L'Accademia del Cyber

Prefazione
A cura di ANRA

La pandemia ha amplificato l'importanza della IT & cyber resilience per le organizzazioni sia a fronte del massivo impiego della modalità di remote working - che ha esteso la superficie di attacco - sia per l'accelerazione del processo di digitalizzazione e automazione in atto. Ne consegue che si ponga maggiore enfasi sulla necessità di un'infrastruttura IT resiliente e sicura, oltre a far considerare ulteriori misure di sicurezza dei sistemi.

Pertanto, le organizzazioni, per sopravvivere in questo contesto sempre più complesso ed erratico devono investire maggiormente in resilienza, a tutti i livelli, in modo tale da creare un ecosistema più flessibile e sicuro, focalizzandosi sempre più sulla cyber resilience, ossia, sulla capacità di anticipare, resistere e riprendersi da eventi cyber avversi e inattesi che possono compromettere l'operatività dell'organizzazione.

In quest'ottica ANRA ha voluto farsi promotrice di un ciclo di webinar sulla cyber security volto illustrare le tematiche più importanti ed accompagnare le organizzazioni nella "selva oscura" del mondo cyber per conoscere meglio il "nemico", per imparare a difendersi dagli attacchi ransomware e dal social hacking. Senza dimenticare le sfide che si devono affrontare nell'implementazione del cloud ibrido e quanto sia importante individuare quali coperture assicurative considerare per proteggere l'organizzazione.

Si tratta di costruire un modello di business resiliente, "antifragile" così come descritto da Nassim Nicholas Taleb nel suo libro "Antifragile, prosperare nel disordine" che presuppone l'adozione di discipline strategiche come il risk management, la business continuity e la cyber security in un mondo sempre più data-driven. È quanto mai urgente diffondere la cultura digitale all'interno dell'organizzazione e la programmazione di training ad hoc per dotare il personale degli skill necessari per l'utilizzo adeguato della tecnologia implementata.

"ANRA vuole essere a fianco dei propri soci, delle organizzazioni, dei vari attori istituzionali e governativi – afferma il presidente Carlo Cosimi – soprattutto in questo momento di ripresa delle attività e deli investimenti strategici del Recovery Fund. Vogliamo metterci a disposizione delle organizzazioni ed aiutarle a raggiugere la resilienza necessaria per poter rispondere prontamente alle sollecitazioni contingenti ed affiancarle nel far fronte alle sfide ed ai rischi cyber. Gli scenari in cui ci troviamo a vivere richiedono una risposta subitanea e una resilienza strutturata. Non possiamo più attendere l'inaspettato, è ora di essere proattivi e anticipare l'inaspettato".

Federica Maria Rita Livelli
Consigliera ANRA

Introduzione

Il **Cyber Risk** è una minaccia in continua evoluzione che può colpire qualsiasi attività e organizzazione. Richiede risorse adeguate per prevenire e mitigare le conseguenze di eventuali attacchi.

Le violazioni dei dati rimangono gli eventi più frequentemente segnalati in ambito cyber con importanti effetti finanziari. Inoltre, le violazioni di dati effettuate da terzi (in contrapposizione alle violazioni accidentali di dati da parte dell'azienda o violazioni di dati effettuate da dipendenti infedeli) sono il tipo più frequente e più costoso di perdita di dati.

La ricerca **"The State of Ransomware 2021"** di Sophos, ha evidenziato come nel nostro Paese **più del 30% delle aziende è stata vittima di ransomware nel corso dell'ultimo anno**. In quasi il 60% dei casi l'attacco è stato sventato prima che potesse compromettere la sicurezza e la disponibilità dei dati, mentre nella restante percentuale dei casi le aziende hanno visto i propri dati crittografati e quindi impossibili da utilizzare, oltre che nella piena disponibilità degli hacker autori dell'attacco.

Il ransomware si riconferma la minaccia per eccellenza nel panorama della sicurezza informatica a livello globale, anche nel periodo Gennaio-Maggio 2021. È quanto emerge dalla ricerca di Tinexta Group, che ha monitorato e analizzato gli attacchi verificatisi nei primi cinque mesi di quest'anno.

Dalle considerazioni del contesto attuale nasce **CyberBrain**, il progetto per affrontare la minaccia cyber da diverse angolazioni e prospettive rispondendo ai diversi bisogni di cui ciascuna azienda necessita.

CyberBrain è un progetto in grado di autofinanziare l'investimento nella protezione cyber, nel trasferimento del rischio in caso di incidenti e nel garantire la continuità del business. **CyberBrain** è costituito da un **ecosistema di attori** in stretta relazione tra loro in grado di intervenire a complementarietà in differenti aree aziendali e con differenti competenze: **Cosman**, **OGR**, **HRC** e **Willis Towers Watson**.

Ciascun partner contribuisce a fornire elementi fondamentali per ottenere una sicurezza informatica.

Il progetto adotta una formula che consente di investire in:

- **INFRASTRUTTURA**: dedicata al data center, attraverso Servizio Cloud, Hybrid Cloud e Colocation e servizio di back up disaster recovery per la replica remota dei dati aziendali;
- **CYBER SECURITY**: attraverso la protezione di quello che oggi è il vero patrimonio aziendale, i dati, da minacce ed attacchi informatici, in differenti modalità;
- **CYBER INSURANCE**: per trasferire l'impatto economico degli incidenti informatici e garantirsi il supporto di esperti nella risoluzione della crisi;
- **BUSINESS CONTINUITY**: capacità e rapidità nel continuare ad erogare prodotti e servizi a valle di un evento distruttivo.

CyberBrain prevede la possibilità di recuperare le risorse necessarie attraverso un'attività di digital cost management in grado di efficientare quelle aree aziendali dove possono "insediarsi" inefficienze per gli investimenti in cyber insurance, cyber security e business continuity.

Da questo progetto nasce **"L'Accademia del Cyber"**, un percorso di quattro eventi organizzato in collaborazione con **ANRA – Associazione Nazionale Risk Manager**, dedicati alla cyber security e alla sua modalità di finanziamento.

Il percorso ideato intende fornire consapevolezza concentrandosi su quattro tematiche specifiche per disegnare una prospettiva allargata:

1. **Conosci il nemico**
2. **Sfida al ransomware**
3. **Social Hacking**
4. **Hybrid Cloud**

In questo documento sono raccolti gli estratti degli interventi dei relatori e le considerazioni emerse nel corso delle puntate. Inoltre, è possibile trovare alcuni dati e statistiche sui quesiti posti durante gli eventi accompagnati da un breve commento degli specialisti. Nel percorso de "L'Accademia del Cyber" è intervenuto Agostino Ghiglia, Componente del Garante per la protezione dei dati personali, per trattare il tema della resilienza del dato e dimostrare l'importanza della figura del responsabile della protezione dei dati (RPD) quale figura strategica per una corretta e serena gestione aziendale, che prevenga, nei limiti del possibile, perdite, fughe, furti, uso improprio dei dati dei lavoratori; accadimenti che potrebbero avere come conseguenza ispezioni e sanzioni a norma del GDPR.

Speriamo quindi con questa iniziativa di poter contribuire ad un dibattito sulla cyber security offrendo una prospettiva allargata.

Marco Olivieri
Marketing & Communication Manager
Willis Towers Watson

La resilienza del dato dal punto di vista del garante

Agostino Ghiglia
Componente Collegio del Garante per la protezione dei dati personali

Fino a qualche anno fa, pensando ad un'azienda, si poneva l'attenzione esclusivamente alla tutela del lavoratore o della lavoratrice, alla sicurezza sui luoghi di lavoro. Oggi è fondamentale prendersi cura, oltre che della persona fisica, anche della "persona-dato", ossia di tutti quei dati personali, più o meno sensibili, che ogni giorno vengono trattati in un ambiente lavorativo. A tal proposito, è fondamentale che ogni azienda che tratta a vario titolo dati, si doti di un bravo RPD e sottolineo il termine "bravo" poiché tale ruolo è diventato (e sarà sempre di più) strategico per una corretta e serena gestione aziendale che prevenga, nei limiti del possibile, perdite, fughe, furti, uso improprio dei dati dei lavoratori; accadimenti che potrebbero avere come conseguenza ispezioni e sanzioni a norma del GDPR.

Il fatto che il nuovo Regolamento sia recente e che i lunghi mesi di emergenza pandemica abbiano portato il Garante a sospendere le ispezioni onde non gravare ulteriormente le difficoltà delle aziende, non deve ingenerare un sentimento di sottovalutazione relativamente al trattamento dei dati. Occorrerà quindi non considerare la privacy come un orpello inutile e senza conseguenze e, di conseguenza, sarebbe opportuno tutelarsi non indirizzandosi verso scelte "low cost" di scarsa professionalità tenendo anche conto che l'evoluzione tecnologica esige dei Responsabili della Protezione dati sempre più multidisciplinari.

La violazione dei dati personali (data breach) è, a termini del Regolamento, una violazione di sicurezza "che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Le notifiche di "violazioni dei dati", che vanno indirizzate al Garante entro 72 ore, sono state 1.443 nel 2019 e 1.387 nel 2020 mentre, nei primi tre mesi del 2021, siamo a 413. Sono numeri importanti che, tuttavia, a mio avviso non fotografano il problema con la dovuta esattezza. Il timore delle sanzioni porta e ha portato un significativo numero di titolari ad omettere le notifiche, omissione che ha sempre avuto come conseguenza un aggravamento delle posizioni.

Il consiglio, quindi, è di non nascondere la "polvere (di dati) sotto il tappeto" ma di notificare con tempestività le violazioni al Garante offrendo una collaborazione totale e trasparente cui si dà grande importanza nella commisurazione delle eventuali sanzioni.

Il Garante, a seguito della notifica, può prescrivere misure correttive prevedere sanzioni pecuniarie fino a 10 milioni di Euro o, nel caso di multinazionali, fino al 2% del fatturato annuo mondiale.

Per evitare incidenti di percorso e per costruire, sin dall'inizio, una "privacy by design" ossia un trattamento dei dati adeguato alla normativa europea e nazionale sulla privacy, è consigliabile, oltre a quanto sopra detto, una valutazione d'impatto sul trattamento dei dati dei lavoratori e dei dati che, in tutto o in parte, costituiscono il business dell'azienda.

Tale valutazione, unita ad una attenzione particolare e, vorrei dire, indispensabile, alla cyber sicurezza quindi ai sistemi di protezione costruiti a tutela dei dati, dovrebbe rappresentare una "buona pratica" (che in realtà dovrebbe diventare una "ordinaria pratica") per tutte le aziende che in qualche modo gestiscano dati.

Un recente spot del Garante recita : " i tuoi dati sono un tesoro". I dati di tutti (personali e "dati - business") sono un tesoro e, come tale, vanno trattati, conservati adeguatamente, tutelati e difesi. Il Garante , attraverso la collaborazione permanente con tutte le Istituzioni pubbliche , un'interlocuzione fruttuosa con le varie entità portatrici di interessi collettivi, anche mediante l'ausilio di FAQ settoriali sugli argomenti privacy di maggior interesse e con la partecipazione dei suoi componenti ad un numero elevatissimo di incontri , tenta di difendere quel "tesoro" e di diffondere una nuova cultura della privacy che, in quanto protezione dei nostri dati, rappresenta un vero e proprio scudo per la nostra libertà.

Agostino Ghiglia
Componente Collegio del Garante
per la protezione dei dati personali

L’ecosistema

CyberBrain è un progetto in grado di autofinanziare l’investimento nella protezione cyber, nel trasferimento del rischio in caso di incidenti e nel garantire la continuità del business.
L’ecosistema è costituito da attori in stretta relazione tra loro in grado di intervenire a complementarietà in differenti aree aziendali e con differenti competenze.

Una soluzione integrata e modulare di cyber security e protezione dei dati

FINANZIAMENTO

DIGITAL COST MANAGEMENT

Miglioramento dell’efficienza economica ed eliminazione dei costi aziendali superflui

INFRASTRUTTURA TECNOLOGICA

DATA CENTER

Servizio Cloud, **Hybrid Cloud** e Colocation e servizio di **back up disaster recovery** per la replica remota dei dati aziendali

RIPRISTINO DEI PROCESSI AZIENDALI

BUSINESS CONTINUITY

Capacità e rapidità nel **continuare ad erogare prodotti e servizi** a valle di un evento distruttivo

PROTEZIONE DAGLI ATTACCHI

CYBER SECURITY

Massima protezione di quello che oggi è il vero patrimonio aziendale, **i dati**, **da minacce ed attacchi informatici**, in **differenti modalità**: **azioni simulate** o **reali**, **esecuzioni** in **modalità proattiva** o **reattiva**, **approcci attivi** o **passivi**

COPERTURA ASSICURATIVA

CYBER INSURANCE

Cyber insurance per **trasferire l’impatto economico** degli incidenti informatici e garantirsi il **supporto di esperti** nella risoluzione della crisi

I partner dell'iniziativa

COSMAN
cost management

Azienda specializzata nella realizzazione di progetti di Digital Cost Management capaci di ottimizzare i costi aziendali, migliorando l'efficienza e massimizzando i risultati. Offre servizi che liberano risorse da aree a basso valore aggiunto da dedicare ad aree strategiche, come la cybersecurity.

ogr

È sede dell'OGR Data Brain, datacenter TIER3 per la custodia e replica del dato. OGR, con i suoi 35.000 mq di contemporaneità, arte e innovazione, è un esempio unico di riqualificazione urbana. Dal 2019 inaugura OGR Tech, hub internazionale tecnologico unicum in Italia.

HRC
IT SOLUTIONS AND CONSULTING

Azienda informatica presente a Torino da più di 20 anni. Ha al suo interno un laboratorio di ricerca e si occupa di sviluppo software, architettura progetti, servizi e consulenza specialistica e certificata in ambito IT. Per CyberBrain offre una gestione evoluta del dato con disaster recovery Integrato e un servizio di CyberSecurity Intelligence per mettere al sicuro le aziende dagli attacchi informatici.

Willis Towers Watson

Società di consulenza e brokeraggio globale che aiuta clienti di tutto il mondo a trasformare i rischi in un percorso di crescita. Progetta e fornisce soluzioni per la gestione del rischio, l'ottimizzazione dei benefits e lo sviluppo dei talenti che rinforzano il capitale e proteggono le aziende e le persone.

Le aree di attività

DIGITAL COST MANAGEMENT

Cosman da oltre 20 anni è la società leader in Italia nei servizi per il **miglioramento della gestione dei costi**.
Libera rapidamente risorse già presenti nell'organizzazione del Cliente apportando:

- Tecnologia
- Metodo efficace
- Specialisti autorevoli
- Best practices

Le aree coinvolte sono costi del personale, costi tecnici, costi logistici ed costi di struttura che grazie all'applicazione della piattaforma digitale SHAPER® vengono «modellati» per: controllarne l'evoluzione nel tempo, ottimizzarne in modo continuativo la gestione, semplificarne la gestione incrementando le competenze del personale interno.

DATA CENTER

HRC gestisce e manutiene il Datacenter Tier 3 ubicato in OGR.
Resilienza del dato con repliche sicure (backup primari e copie di terzo livello). Garanzia di inalterabilità del dato, anche contro attacchi ransomware.

I dati sono conservati in un ambiente sicuro con più livelli di **protezione**: **fisica** (location in DataCenter Tier 3 e infrastruttura con server iperconvergenti), **logica** (sicurezza perimetrale, criptazione e segregazione degli ambienti), **software** (sistemi antimalware, intelligenza artificiale e deep learning contro minacce note e sconosciute).

CYBER SECURITY

HRC offre la sua consulenza per salvaguardare il patrimonio aziendale del XXI secolo: i dati. Poche macrofasi progettuali, semplici e modulabili in base alle vostre concrete esigenze, per avvicinarvi quanto più possibile al 100% di resilienza verso le minacce, gli attacchi informatici ed i data breach, attraverso sistemi intelligenti di Cybersecurity certificabili, affidabili e robusti.

Offriamo servizi di verifica e test del livello di sicurezza esistente, dall'analisi della vostra Digital Presence aziendale sul Dark Web sino alle esclusive piattaforme di Cyber Intelligence e di Endpoint Protection avanzate, progettate e configurate per le diverse tipologie di aziende e Pubbliche Amministrazioni.

CYBER INSURANCE

Willis Towers Watson è una delle principali società globali di consulenza, intermediazione e soluzioni aziendali.

Protezione tramite trasferimento assicurativo dalle conseguenze finanziarie di **minacce ed attacchi informatici** e supporto nella **gestione di cyber eventi** tramite accesso ad un **panel di specialisti** (legali, forensi, IT, negoziatori, PR, etc.) per limitare gli eventuali impatti di una crisi.

Copertura di costi e di richieste di indennizzo di soggetti terzi danneggiati.

BUSINESS CONTINUITY

Willis Towers Watson aiuta i clienti di tutto il mondo a trasformare i rischi in un percorso di crescita.

Costituzione di un sistema di supporto decisionale che renda in grado l'organizzazione di **far ripartire i propri processi/servizi** più critici, esposti ai rischi più rilevanti, **in maniera tempestiva** e coordinata a valle di un evento distruttivo.

In collaborazione con

ANRA

Il percorso
L'Accademia del Cyber

Un percorso dedicato ai temi della Cyber Crime e Cyber Security, inserito in un calendario di eventi formativi su temi specifici con la partecipazione di prestigiose personalità nell'ambito dei rischi cyber.

La trasformazione digitale ha coinvolto le organizzazioni a 360° ponendole di fronte ad una visione globale dei processi in azienda. Conoscere come agiscono gli hacker può rivelarsi fondamentale, così come avere un piano di risposta tempestivo in caso di attacco, unito alle corrette coperture assicurative.

A seguito di una panoramica del fenomeno del ransomware e del phishing, poniamo l'attenzione sui costi che un'azienda deve fronteggiare in caso di attacco. Le giuste coperture assicurative cyber garantiscono alle aziende una tutela adeguata, accompagnata ad azioni di mitigazione e un piano che garantisca la business continuity.

Clicca sulle sezioni e vai alle **pagine dedicate**

Conosci il nemico
01

Sfida al Ransomware
02

È bene conoscere quali sono le azioni fondamentali di cybersecurity e cosa succede quando ad essere "hackerate" sono le persone, i loro dati e informazioni sensibili. Il tema della reputazione è strettamente collegato ed è importante farsi trovare pronti: una corretta comunicazione può limitare gli impatti negativi, e in caso di crisi, il settore assicurativo può offrire supporto tramite consulenti esperti.

Il Social Hacking
03

Hybrid Cloud
04

Sfruttare e ottimizzare diversi tipi di piattaforme cloud, proteggere in modo efficace i dati e rielaborarli più rapidamente: sono solo alcuni dei vantaggi offerti dall'hybrid cloud. Mantenere la qualità dei dati, sviluppare la resilienza sarà una capacità sempre più strategica per le aziende. Unita al controllo dei propri rischi, la maturità in termini di gestione dei dati può portare a dei vantaggi anche nel processo di sottoscrizione assicurativa, soprattutto in un periodo di hard market.

01
Conosci il nemico

Rivedi la puntata

La Cyberevolution

Nino D'Amico, CTO - HRC S.r.l.

La trasformazione digitale ha favorito il rinnovamento della figura dell'IT Manager in azienda. Come cambia il suo ruolo e quali sono le sue nuove competenze? L'IT Manager dispone oggi di una visione globale dei processi in azienda, per poter garantire un supporto adeguato all'intera struttura e assicurare una stretta e fruttifera collaborazione tra area tecnica e resto dell'organizzazione. L'IT ha acquisito un ruolo sempre più centrale nella strategia di business, portando l'IT Manager ad assumere molta più importanza nell'ambito del management aziendale. Digitalizzazione dei processi, corretto utilizzo dei software a disposizione, integrazione tra i sistemi informativi: tutto ciò coinvolge allo stesso modo aree differenti, le quali hanno bisogno di essere guidate e supportate da un management con una visione a 360° di ciò che avviene in azienda.

Conosci il nemico

Marco Ivaldi, Technical Director - HN Security

La cyber security è un processo continuo che dovrebbe essere parte di tutto ciò che fai. Tuttavia, nessuno ha le risorse per fare tutto in modo perfetto. Dunque, l'obiettivo da parte di chi rischia di essere attaccato, cioè qualsiasi azienda, deve essere il miglioramento costante. Dal punto di vista dell'attaccante il primo obiettivo è quello di identificare potenziali target per la sua missione. Gli attaccanti sono spesso motivati dal guadagno economico, dall'accesso a informazioni sensibili o dal danno al brand.

Business Continuity Management

Valentina Visconti, Senior Risk Consultant, Deputy Manager R&A Italy - Willis Towers Watson

Nonostante gli attacchi cyber abbiano raggiunto la loro "notorietà" soprattutto in conseguenza della violazione della riservatezza di dati personali, è indispensabile sottolinearne anche la capacità distruttiva nei confronti della continuità dei sistemi informatici e – in ultima analisi - dell'azienda stessa. E' quindi indispensabile mitigare il rischio di un attacco con le tecniche più avanzate e sviluppare le conseguenti strategie di risposta, ma è necessario che queste strategie siano sempre più collegate con il sistema di gestione della continuità operativa (BCMS) dell'azienda, in modo che anche in caso di eventi cyber, l'azienda sia in grado rispondere tempestivamente ed in maniera efficace e, nel caso peggiore di compromissione della disponibilità dei sistemi IT, mantenere comunque ad un livello di servizio accettabile i propri processi critici.

Gestione e trasferimento del rischio cyber

Camilla Brena, Head of Cyber Risk, FINEX Italy - Willis Towers Watson

I rischi residui sono quei rischi che rimangono alla fine del processo virtuoso: una volta conosciuti, valutati e analizzati i rischi, dopo aver implementato strategie che permettono di controllarli e mitigarli e aver predisposto piani ad hoc, che permettono di gestire al meglio un eventuale incidente informatico e di ridurne gli impatti dannosi, qualcosa rimane sempre fuori da ogni tentativo di controllo. Qualunque sia la cura e professionalità che si impiegano nelle attività precedentemente descritte, i rischi non sono azzerabili. Alla fine del ciclo virtuoso rimane una – pur ridotta - serie di rischi che ogni organizzazione deve considerare. La buona notizia è che una buona parte di questi rischi è trasferibile agli assicuratori..

Cosa è emerso durante la puntata?

La vostra organizzazione ha una polizza cyber?

44%

dichiara di avere una polizza cyber

20%

dichiara di non avere una polizza cyber, ma è in attesa di quotazioni per valutarla

Il commento dell'esperto

Camilla Brena
Head of Cyber Risk, FINEX Italy
Willis Towers Watson

"Sommando chi ha già una polizza cyber e chi ne sta valutando l'acquisto, si raggiunge una percentuale del 64%: evidente l'importanza assunta, negli ultimi mesi, da questo tipo di protezione assicurativa."

Il commento dell'esperto

Camilla Brena
Head of Cyber Risk, FINEX Italy
Willis Towers Watson

"Il successo di un attacco cyber dipende generalmente da un mix di cause tra cui – come correttamente evidenziato dalla platea – sono correlate innanzi tutto al comportamento umano.

La gestione virtuosa dei rischi cyber infatti richiede un forte impulso sulla formazione e creazione di consapevolezza tra il personale, che deve accompagnare la conoscenza dei rischi e l'utilizzo di procedure e strumenti tecnologici adeguati e sempre aggiornati."

Qual è, secondo voi, la maggiore vulnerabilità?

47%

errore umano o distrazione

45%

sistemi e procedure di difesa non adeguati

Nota metodologica
I dati e le percentuali presenti in questo documento sono il risultato di survey in tempo reale poste nel corso dei webinar de "L'Accademia del Cyber" svolti nel mese di Giugno 2021.

02
Sfida al ransomware

Rivedi la puntata

Sfida al ransomware

Walter Narisoni, Sales Engineer Manager - SOPHOS

Il ransomware è una forma di software dannoso (denominato anche “malware”) che ha la capacità di bloccare un computer o una rete, negando l’accesso degli utenti ai dati. Dopo l’installazione del malware, l’hacker richiede un riscatto alla vittima, promettendo di ripristinare l’accesso ai propri dati solamente dopo aver ricevuto il pagamento. Ovviamente, la promessa non è sempre mantenuta...

Attacchi phishing

Walter Narisoni, Sales Engineer Manager - SOPHOS

La forma più comune di phishing è quella generica, di tipo mass-mailed e spesso supportato da botnet, in cui qualcuno invia un’e-mail fingendo di essere qualcun altro e cerca di ingannare il destinatario intimandogli di compiere una specifica azione (di solito indirizzando la vittima a un sito web malevolo o scaricando malware). Come difendersi?

Business Continuity Management

Valentina Visconti, Senior Risk Consultant, Deputy Manager R&A Italy - Willis Towers Watson

In alcuni casi gli effetti di un attacco ransomware possono essere significativamente mitigati grazie all’adozione di un piano di gestione della Business Continuity. Certamente il ransomware può compromettere la fruibilità e funzionalità di uno o più sistemi informativi ma la vera domanda che ci dobbiamo porre è: come è possibile che l’interruzione di uno o più sistemi arrivi a giocare un ruolo così determinante nell’operatività complessiva dell’azienda? È ancora possibile che lo scenario “indisponibilità dei servizi ICT” non sia stato contemplato ed indirizzato nel BCMS?

Gestione e trasferimento del rischio cyber

Camilla Brena, Head of Cyber Risk, FINEX Italy - Willis Towers Watson

Le Garanzie attivabili in caso di eventi complessi: l’ambito cyber è in continua evoluzione. Se è vero che le organizzazioni hanno imparato a difendersi dai tipici attacchi ransomware degli scorsi anni, i criminali hanno elaborato tecniche di attacco più evolute per aumentare le probabilità di successo e oggi sono frequenti i cosiddetti attacchi duplici.
Quali sono le protezioni che può garantire una buona polizza cyber anche in questo caso? E in quale modo anche gli assicuratori stanno modificando la loro offerta per proteggere il settore, cercando di coinvolgere maggiormente gli assicurati nell’adottare maggiori precauzioni.

Cosa è emerso durante la puntata?

Investite nella formazione sulla cybersecurity dei vostri utenti?

33%

ha un programma continuo di formazione

34%

dichiara di non aver mai stanziato budget per questo tipo di formazione

Il commento dell'esperto

Walter Narisoni
Sales Engineer Manager
SOPHOS

"L'anello debole della sicurezza è indubbiamente l'utente e gli attaccanti lo sanno, infatti utilizzano molte tecniche di attacco legate al social engineering.

Investire nella formazione è importante per diminuire la probabilità che un utente possa sbagliare e mettere a rischio la sicurezza dell'azienda.

Dalla survey però si nota che 1 azienda su 3 non investe nella formazione delle proprie risorse mettendo così in pericolo l'azienda stessa e i dati che custodisce."

Il commento dell'esperto

Valentina Visconti
Senior Risk Consultant, Deputy Manager R&A Italy
Willis Towers Watson

"Le risposte evidenziano una certa mancanza di maturità nella cultura della continuità.

Avere investito in "logiche" di continuità ma non aver fatto quagli sforzi – necessari - che consentano ai sistemi di funzionare nella realtà quando attivati, è un'opportunità persa che le aziende dovrebbero cogliere in un'ottica di miglioramento continuo e di resilienza di lungo termine."

Avete sistemi di Business Continuity in essere?

27%

dichiara di non avere sistemi di Business Continuity

49%

dichiara di avere sistemi di Business Continuity, di cui il 50% non adeguatamente formalizzati

Nota metodologica
I dati e le percentuali presenti in questo documento sono il risultato di survey in tempo reale poste nel corso dei webinar de "L'Accademia del Cyber" svolti nel mese di Giugno 2021.

03
Il Social Hacking

Rivedi la puntata

Il Social Hacking

Nino D'Amico, CTO - HRC S.r.l.

Gli attacchi informatici alle aziende sono diventati sempre più frequenti e in alcuni casi hanno determinato la chiusura di alcune di loro. Per ridurre il cyber risk è necessario dotarsi di soluzioni di sicurezza informatica di ultima generazione ed attuare una serie di azioni al fine di prevenire cyber attacchi ed accessi non autorizzati da parte di hacker alle risorse business critical.

Azioni fondamentali per la cybersecurity:

- Applicare gli ultimi aggiornamenti software non appena disponibili;
- Informare i dipendenti riguardo i pericoli derivanti dalle e-mail di phishing e altre minacce informatiche attraverso comunicazioni, newsletter e corsi;
- Verificare e organizzare i sistemi e i processi di backup e disaster recovery.
- Studiare un piano di risposta per eventuali attacchi informatici, definire i ruoli delle parti interessate in azienda ed effettuare dei test per verificarne l'efficacia.

Formazione cyber e gestione delle emergenze

Alessandro Scarafile, VP Cyber Security & Operations - Syneto

Hackerare significa violare i sistemi informatici per averne l'accesso completo e fare quello che si vuole, per hackerare un sistema servono delle conoscenze che spaziano dal mondo dei computer, sistemi operativi, le reti e la sicurezza informatica. Hackerare un sistema significa quindi violarlo usando le proprie conoscenze informatiche, ma non sempre l'obiettivo di un hacker è violare i sistemi informatici, molto spesso infatti l'obiettivo può essere quelli di rendere le persone vittime di sé stesse violando dati e informazioni personali sensibili. Le conseguenze oltre che materiali possono diventare psicologiche. Come difenderci?

Crisis Management: come gestire la comunicazione in caso di crisi

Valentina Visconti, Senior Risk Consultant, Deputy Manager R&A Italy - Willis Towers Watson

Le organizzazioni sono sempre più dipendenti dai sistemi informativi, tra loro interconnessi, spesso affidati a terzi e sempre più spesso soggetti ad attacchi cyber. Questo contesto rende sempre più probabile che in un'organizzazione - prima o poi - si verifichi un incidente, anche in ambito IT, che meriti la definizione di "crisi": si sviluppa in un periodo di tempo limitato, incide sulla capacità di un'azienda di raggiungere i propri obiettivi, spesso comporta significative perdite finanziarie o di reputazione e richiede quasi sempre una risposta interfunzionale e organizzativa immediata. È chiaro quindi che in queste occasioni sia fondamentale un approccio lungimirante e sistematico per far sì che l'azienda sia pronta ad affrontare tutte le conseguenze del caso. Il team di gestione delle crisi deve disporre di solide linee guida, che consentano di coordinare efficacemente il processo di comunicazione interna ed esterna.

Cyber insurance: il supporto di esperti per limitare gli impatti negativi sulla reputazione

Camilla Brena, Head of Cyber Risk, FINEX Italy - Willis Towers Watson

Le polizze assicurative cyber sono prima di tutto delle polizze di servizio. Nel momento della crisi offrono - direttamente o indirettamente - il supporto concreto e decisivo di un gruppo di consulenti esperti nella gestione dell'evento. In ambito cyber, difficilmente l'assicuratore potrà coprire i danni derivanti dalla perdita di reputazione e quindi dalla perdita di clienti, fatturato e valore. Invece fornirà il supporto di esperti che potranno guidare l'Assicurato nel compiere le azioni più adeguate in modo da limitare al massimo l'impatto negativo sulla reputazione. La differenza tra un evento disastroso e una crisi passeggera dipende anche dall'abilità nel comunicare con il pubblico, i partner e i clienti.

Cosa è emerso durante la puntata?

La vostra organizzazione si è dotata di un team di gestione delle crisi?

38%

dichiara di non avere un team di gestione delle crisi

43%

dichiara di avere un team di gestione delle crisi. Il 44% di questi non ha mai svolto esercitazioni

Il commento dell'esperto

Valentina Visconti
Senior Risk Consultant, Deputy Manager R&A Italy
Willis Towers Watson

"La presenza di un Crisis Management Team consapevole, 'allenato' e competente può realmente fare la differenza in caso di crisi.

Il primo passo necessario è quindi costituire le strutture organizzative preposte alla gestione ma, una volta compiuto questo passo, è altrettanto indispensabile dotarsi di un programma di esercitazioni che rendano in grado di rispondere in maniera ordinata e coordinata a qualunque evento di crisi dovesse colpire l'organizzazione."

Il commento dell'esperto

Valentina Visconti
Senior Risk Consultant, Deputy Manager R&A Italy
Willis Towers Watson

"Le risposte evidenziano che, pur in presenza di logiche di gestione della crisi, sia ancora difficile disporre di metriche oggettive grazie alle quali valutare un evento come crisi.

È fondamentale che le organizzazioni definiscano con grande chiarezza cosa sia crisi e cosa non lo sia, allo scopo di poter attivare le opportune strutture di gestione solo se e quando queste siano davvero necessarie."

Vi siete dotati di metriche oggettive per la valutazione degli eventi di crisi?

47%

dichiara di non esserne dotato, ma il 28% di questi sta provvendendo

26%

dichiara di esserne dotato, ma il 56% di questi lo è solo per alcune tipologie di eventi

Nota metodologica
I dati e le percentuali presenti in questo documento sono il risultato di survey in tempo reale poste nel corso dei webinar de "L'Accademia del Cyber" svolti nel mese di Giugno 2021.

04
Hybrid Cloud

Rivedi la puntata

La resilienza del dato

Nino D'Amico, CTO - HRC S.r.l.

Con hybrid cloud si intende l'utilizzo congiunto di piattaforme di private cloud e public cloud. Questa locuzione può indicare qualsiasi combinazione di soluzioni cloud utilizzate insieme on-premise e off-site per fornire servizi di cloud computing a un'azienda. Un ambiente di hybrid cloud consente alle organizzazioni di sfruttare entrambi i tipi di piattaforma cloud e di scegliere il cloud da utilizzare in base alle esigenze specifiche dei dati. Le aziende si avvalgono dell'hybrid cloud per ottimizzare le risorse esistenti in modo rapido ed economico. Con questa soluzione, possono proteggere i dati sensibili in un private cloud e aggiungere velocemente più risorse di elaborazione, larghezza di banda della rete o storage in un public cloud di terze parti per far fronte a picchi provvisori della domanda.

Hybrid Cloud

Davide Custode, Channel Account Manager - Syneto

Chi detiene i dati ha il potere di innovare. I dati rappresentano la nostra memoria storica ed il nostro futuro. Investire nei dati ha diversi vantaggi. L'accesso globale a Internet ha cambiato la nostra società, le interazioni tra gli utenti e con l'ambiente, ma anche il modo di condurre gli affari. All'inizio di quest'anno, IDC ha previsto che entro il 2021 i dati saranno circa 44 trilioni di gigabyte (o 44 zettabyte). Considerando che la maggior parte di questi può essere utilizzata per alimentare e avviare aziende, si può affermare che sia più preziosa dell'oro. Ma esattamente, come vengono generati i dati e come possono essere utilizzati?

L'importanza della conoscenza e della preparazione

Valentina Visconti, Senior Risk Consultant, Deputy Manager R&A Italy - Willis Towers Watson

L'importanza della conoscenza e della preparazione: Un'azienda che decida di avvalersi dell'hybrid cloud, ha ragionevolmente intrapreso un percorso di conoscenza delle interconnessioni tra business e sistemi informativi, nonché di controllo dei propri rischi, che la porta ad un livello significativo di maturità sugli aspetti di resilienza. Quali sono i passaggi per poter intraprendere un percorso evolutivo di questa natura? Da cosa è necessario partire? Quali sono gli aspetti che non ci possiamo più permettere di trascurare? La disciplina del Business Continuity Management supporta le aziende in questo percorso strategico.

Cyber insurance: beneficiare del patrimonio conoscitivo e della capacità di reazione

Camilla Brena, Head of Cyber Risk, FINEX Italy - Willis Towers Watson

Beneficiare del patrimonio conoscitivo e delle capacità di reazione. In una situazione di "hard market" assicurativo, anche le organizzazioni più attente sono penalizzate nella stipula di coperture assicurative, andando a subire spesso incrementi di premio e limitazioni di copertura che gli assicuratori impongono sia in fase di prima sottoscrizione sia nei rinnovi anche per rischi non sinistrati. Cosa può fare la differenza? Sicuramente ciò che i britannici definiscono cyber maturity: la capacità di dimostrare di avere conoscenze approfondite dei rischi e chiare strategie di controllo e mitigazione, oltre che di gestione in caso di incidente o crisi. Saper sviluppare resilienza è fondamentale in questo ambito per difendersi ma anche per ottenere le migliori condizioni dagli assicuratori.

Cosa è emerso durante la puntata?

Quale tipologia di evento ha causato il peggior disagio nel corso del 2020 alla vostra organizzazione?

86%

ha indicato la pandemia COVID-19

17%

dichiara che a guidare la risposta alla pandemia è stato il dipartimento di Business Continuity, mentre per il 46% è stato il Board

Il commento dell'esperto

Valentina Visconti
Senior Risk Consultant, Deputy Manager R&A Italy
Willis Towers Watson

"È interessante notare che, anche nell'anno orribile della pandemia, ci sono organizzazioni che hanno dovuto fronteggiare anche altri eventi di crisi, il che ha sicuramente richiesto l'intervento di funzioni aziendali diverse, soprattutto in assenza di organi di governo ad-hoc predefiniti per la gestione di eventi così significativi."

Il commento dell'esperto

Camilla Brena
Head of Cyber Risk, FINEX Italy
Willis Towers Watson

"La cultura della conoscenza in ambito cyber si sta espandendo rapidamente: lo dimostra la percentuale delle organizzazioni che ha già svolto un'analisi specifica degli scenari cyber e che ha una chiara idea delle massime esposizioni relative agli scenari identificati.

La quantificazione del rischio cyber è un'attività fondamentale per prendere delle decisioni informate."

La vostra organizzazione ha identificato gli scenari di danno in ambito cyber?

26%

dichiara di aver intrapreso uno studio apposito in ambito cyber

Avete un'idea di quale sia la massima esposizione cyber in termini economici?

35%

dichiara di aver fatto delle stime generiche o delle quantificazioni specifiche e il 34% dichiara di non averne idea.

Nota metodologica
I dati e le percentuali presenti in questo documento sono il risultato di survey in tempo reale poste nel corso dei webinar de "L'Accademia del Cyber" svolti nel mese di Giugno 2021.

I relatori

Camilla Brena
Head of Cyber Risk, FINEX Italy
Willis Towers Watson

In Willis Towers Watson dal 2000, dal 2014 si occupa di rischi cyber per i clienti italiani. In particolare, si occupa delle seguenti attività: analisi di assicurabilità e gap analysis relativamente a scenari cyber, quantificazione degli impatti tramite tool proprietari di gruppo, analisi di wording; piazzamento di polizze cyber tradizionali e di polizze su misura per rischi speciali, indagini di mercato e due diligence assicurative.

Nino D'Amico
CTO
HRC S.r.l.

È in HRC dalla fondazione e ha contribuito alla sua evoluzione nella realtà aziendale articolata che è oggi.
Filosofo-informatico, grazie agli studi umanistici e scientifici, riesce ad avere una visione più ampia dell'informatica che gli consente di trovare soluzioni semplici a problemi complessi. Negli anni ha maturato competenze ed esperienze su diversi ambiti tecnologici, qualificandosi come uno dei pionieri in Italia per gli ambienti di progettazione virtualizzati. È tra gli ideatori dell'ecosistema CyberBrain di cui è responsabile tecnologico, nonché CTO di HRC.

Walter Narisoni
Sales Engineer Manager
SOPHOS

Walter Narisoni assume nel gennaio 2008 l'incarico di Sales Engineer Manager di Sophos Italia, ruolo che lo vede ancora più impegnato a diffondere la cultura della sicurezza informatica e le soluzioni di sicurezza Sophos.
Laureato in Ingegneria Informatica all'Università degli studi di Pavia, prima di entrare in Sophos Narisoni ha ricoperto i ruoli di Software e Network Specialist in Minolta fino al 2002, di IT Support per l'Italia in GE Medical System S.p.A. e di Pilota informatico per Carrefour S.p.A.

Alessandro Scarafile
VP Cyber Security & Operations
Syneto

Appassionato di informatica e tecnologia ho modellato il mio percorso e la mia carriera partendo dalla programmazione a riga di comando negli anni '80, attraverso lo sviluppo web e la modellazione di database negli anni '90, passando alle reti e alla relativa all'analisi del traffico negli anni 2000, fino alle moderne tecniche di Ethical Hacking, Offensive Security e Social Engineering dal 2010, ricoprendo il mio ultimo ruolo dirigenziale come Operations Manager in Hacking Team, una delle aziende più discusse degli ultimi anni. Ora arrivata al termine. Ad oggi ho maturato oltre 20 anni di esperienza professionale in ambito ICT, gestendo operazioni in oltre 60 Paesi del mondo e operando nei settori IT, bancario, assicurativo, industriale, finanziario, business information, telecomunicazioni, energia, governativo, intelligence e forze dell'ordine.

Davide Custode
Channel Account Manager
Syneto

Davide, da sempre appassionato di tecnologia, negli anni ricoprirà vari ruoli, sempre incentrati su concetti di data protection, cercando di accrescere la proprie capacità verso l'erogazione di consulenze e progetti di iperconvergenza, Disaster Recovery e HybridCloud.
Ad oggi, con i suoi partner, guida la trasformazione digitale e la creazione di piani di DR con particolare attenzione alle necessità di Piccole e Medie Imprese del territorio italiano.

Marco Ivaldi
Technical Director
HN Security

Marco Ivaldi è un ricercatore e tech leader con esperienza più che ventennale nel settore della sicurezza informatica. È co-fondatore e direttore tecnico di HN Security, startup specializzata nella fornitura di servizi di offensive security. Collabora allo sviluppo dell'Open Source Security Testing Methodology Manual (OSSTMM), lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza. Marco è inoltre uno sviluppatore di exploit di fama internazionale. Negli anni '90, è stato tra i fondatori di Linux&C, la prima rivista italiana dedicata a Linux e all'open source.

Monica Ramazzina
Direttore Commerciale
Cosman

In oltre 25 anni di attività ha sempre operato in ambito commerciale sia gestendo le relazioni con i clienti anche a livello internazionale sia svolgendo attività di project management per commesse complesse. In aziende di varie dimensioni si è occupata di gestire i portafogli clienti, di accrescere contatti e relazioni con società partner e di sviluppare e proporre progetti integrati ad elevato contenuto tecnico. Dal 2016 Direttore Commerciale in Cosman svolge attività di gestione e ampliamento del portafoglio clienti e di supporto agli analisti dei diversi Centri di Competenza in cui è articolata l'attività Cosman. La capacità di essere vicina ai bisogni dei clienti l'ha resa particolarmente efficace nella proposizione dei servizi a valore di Cosman.

Valentina Visconti
Senior Risk Consultant, Deputy Manager R&A Italy
Willis Towers Watson

Laureata in ingegneria per l'Ambiente ed il Territorio (V.O.), comincia con la consulenza manageriale e in società di ingegneria ambientale. In 22 anni di esperienza costruisce una significativa competenza in diversi aspetti del Risk Management, Business Continuity e Crisis Management; sia con un approccio "verticale" (cioè su specifiche aree di rischio) che con un approccio "trasversale" (cioè nella comprensione e gestione dell'intero universo dei rischi). Dal 2008 è docente nel Master "Risk Engineering" di CINEAS, il consorzio per l'ingegneria nelle assicurazioni del Politecnico di Milano; dal 2017 è docente certificato per DRI (Disaster Recovery Institute) per corsi professionali in ambito Business Continuity.

I servizi di Willis Towers Watson

Cyber Risk Management

Una risposta a 360° per la gestione dei rischi cyber

Gestione della crisi

- Costi di esperti informatici e forensi
- Spese legali
- Costi di notifica
- Ripristino dei dati
- Costi di decontaminazione
- Costi di monitoraggio del credito e dell'identità
- Costi del servizio di call center
- Costi di pubbliche relazioni

Responsabilità per danni e terzi

La copertura si attiva quando l'assicuratoè responsabile:

- Di fronte all'Autorità:
  - Costi di investigazione
  - Costi per resistere all'azione dell'Autorità
- Nei confronti dei terzi danneggiati per:
  - Data breach
  - Violazione della sicurezza informative
  - Involontaria pubblicazione di contenuti lesivi (es. diffamazione)
  - Uno degli eventi sopra menzionati anche se avvenuto presso provider

Danni propri

- Costi operativi straordinari
- Spese extra
- Perdita di profitto
- Estorsione cyber

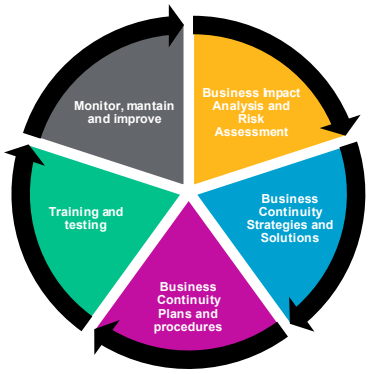
I costi di gestione della crisi sono comunque parte del danno finanziario dell'assicurato stesso.

Business Continuity Management

Definizione ed elementi essenziali

«Il Business Continuity Management è capacità dell'organizzazione di continuare a fornire prodotti ed erogare servizi a livelli accettabili ed entro un tempo predefinito, a seguito di un evento destabilizzante»

ISO 22301:2019
Sicurezza e resilienza
Sistemi di gestione per la continuità operativa



I benefici del Business Continuity Management System

- Diminuire i costi di una business interruption
- Soddisfare i requisiti di conformità normativa
- Assicurarsi un vantaggio competitivo
- Creare un sistema di Risk Management integrato
- Ripristinare le attività il più rapidamente possibile

I servizi di Cyber Security

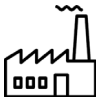
Cybersecurity intelligence

AWARENESS
La consapevolezza è la prima arma per contrastare gli attacchi.
Piattaforma di **training online** per lo sviluppo di comportamenti responsabili da parte dei dipendenti. Attività di **team building per il management** aziendale volta ad aumentare le competenze sul tema cybersecurity.

SECURITY AUDIT ASSESMENT
Misura il livello attuale di sicurezza della tua azienda.
I servizi di **Vulnerability**, **Penetration** e **Hardering** ne testano l'efficacia.
Dark Web Monitoring: l'analisi del dominio aziendale genera un report che riporta tutte le eventuali credenziali di posta elettronica aziendale compromesse.

THREAT MONITORING & INCIDENT ANALYSIS (SOC)
Identifica le minacce tecniche nell'ambito dell'IT security e **monitora i logs** degli apparati per **analizzare le attività sospette**.

THREAT INTELLIGENCE (SIEM)
Monitora lo stato di salute e **gli eventi di sicurezza** relativi alla presenza di malware, worm e **tentativi di accesso non autorizzati** verso le infrastrutture.



INDUSTRIAL CYBERSECURITY
Tecnologie e servizi progettati per proteggere i sistemi industriali e gli elementi dell'organizzazione, compresi **server SCADA, HMI, Engineering Workstation, PLC, connessioni di rete...**

Back up dei dati

CyberBrain

DISASTER RECOVERY
Consulenza per la preparazione dei piano di DR, planning e test periodici di Disaster Recovery.

Disponibilità di un **tenant dedicato** e segregato per il **salvataggio dei dati** in cloud.

Resilienza del dato – **immunità da attacchi ransomware**.

Datacenter Tier 3 in Italia con garanzia del rispetto **GDPR** e **legislazione nazionale**.

Ripristino e Recupero dei dati **in pochi minuti** indipendentemente dalla dimensione.

Digital Cost Management

All'interno de "L'Accademia del Cyber", **Cosman** porta il suo prezioso contributo illustrando come liberare risorse da aree a basso valore aggiunto grazie al **Digital Cost Management**, una nuova modalità per gestire, semplificare ed ottimizzare in continuo i costi aziendali.

Cosman analizza le diverse nature di costo (costi di struttura, costi tecnici, costi logistici e del personale) con le più innovative tecnologie digitali.

Attraverso la sua **piattaforma Shaper®** e la sua attività data driven Cosman si inserisce nell'ecosistema CyberBrain ponendo **al centro i dati e la loro sicurezza** con l'obiettivo di migliorare l'**efficienza economica**, **semplificare i processi** e apportare **risorse da destinare a progetti strategici** quali la Cybersecurity.

Propone un **approccio digitalizzato** che semplifica e migliora la gestione dei costi.

Attraverso la piattaforma Shaper®:

- **costruisce e alimenta** in modo continuativo la **base dati dei costi**
- **elabora scenari di ottimizzazione**
- **accompagna l'implementazione**
- **monitora** costantemente **l'andamento dei costi**, orientando il comportamento organizzativo verso il miglioramento continuo

Quali sono i vantaggi?

RISULTATI PERMANENTI: il processo di miglioramento dei costi è strutturato per diventare patrimonio dell'azienda.

AFFIANCAMENTO SENZA INVASIVITÀ: l'esperienza maturata e l'uso della tecnologia consente di ridurre al minimo l'invasività semplificando la gestione.

VERIFICA DEL CORRETTO POSIZIONAMENTO: sia rispetto ai benchmark, sia rispetto alla correttezza degli adempimenti normativi.

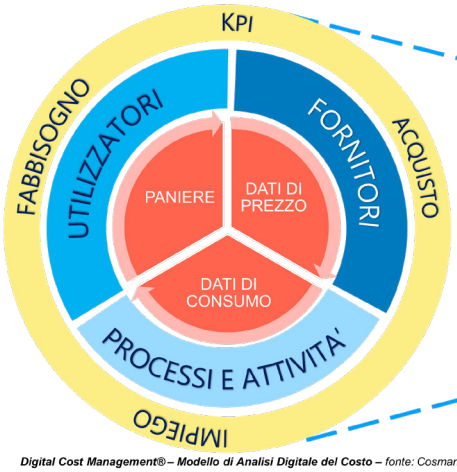
INNOVAZIONE: realizzare il Digital Cost Management, nuovo modo per presidiare i costi.

REMUNERAZIONE VARIABILE sui risultati effettivamente conseguiti.

TEMPESTIVITÀ DI REALIZZAZIONE: i primi miglioramenti sono visibili dopo i primi 30 giorni.

Il modello 3D nel Digital Cost Management

» Il Modello di Analisi Digitale del Costo*



Digital Cost Management® – Modello di Analisi Digitale del Costo – fonte: Cosman Srl

Il Processo di Ottimizzazione del Costo

Digital Cost Management® – Ottimizzazione della gestione costi – fonte: Cosman Srl

L'Accademia del Cyber

Willis Towers Watson

Mauro Mottura
Sales Manager

+39 348 3800586
Mauro.Mottura@willistowerswatson.com

COSMAN
cost management

Monica Ramazzina
Direttore Commerciale

+39 366 3245142
Monica.Ramazzina@cosmanitalia.it

HRC
IT SOLUTIONS AND CONSULTING

Rocco D'Agostino
Chief Executive Officer

+39 348 8976840
rda@hrcsrl.it

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson