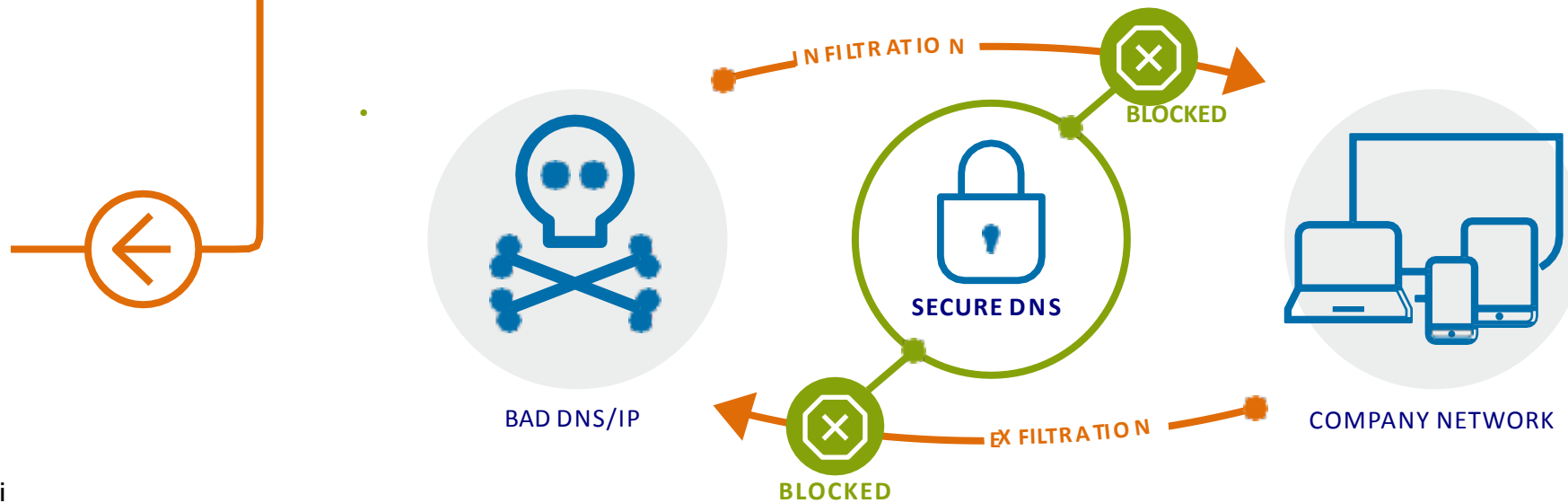


Servizi di Fornitori Selezionati

• SecureDNS

- Powered by Wombat Security

• SecureDNS fornisce una difesa costante contro le minacce basate su "domini" identificando le comunicazioni fatte con domini corrotti, reindirizzando gli utenti su una pagina sicura e respingendo il traffico nocivo su una "dolina" (sinkhole). Questo servizio rimuove il "percorso critico" usato dagli hackers per fare phishing e ingannare gli utenti, consegnare ransomware, infettare i sistemi, rimuovere i dati rubati e causare un cyber-breach.



Servizi di Fornitori Selezionati



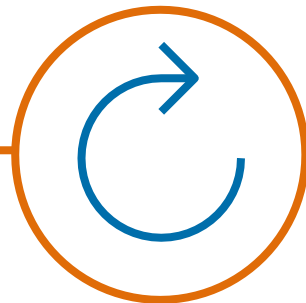
Portfolio Analysis

Powered by AXIO

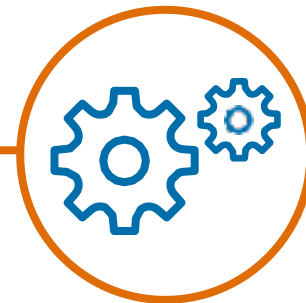
Gli Acquirenti di una polizza CyberEdge possono richiedere a Axio Global una rappresentazione olistica della loro esposizione cyber così da poter meglio armonizzare i loro controlli tecnologici e organizzativi rispetto alla copertura assicurativa. Il metodo di Axio individua tutte le potenziali esposizioni a perdite cyber incluso il furto di dati, la responsabilità, danni alle proprietà ed all'ambiente, danni alle persone (infortuni) e interruzione dell'operatività aziendale.



Quantificazione
Impatto potenziale di
un evento cyber



Ottimizzazione
Trasferimento
del rischio



Implementazione
Effettività controlli

PER ULTERIORI INFORMAZIONI SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SET INFORMATIVO
DISPONIBILE SU RICHIESTA PRESSO LA COMPAGNIA E GLI INTERMEDIARI AUTORIZZATI

MILANO
Piazza Vetra, 17 20123 Milano

Tel: 02 36901
michele.lavaggi@aig.com
monica.orlando@aig.com
erika.chemello@aig.com

www.aig.com



American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange. Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. Products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

AIG Europe Limited is registered in England; company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. AIG Europe Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 202628). This information can be checked by visiting the FSR register (www.fca.org.uk/register).