POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

GDPR e Security: un percorso impervio… a trazione integrale

Febbraio 2018

Indice

Introduzione

L'avvento del nuovo Regolamento europeo sulla Protezione dei Dati Personali (GDPR) ha letteralmente sconvolto il mercato digitale nel corso dell'ultimo anno. L'attenzione alle modalità con cui raccogliere ed utilizzare i dati dei clienti e la scelta delle tecnologie da mettere in campo per garantirne la sicurezza sono sempre più un punto cruciale nel percorso di introduzione di nuovi progetti di innovazione digitale. Accanto a ciò, la crescente minaccia derivante da attacchi sempre più sofisticati ha smosso l'interesse del mercato delle soluzioni tecnologiche legate alla sicurezza dei dati, che riscuotono sempre maggior successo.

In questo scenario si muove l'Osservatorio Information Security & Privacy – promosso dalla School of Management del Politecnico di Milano – in collaborazione con CEFRIEL e DEIB e con il patrocinio di CLUSIT, Associazione Italiana per la Sicurezza Informatica.

L'Osservatorio, al suo terzo anno di Ricerca, intende rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'information security & privacy e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user, creando una community permanente di confronto.

La Ricerca 2017 dell'Osservatorio ha previsto una Survey di rilevazione che ha coinvolto 1107 CISO, CSO e CIO di imprese italiane. In particolare sono state coinvolte 160 organizzazioni grandi (>249 addetti) e 947 PMI (tra 2 e 249 addetti).

Sono inoltre stati coinvolti nella Ricerca Risk Manager e Chief Risk Officer, con un'indagine ad hoc che ha visto la partecipazione di 106 organizzazioni italiane.

In ultimo, alla luce dell'imminente applicabilità del GDPR, è stata effettuata un'ulteriore rilevazione, volta ad indagare l'interesse per la Data Protection, che ha visto il coinvolgimento di 313 professionisti del settore appartenenti a organizzazioni operanti in Italia.

Nel corso del 2017 sono stati organizzati tre Workshop a porte chiuse che hanno visto la partecipazione di circa 150 decisori aziendali delle principali aziende operanti in Italia e dei player dell'offerta. È stato inoltre istituito un Gruppo di Lavoro finalizzato a produrre una metodologia e una linea guida operativa di attuazione del Data Protection Impact Assessment nel contesto del nuovo General Data Protection Regulation (GDPR).

È infine stato realizzato il fascicolo di approfondimento "Information Security & Privacy", pubblicato e distribuito dal Gruppo Sole 24 ORE in abbinamento al quotidiano. Lo speciale ha toccato i seguenti argomenti: lo stato di maturità delle organizzazioni italiane sul tema della sicurezza informatica, le implicazioni dell'innovazione digitale sulla security e il quadro normativo di riferimento, con particolare attenzione rivolta alla nuova regolamentazione europea in materia di protezione dei dati (GDPR – General Data Protection Regulation). I capitoli redatti sono stati corredati da numerosi studi di caso relativi ad aziende utente che hanno voluto condividere le progettualità messe in campo.

Gli obiettivi della Ricerca 2017 sono stati i seguenti:

- Quantificare il mercato della sicurezza informatica in Italia;
- Comprendere l'impatto del Regolamento UE sulla protezione dei dati e sulle nuove professionalità;
- Indagare come i trend dell'innovazione digitale impattano sulla gestione dell'information security e della privacy;

- Identificare le competenze e i ruoli coinvolti nella gestione dell'information security e le modalità di gestione del fattore umano;
- Analizzare le modalità di gestione del rischio Cyber;
- Monitorare lo stato di adozione di sistemi di information security e privacy nelle organizzazioni italiane;
- Studiare gli impatti sulle grandi imprese e sulle PMI;
- Identificare i casi di successo.

Comitato Scientifico

Umberto Bertelè
Chairman degli Osservatori Digital Innovation

Alessandro Perego
Direttore Scientifico Osservatori Digital Innovation

Raffaello Balocco
Comitato Scientifico Osservatori Digital Innovation

Mariano Corso
Comitato Scientifico Osservatori Digital Innovation

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

GDPR e Security: un percorso impervio… a trazione integrale

La Ricerca

Febbraio 2018

Executive Summary

Una nuova opportunità in un contesto di crescente incertezza

Per anni la gestione della sicurezza informatica e della privacy è rimasta secondaria nell'agenda della trasformazione digitale delle organizzazioni italiane. La recente indagine sulle priorità di investimento per il 2018 svolta dalla Digital Transformation Academy[1], mostra però un segnale in controtendenza: i sistemi di gestione dell'information security, della privacy e del risk management si collocano infatti al quarto posto in un lungo elenco di aree di investimento, segnalati come prioritari dal 28% dei rispondenti, in netta crescita rispetto al passato.

Il trend di incremento degli attacchi informatici in compenso non conosce crisi: anche il 2017 ha confermato e rafforzato la tendenza all'aumento incessante e progressivo del cybercrime.

Secondo il Rapporto CLUSIT 2017, gli attacchi informatici gravi a livello globale nel primo semestre 2017 sono cresciuti dell'8,35% rispetto al secondo semestre 2016, che era finora considerato come l'annus horribilis della cybersecurity. Sempre secondo i dati CLUSIT, oltre il 50% delle organizzazioni nel mondo ha subìto almeno un attacco grave nell'ultimo anno e qualsiasi azienda, indipendentemente dalla dimensione o dal settore in cui opera, è a rischio concreto di subire un attacco informatico di entità significativa entro i prossimi 12 mesi[2].

Tra i più significativi incidenti che si sono susseguiti durante l'ultimo anno va sicuramente menzionato il caso WannaCry, avvenuto a maggio. L'attacco, di portata mondiale, ha colpito i sistemi di organizzazioni, aziende e istituzioni pubbliche in oltre 150 Paesi, dalle strutture sanitarie pubbliche inglesi ai computer di FedEx, fino ai server della telco spagnola

[1] Secondo quanto emerge dalla Survey Innovation 2017 dell'Osservatorio Digital Transformation Academy, condotta a Novembre 2017. La rilevazione ha visto il coinvolgimento di 264 Innovation Manager e CIO di grandi organizzazioni italiane.

[2] Secondo quanto emerge nel "Rapporto Clusit sulla sicurezza ICT" del CLUSIT, aggiornamento ottobre 2017.

Telefonica, infettandoli tramite un ransomware, che ha reso inaccessibili i dati richiedendo il pagamento di un riscatto da effettuare in Bitcoin.

Poche settimane dopo l'epidemia WannaCry, una nuova minaccia analoga, denominata NotPetya, si è diffusa in numerosi Paesi, partendo dall'Ucraina. Come per WannaCry, NotPetya ha integrato l'exploit d'attacco EternalBlue, sviluppato dal National Security Agency (NSA) statunitense e sfuggito al controllo della stessa agenzia. Anche in questo caso l'attacco richiedeva alle vittime un riscatto di circa 300 dollari, criptando l'intero disco fisso fino al pagamento della somma richiesta.

Non di minore rilevanza l'attacco a Equifax: un enorme data breach che ha messo a rischio i dati personali di oltre 143 milioni di consumatori, prevalentemente americani, oltre che inglesi e canadesi. L'agenzia di controllo dei crediti americana ha scoperto a fine luglio un'intrusione nella propria banca dati, iniziata a maggio e durata fino alla metà di luglio. L'azienda ha però affermato, rassicurando i suoi clienti, che i malintenzionati non sarebbero riusciti ad avere accesso alle informazioni più sensibili. Si tratta in ogni caso di uno dei più imponenti attacchi hacker della storia.

Tra le più recenti notizie di fine anno, ha suscitato molto clamore l'annuncio di Uber, il cui CEO ha dichiarato che nel 2016, sotto la precedente gestione, l'azienda avrebbe subito un grave attacco informatico in cui furono violati i dati di 57 milioni di utenti, tra clienti e autisti. Tra le informazioni rubate figurano nomi, indirizzi email, numeri di telefono, conti bancari e dettagli delle patenti.

Infine, sono state recentemente scoperte due importanti vulnerabilità, denominate

Meltdown e Spectre, che sfruttano alcuni difetti di progettazione dei principali processori commercializzati nell'ultimo decennio, esponendo ad eventuali attacchi buona parte dei dati che passano dalle CPU per essere elaborati. Il fattore che rende straordinaria la rilevanza di questa scoperta è la portata di questa vulnerabilità, che interessa più del 90% dei dispositivi informatici di tutto il mondo.

Nonostante lo scenario delineato, per le organizzazioni si profila oggi un'opportunità importante, derivante dalla necessità di adeguamento al nuovo Regolamento europeo sulla data protection (General Data Protection Regulation o, in breve, GDPR): un'occasione per smuovere investimenti, per disegnare nuovi ruoli organizzativi, per mettere in campo strumenti e metodologie in grado di supportare in sicurezza la trasformazione digitale, che riguarda tutti noi, nella doppia veste di consumatori ed utenti professionali.

La nuova *regolamentazione UE in materia di trattamento dei dati personali*, che diventerà pienamente applicabile a partire dal 25 maggio 2018, pone l'accento infatti su una maggiore strutturazione dei processi di gestione dei dati, sulla creazione di nuovi ruoli organizzativi e sulla messa in atto di pratiche e strumenti più complessi rispetto al passato.

Nella trattazione dell'Osservatorio quest'anno abbiamo tracciato un'analisi approfondita dei percorsi intrapresi dalle organizzazioni, con il fine di comprendere se è in corso un cambio di marcia, un'accelerazione rispetto al passato, con nuovi strumenti in grado di gestire in modo maturo la security e la privacy aziendale.

Per perseguire questo obiettivo è stata analizzata la maturità delle imprese in molteplici direzioni. La prima prospettiva riguarda l'analisi del mercato, utile per comprende-

re le dinamiche di spesa e le aree di interesse potenziale maggiore. La seconda concerne l'approfondimento sul percorso di adeguamento al GDPR, a cui spetta il ruolo di motore delle iniziative dell'anno. La terza l'analisi delle nuove competenze per la gestione dell'information security e privacy, tramite una Ricerca ad hoc sulla percezione della data protection in azienda. Si prosegue con l'analisi del fattore umano e delle azioni messe in atto dalle imprese per sensibilizzare gli utenti. L'analisi si conclude con due ulteriori prospettive: la prima legata alla sensibilità delle organizzazioni alla gestione del rischio cyber, alla sua mitigazione e al suo trasferimento, con una Ricerca ad hoc dove sono stati coinvolti i Risk Manager di grandi imprese italiane; la seconda relativa all'approccio delle PMI alla gestione dell'information security e privacy, con una rilevazione condotta su poco meno di mille realtà del territorio.

L'evoluzione del mercato dell'information security in Italia e la sua scomposizione

L'Osservatorio, al suo terzo anno di attività, ha coinvolto nella rilevazione un campione di 1.107 organizzazioni italiane, ripartite tra 160 grandi imprese (oltre i 250 addetti) e 947 PMI (aventi un numero di addetti compreso tra 2 e 249).

Se già nel 2016 era stata registrata una crescita della spesa in information security e un progressivo aumento di consapevolezza, l'ultimo anno, complice anche il panorama degli attacchi delineato, ha rappresentato per il mercato italiano un importante punto di svolta, con una spinta decisa nella tutela del patrimonio informativo delle organizzazioni.

Il mercato dell'information security in Italia ha infatti raggiunto nel 2017 un valore di 1,09

miliardi di Euro, in crescita rispetto ai 12 mesi precedenti.

La spesa è concentrata nelle grandi imprese, per il 78% circa della cifra complessiva.

Secondo i dati emersi dalla Ricerca sulle grandi imprese, solo il 4% degli intervistati dichiara di aver subito una diminuzione del budget dedicato all'information security e privacy nel corso dell'ultimo anno, a fronte del 75% dei rispondenti che afferma invece di aver aumentato gli investimenti in materia di sicurezza, con incrementi di varie entità. Complessivamente, il mercato ha registrato una crescita di circa 12 punti percentuali, con un ruolo importante giocato dai progetti di adeguamento al General Data Protection Regulation, che contribuiscono per più della metà alla dinamica di crescita registrata.

Entrando maggiormente in dettaglio, è possibile scomporre il mercato in alcune voci di spesa e identificare gli atti di moto delle singole quote che lo compongono. Escludendo il già citato tema del GDPR, sono le componenti di sicurezza più tradizionali a catalizzare ancora le quote maggiori: il 19% del totale è attribuibile a sistemi dedicati a *Business Continuity e Disaster Recovery*, il 14% è ascrivibile alla componente di *Network Security* e il 9% alla voce di *Security testing* (Penetration Test, Vulnerability Assessment).

Seguono le quote dedicate alle piattaforme di *Incident response* (quali ad esempio SIEM e SOC – pari a 8%), ai sistemi di *Identity and Access Management* (6%) e alle soluzioni per *Data Leakage e Data Loss Prevention* (4%).

Un differente scenario appare osservando le dinamiche di spesa in ottica prospettica: le componenti che registrano infatti le maggiori percentuali di incremento sono legate a Mobile e Cloud Computing, trend dell'innovazione digitale che sono ormai diffusi nelle aziende e richiedono opportuni investimenti di sicurezza.

Il 63% delle aziende intervistate dichiara infatti un aumento della spesa dedicata alla *protezione per i device mobili*, ormai diventati naturali strumenti di lavoro e canale di accesso alle informazioni personali e aziendali, a cui è riconducibile nel 2017 una quota pari a poco meno del 4% del mercato complessivo dell'information security. Alla stessa stregua il 59% dei rispondenti definisce in crescita gli investimenti relativi alla *protezione degli ambienti Cloud Computing*, attualmente pari a circa il 3% del totale.

Altre voci di spesa in forte aumento si focalizzano su *Security Awareness e Training* (che cresce per il 56% dei rispondenti), sintomo della necessità di gestire in maniera più efficace la vulnerabilità legata al fattore umano, e sulla *Cyber Insurance*, argomento che appare ancora marginale (la quota di mercato nell'anno in oggetto si attesta a circa il 2,5%) ma di forte interesse in ottica prospettica, dichiarato in crescita dal 52% degli intervistati.

La metà delle grandi imprese intervistate (50%) afferma di dedicare al tema dell'information security e privacy un piano di investimenti con orizzonte pluriennale, che nel 23% dei casi è anche inserito nel piano industriale, mentre il 29% pianifica gli investimenti su base annua. Sebbene anche questo dato registri un miglioramento rispetto alle rilevazioni del 2016, in cui la percentuale di organizzazioni che dichiarava di pianificare la spesa su base pluriennale si attestava sul 39%, è doveroso evidenziare che esiste ancora un 21% di imprese che dichiara di stanziare un budget dedicato alla sicurezza e alla protezione dei dati solo in caso di necessità.

Il percorso verso il GDPR

Il percorso legislativo che ha portato all'emanazione del General Data Protection Regulation (n. 2016/679, c.d. GDPR) è iniziato il 4 novembre 2010, quando la Commissione europea ha elaborato una proposta di riforma della normativa in materia di protezione dei dati personali. Il GDPR persegue due obiettivi fondamentali: da un lato, adeguare la normativa, ormai risalente al 1995, alle nuove tecnologie, dall'altro armonizzare ed uniformare la normativa stessa a livello europeo, creando un quadro normativo comune. Il Regolamento Generale è entrato in vigore il 24 maggio 2016 e diventerà applicabile a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in modo da permettere ai soggetti destinatari di implementare quanto necessario per mettersi in regola.

La Ricerca, per il secondo anno consecutivo, si è soffermata ad indagare il percorso di adeguamento delle imprese ai requisiti imposti dal GDPR. La rilevazione ha esplorato tre aspetti in particolare: l'awareness, il budget dedicato e le azioni implementate.

L'indagine ha evidenziato un sensibile incremento dell'awareness delle aziende rispetto all'anno precedente. Sono infatti diminuite le aziende che dichiarano una scarsa conoscenza delle implicazioni del GDPR, passando dal 23% del campione dell'anno scorso all'8% di quest'anno. Coerentemente è emerso come nell'85% dei casi l'intera tematica sia ormai posta all'attenzione del vertice e non solo delle funzioni specialistiche (Security, Legal, Compliance, ecc.). A sostegno di tali dati va rilevato come nel 2016 solamente il 9% del campione dichiarava che fosse già in corso un vero e proprio progetto strutturato di adeguamento alla normativa; nel 2017 tale percentuale si attesta invece sul 51%, mentre il 34% afferma che è in corso un'analisi di dettaglio dei requisiti richiesti e dei piani di attuazione possibili.

Parallelamente si registra un notevole incremento del budget dedicato a misure di adeguamento e risposta al GDPR. Mentre nel 2016 solamente nel 15% dei casi esisteva un budget dedicato (nel 7% pluriennale e nell'8% annuale), nell'ultimo anno la percentuale ha raggiunto il 58%: il 35% del campione dichiara l'esistenza di un budget con orizzonte annuale, il 23% con orizzonte pluriennale. Come già anticipato precedentemente, il GDPR rappresenta infatti una delle voci di spesa che incidono maggiormente sul valore complessivo del mercato dell'information security per il 2017.

È tuttavia ancora alta la percentuale di aziende che afferma che attualmente non esiste un budget: nel 23% dei casi sarà stanziato nel corso dei prossimi 6 mesi e nel restante 19% non è previsto del tutto.

Entrando nello specifico nelle fasi che compongono il processo di adeguamento al GDPR intrapreso dalle organizzazioni, le principali azioni in corso o che sono già state implementate riguardano la valutazione della compliance (87%), l'individuazione dei ruoli e delle responsabilità (80%), la stesura o la modifica della documentazione (77%), la definizione delle politiche di sicurezza e valutazione dei rischi (77%), la creazione e l'aggiornamento del registro dei trattamenti (74%), la valutazione di impatto sulla protezione dei dati personali (57%), la procedura di data breach (53%), il servizio di Data Protection Officer (50%) e l'implementazione dei processi per l'esercizio dei diritti dell'interessato (49%).

Le imprese più dimensionate, o comunque appartenenti ai settori di mercato dove il trattamento del dato personale appare essere core-business (GDO, settore bancario e finanziario, settore assicurativo, fashion & luxury per fare alcuni esempi), hanno avviato ormai da mesi importanti e complessi progetti di adeguamento al GDPR seppur, in larga parte, in grande ritardo rispetto ai due anni che il legislatore europeo aveva lasciato come tempistica di adeguamento.

Nel corso degli ultimi mesi, peraltro, è apparso chiaro come non ci sarebbe stato alcun rinvio nella data di completa applicazione del GDPR anche alla luce della gran quantità di linee guida emesse dall'Article 29 Data Protection Working Party che hanno aiutato l'interpretazione e quindi l'applicazione della normativa.

Inoltre, sono in corso di emanazione in tutti i Paesi europei le norme di raccordo fra le normative vigenti e il GDPR, elemento di grande rilevanza perché discenderà dalle scelte dei singoli legislatori la maggiore o minore uguaglianza legislativa fra i vari Paesi. In particolare in nazioni come l'Italia, dove la legislazione vigente e i vari provvedimenti del Garante hanno creato un apparato normativo parallelo al decreto legislativo 196/2003, la scelta di mantenere o meno tali normazioni o provvedimenti può determinare, nuovamente, una sostanziale diversità di costo e di complessità di adeguamento e mantenimento della conformità rispetto agli altri Paesi.

La Ricerca rende comunque evidente che è in corso un sostanziale cambio di marcia.

Il fatto stesso che quasi tutte le aziende che hanno partecipato alla rilevazione dichiarino di aver intrapreso processi di valutazione della compliance normativa e di aver iniziato a individuare ruoli e responsabilità interne alle organizzazioni significa che lo scopo normativo, perlomeno sulle aziende di più alto livello, è stato raggiunto. Il dato probabilmente più significativo è quello per il quale oltre tre quarti delle organizzazioni ha dichiarato di aver steso o iniziato a stendere politiche di sicurezza e valutazione dei rischi: significa aver coinvolto le giuste competenze, aver avviato un processo di valutazione interna, di analisi dei rischi e quindi, in definitiva, di coscienza della problematica.

Nei prossimi mesi assisteremo al completamento dei progetti di adeguamento al GDPR: sa-

ranno finiti gli assessment, saranno stesi i registri dei trattamenti, saranno state adottate le procedure interne a garanzia dei diritti degli interessati e saranno state effettuate le analisi dei rischi. Perlomeno dalle società più attente al tema.

In seguito è presumibile che l'attenzione al tema cominci a permeare anche le PMI per le quali i dati personali non rappresentano il core-business. È probabile inoltre che si assista a una progressiva esternalizzazione dei servizi verso soggetti che, potendo contare su economie di scala, possano proteggere meglio le infrastrutture e le applicazioni e, in ultimo, i dati dei clienti.

Infine, ci si può attendere un'ulteriore crescita degli investimenti in sicurezza informatica e uno spostamento delle attività consulenziali dai progetti di adeguamento al GDPR alle attività sottese al mantenimento della compliance: analisi dei rischi su nuovi trattamenti, Data Protection Impact Assessment e impostazione legale e tecnologica sotto il profilo della privacy by design.

La figura del Chief Information Security Officer (CISO)

Il ruolo del Chief Information Security Officer (CISO) sta evolvendo verso un profilo completo, che affianca alle competenze tecnologiche e organizzative soft skill relazionali, conoscenze del dominio di business e capacità di sviluppare e governare un team complesso. Oggi aumentare la consapevolezza delle problematiche di cybersecurity richiede sempre più la capacità di comprendere il business, interfacciandosi con i responsabili di prodotto, e di comunicare al Top Management i rischi derivanti dalle nuove minacce con una visione sistemica. Le conoscenze di industry diventano distintive, a fronte di obblighi di compliance, le-

gislazioni e minacce sempre più focalizzate su settori di mercato ben identificati. Dotarsi di competenze tecnologiche eterogenee richiede una progressiva strutturazione di ruoli e strumenti di governo: diventa fondamentale sviluppare capacità di project management e di gestione e sviluppo del capitale umano.

Identificare il corretto mix delle competenze appena citate non è semplice e non è univocamente valido per tutte le situazioni. Il ruolo ricoperto dal CISO può essere maggiormente strategico, non limitandosi esclusivamente a compiti tecnici, e richiedere maggiore relazione con il management aziendale; in questi casi le competenze relazionali e di business diventano fondamentali. L'attività, per contro, può essere orientata alla mera gestione e monitoraggio del servizio, e quindi essere incentrata sulla gestione dei processi e delle tecnologie. Infine ci può essere un ruolo di stampo manageriale, con la responsabilità di controllo e supervisione di persone afferenti ad aree di sapere diverse, dalla gestione del rischio alla compliance e privacy.

La crescente attenzione al tema dell'information security è testimoniata, a livello organizzativo, dall'intenzione di potenziare i team dedicati alla sua gestione. Con riferimento al campione di grandi organizzazioni analizzate, ben il 39% delle imprese prevede un aumento dell'organico di figure dedicate, a fronte di un limitato 2% che prevede di diminuirlo (il resto del campione dichiara invece una situazione di stabilità). Con riferimento al tema privacy, la percentuale di organizzazioni che dichiarano un aumento dell'organico sale al 49%, a fronte di un 1% di riduzione.

Le responsabilità del CISO possono variare a seconda del settore di industria e della collocazione organizzativa della figura. Di seguito sono indicate le principali aree di responsabili-

tà, con la percentuale di CISO del campione di grandi organizzazioni che dichiara di esserne responsabile in prima persona:

- *Assessment della sicurezza (81%)*: la responsabilità principale del CISO riguarda la comprensione della situazione as-is dell'impresa, la conduzione della gap analysis tecnologica ed organizzativa e l'identificazione di un piano strategico ed una roadmap per aumentare la readiness dell'azienda alle minacce della sicurezza. Il piano strategico prende in considerazione processi, tecnologie e modelli organizzativi. Dall'identificazione di una strategia discende poi la creazione di un piano operativo, che sia in grado di traguardare obiettivi in modo coerente con il tempo ed il budget a disposizione.
- *Identificazione delle minacce (69%)*: conoscere le nuove minacce e le differenti tipologie di attacco è un elemento importante per un CISO. Vi sono svariati servizi che permettono di avere informazioni aggiornate. È possibile fare riferimento a CERT nazionali (Computer Emergency Response Team) che dispongono di database aggiornati sulle vulnerabilità rilevate.
- *Definizione delle policy (68%)*: l'identificazione delle regole e la relativa applicazione prevede il coinvolgimento di differenti funzioni aziendali. È necessario però che coloro che definiscono le policy siano soggetti differenti rispetto a chi si occupa della reale implementazione. Nel caso in cui la responsabilità della gestione della sicurezza sia in capo ad un componente della direzione IT non è sempre scontato che ci sia questa separazione netta di responsabilità; è quindi fondamentale definire in modo chiaro ruoli e relative attività. In modelli maturi il CISO ha la responsabilità di definire le policy nel rispetto delle regolamentazioni vigenti e riveste il ruolo di auditor nella definizione degli standard e delle possibili eccezioni. L'implementazione di tali policy risiede poi in altre mani, che hanno l'obiettivo di rendere operativo quanto indicato dal CISO.

- *Scouting dei prodotti di sicurezza (63%)*: il mercato delle soluzioni evolve in modo rapido, diventa fondamentale istruire un'analisi continua delle opportunità offerte da prodotti allo stato dell'arte. La conoscenza dell'ecosistema dell'offerta, della strategia dei grandi player, così come i servizi innovativi offerti dalle startup internazionali diventano un elemento fondamentale per la gestione della sicurezza informatica.
- *Analisi del rischio cyber (62%)*: la comprensione delle potenziali vulnerabilità e minacce per l'organizzazione serve al CISO per fornire al Top Management gli elementi per mettere in atto scelte di gestione del rischio cyber, in termini di politiche e strumenti coerenti all'interno dell'organizzazione. L'importanza di attuare una politica di gestione del rischio cyber allineata con la strategia di impresa diventa fondamentale. Il CISO deve essere in grado di comprendere come affrontare e mitigare il rischio ed eventualmente se e come trasferire parte di esso ad una terza parte tramite una polizza di cyber insurance.
- *Monitoraggio degli eventi di sicurezza (62%)*: il costante controllo del traffico sui diversi canali diventa fondamentale per identificare potenziali minacce. Per garantire l'efficacia dei controlli ed il monitoraggio continuo, il CISO deve sviluppare un Security Operation Center (SOC) interno all'azienda o in alternativa avvalersi di un provider esterno di servizi gestiti.
- *Risposta agli incidenti (61%)*: l'incidenza di un data breach è tanto più grave quanto più tempo trascorre dalla sua identificazione. La capacità di rispondere in tempi brevi in un momento di crisi diventa fondamentale per mitigare gli effetti dannosi. Il CISO ha il compito di definire i processi da mettere in atto qualora dovesse verificarsi un incidente e di individuare il team da coinvolgere. In seguito ad un evento di sicurezza il team si deve attivare rapidamente, in modo da valutare le possibili conseguenze e risolvere il problema nel tempo più breve possibile. Per essere efficace è necessario definire un piano di formazione continuo con incontri periodici di allineamento.

- *Definizione di iniziative di formazione e awareness (55%)*: il fattore umano è un elemento chiave da governare per ridurre l'entità dei danni causati da attacchi cyber. Si rende quindi necessaria la progettazione una strategia di lungo periodo, affiancata da un piano operativo in grado di aumentare la sensibilità delle persone all'utilizzo delle tecnologie digitali e alla comprensione delle loro implicazioni.
- *Definizione dell'architettura (44%)*: il disegno della corretta architettura di gestione della sicurezza ed il monitoraggio continuo delle scelte architetturali (ad esempio in seguito a cambiamenti dei diritti di accesso o dei firewall) sono fondamentali per prevenire possibili vulnerabilità nella rete aziendale. A tal proposito è auspicabile che nel team cybersecurity ci siano professionisti come architetti ed ingegneri della sicurezza.
- *Investigazione forense (26%)*: in caso di data breach è necessario avere la capacità di condurre successive indagini forensi. L'investigazione può essere perseguita con risorse interne o più spesso tramite competenze specialistiche esterne all'organizzazione. La definizione dei corretti processi e delle responsabilità diventano elementi distintivi, così come i meccanismi di coordinamento con le altre funzioni aziendali.

Le nuove professionalità in ambito information security e privacy

Il crescente interesse verso il tema della cybersecurity ha portato alla strutturazione di funzioni dedicate alla gestione delle tematiche di security management all'interno delle aziende di dimensioni più grandi. La complessità delle problematiche richiede competenze specialistiche, spesso molto difficili da reperire sul mercato.

Le professioni relative alla gestione della sicurezza informatica sono altamente qualificate e le certificazioni molto diffuse.

È possibile identificare differenti profili che ricoprono ruoli specialistici nell'ambito della sicurezza informatica. Si propone di seguito un elenco, non esaustivo, di tali profili e della percentuale di organizzazioni che dichiara di averle già al proprio interno o di essere in fase di valutazione di introduzione:

- *Security Administrator (76%)*: si occupa si rendere operative le soluzioni tecnologiche di security, dalla loro messa in produzione alle attività di manutenzione e supporto agli utenti finali.
- *Security Architect (57%)*: ha forti competenze modellistiche, si occupa di svolgere l'assessment delle soluzioni di security presenti in azienda e di curare il disegno armonico e coerente delle misure di sicurezza e delle policy adottate dall'organizzazione. Viene coinvolto nelle attività di disegno di nuovi prodotti e servizi di security.
- *Security Engineer (56%)*: ha un forte bagaglio tecnico e modellistico, si occupa di monitorare i sistemi e proporre soluzioni relative alla risposta agli incidenti. Può avere un ruolo attivo in attività di audit, così come nell'identificazione di soluzioni volte a migliorare la sicurezza dell'organizzazione.
- *Security Analyst (55%)*: ha competenze di analisi di processo e si occupa di valutare le vulnerabilità che possono interessare reti, apparati, applicazioni e servizi proponendo soluzioni ed accorgimenti pratici. Fa scouting di mercato, identificando le soluzioni più adatte a specifici ambiti di impiego. Si può occupare di attività di verifica e conformità di soluzioni e policy a specifiche normative. Può essere inoltre coinvolto nella realizzazione di nuovi prodotti/servizi di security.
- *Ethical Hacker (39%)*: Conosce le principali modalità di attuazione di penetration test e ha il compito di mettere in atto operazioni in grado di dimostrate l'effettiva pericolosità di alcune vulnerabilità di cui soffre l'azienda. Redige la documentazione per il Top Management e gli Executive security per argomentare con elementi concreti i fattori di debolezza nella strategia di security dell'organizzazione.

- *Security Developer (28%)*: con competenze informatiche specialistiche, si occupa dello sviluppo ad hoc di soluzioni di security così come dell'integrazione di servizi di terze parti.
- *Machine Learning Specialist (19%)*: ha un bagaglio nel campo dell'analisi statistica, della matematica e delle tecniche di analytics, si occupa di sviluppare e monitorare sistemi di risposta real time in grado di identificare e trattare possibili minacce in modo automatico e cognitivo.

Guardando all'ambito privacy e coerentemente al percorso di adeguamento al GDPR illustrato precedentemente, la Ricerca ha indagato infine la presenza del Data Protection Officer (DPO) all'interno delle aziende. L'introduzione di tale figura, in alcuni casi obbligatoria, è di fondamentale importanza in quanto è volta a facilitare il rispetto, da parte delle singole organizzazioni, delle disposizioni dettate dalla nuova normativa europea. Analizzando il campione, nel 15% delle aziende la figura del DPO risulta formalizzata, nell'10% è una presenza di tipo informale e nel 3% dei casi la responsabilità è delegata a una figura esterna all'azienda. Rispetto alla rilevazione compiuta l'anno precedente, negli ultimi 12 mesi è aumentata la percentuale di aziende che ha dichiarato di voler introdurre la figura del DPO nel prossimo futuro (57%, laddove nel 2016 era il 31%); conseguentemente è diminuita la percentuale di imprese che ha affermato di non prevederne l'introduzione (attualmente pari al 15%).

Per quanto riguarda le attività affidate al DPO all'interno dell'azienda, le principali sono: assicurare il rispetto dei requisiti previsti dal GDPR (93%), sorvegliare l'osservanza del Regolamento (76%), fornire pareri al Titolare o al Responsabile del trattamento (59%) e curare i rapporti con gli interessati e con l'Autorità di controllo (55%).

La percezione della data protection all'interno delle organizzazioni italiane

Come anticipato, l'avvento del nuovo Regolamento europeo sulla protezione dei dati personali rende necessaria l'introduzione di nuove competenze e strumenti per la gestione del patrimonio informativo aziendale. A tal proposito l'Osservatorio ha condotto un'ulteriore indagine, specifica sul tema, che ha visto il coinvolgimento di 313 professionisti del settore appartenenti ad organizzazioni operanti in Italia con lo scopo di comprendere lo stato attuale ed il potenziale impatto sulle organizzazioni in termini di strutture di governo, competenze e strumenti, e al fine di indagare l'interesse delle aziende verso nuove figure professionali in questo ambito.

La sensibilità nei confronti del tema della protezione dei dati è particolarmente alta all'interno delle organizzazioni. Il 74% dei professional intervistati dichiara infatti che il tema della data protection è diventato negli ultimi anni rilevante o addirittura fondamentale per l'azienda di appartenenza, mentre solo il 14% lo considera un argomento poco o per nulla importante. Per il 12% delle figure coinvolte il livello di rilevanza associato alla data protection all'interno dell'azienda è rimasto invariato rispetto al passato.

L'elevato interesse nei confronti della tematica in esame si scontra con il dato secondo cui il 39% delle organizzazioni di riferimento non ha in organico risorse che si occupano di data protection. Nel 40% delle organizzazioni sono invece presenti figure interne dedicate, mentre il 28% si rivolge a consulenti esterni. Nei restanti casi la funzione è ricoperta sia internamente che esternamente oppure è affidata a persone interne all'azienda non specificamente dedicate.

Un dato in linea con la rilevanza attribuita dalle organizzazioni a tutta la materia relativa alla protezione dei dati è quello per cui il 75% degli intervistati dichiara che la propria azienda sta adottando le soluzioni necessarie per gestire gli aspetti che in qualche modo sono ad essa legati. Le principali sfide e i cambiamenti organizzativi riguardano la sensibilizzazione del personale (67%), l'individuazione di un corretto modello di gestione della data protection (64%), l'applicazione della specifica regolamentazione (53%), l'integrazione o l'implementazione della documentazione relativa alla privacy (40%) e l'identificazione delle risorse dedicate (39%).

La rilevazione ha indagato parallelamente quali sono le principali azioni che le imprese dovrebbero compiere in vista di una corretta gestione della data protection. A tal fine gli interventi ritenuti maggiormente efficaci dai professional intervistati riguardano sia aspetti inerenti alla struttura di governo aziendale, quali l'individuazione e la formalizzazione di ruoli specifici e delle relative responsabilità (44%) e la creazione di un team dedicato (36%), sia aspetti relativi a progettualità e processi, come le attività di training (51%), la puntuale definizione e adozione di procedure e regole per la gestione dei trattamenti dei dati personali (51%), la realizzazione di audit periodici sul tema (43%) e la progettazione e definizione di un cruscotto di KPI per il monitoraggio della compliance alla normativa (37%). Quale che sia la tipologia di intervento, il trend per il prossimo futuro fa ben sperare in quanto il 68% delle aziende analizzate ha dichiarato di voler effettuare investimenti nell'ambito della data protection.

Dall'indagine è emerso infine come il 69% delle figure coinvolte ritenga utile istituire un corso di livello universitario in grado di fornire competenze trasversali finalizzate alla formazione di figure professionali sul tema della data protection. Con riferimento specifico alla

questione relativa alla volontà di acquisire nel prossimo futuro nuove risorse aventi competenze embrionali ed accademiche multidisciplinari legate a tale ambito, la metà del campione ha risposto positivamente.

In conclusione, la Ricerca ha evidenziato come le aziende, spinte dall'imminente applicazione del nuovo Regolamento europeo sulla protezione dei dati, considerino particolarmente rilevante la tematica della data protection e la ricerca di nuove figure professionali, al punto da ritenere opportuna l'erogazione di corsi di formazione ad hoc.

L'importanza del fattore umano e della sua gestione

Quando si parla di information security non si può tralasciare il cosiddetto *fattore X*, l'elemento di incertezza legato al comportamento umano.

Spesso le aziende investono su sistemi sofisticati in grado di proteggere l'organizzazione da attacchi esterni, ma non valutano il rischio legato al comportamento dei propri utenti, non considerando che l'anello debole della catena potrebbe essere proprio l'uomo. In molti attacchi informatici, infatti, i cybercriminali non utilizzano sistemi tecnologici particolarmente sofisticati, ma sfruttano aspetti del comportamento umano, come la distrazione o la mancanza di consapevolezza, per fare breccia nei sistemi aziendali.

Gli attacchi che sfruttano questa vulnerabilità sono spesso progettati secondo logiche di Social Engineering. Per Social Engineering si intende una tecnica basata sullo studio del comportamento individuale di una persona, con l'obiettivo di carpire informazioni utili per l'attaccante. Questo approccio fa leva su elementi psicologici ed emozionali, puntando a ge-

nerare empatia nella vittima dell'attacco. Il processo ha soprattutto lo scopo di sfruttare le debolezze insite nella natura umana per trarre in inganno la vittima ed ottenere informazioni e strumenti necessari a perpetrare azioni fraudolente. Un attacco di ingegneria sociale combina generalmente manipolazione e persuasione con elementi di tipo tecnologico.

La fase di attacco vera e propria è preceduta da una lunga sessione di studio della personalità, dei contatti sociali e dei modi di relazionarsi con gli altri. Un processo di Social Engineering parte infatti da un'accurata raccolta di informazioni sull'azienda target, reperite da tutte le fonti a disposizione (sito web aziendale, social network, dati societari, documenti disponibili in rete, ecc.) con l'obiettivo di conoscere a fondo l'azienda identificata come vittima e i dipendenti che vi operano. Una volta che il social engineer ha ottenuto le informazioni di cui aveva bisogno per architettare l'attacco, ecco che si passa alla fase operativa.

Gli strumenti di ingegneria sociale maggiormente utilizzati sono email, telefono, siti web, social network. I metodi per mettere a segno l'attacco posso essere molteplici: dal phishing[3] al pretexting[4], dal baiting[5] allo sfruttamento della "spazzatura informatica"[6].

In aggiunta alle numerose minacce informatiche provenienti dal mondo esterno, una perdita di dati può essere causata anche da un evento accidentale, come per esempio il comportamento inconsapevole di un utente, la perdita di un dispositivo o la cancellazione involontaria.

[3] **Phishing: tentativo di truffa, generalmente realizzato sfruttando la posta elettronica, che ha per scopo il furto di dati personali degli utenti ignari i quali, spinti dalla curiosità o tratti in inganno dal mittente della mail, "abboccano", cliccando sul link malevolo, inserendo le proprie credenziali oppure scaricando un allegato infetto.**

[4] **Pretexting: tecnica di social Engineering in cui l'attaccante contatta telefonicamente la vittima designata simulando un contesto particolare. Il mittente della telefonata finge di essere un soggetto in cui l'utente ha fiducia, per indurlo a comunicargli le informazioni riservate di cui ha bisogno.**

[5] **Baiting: metodologia di Social Engineering in cui l'hacker utilizza un'esca (es. chiavetta USB, hard disk, ecc.), contenente al suo interno del codice maligno. Lo scopo dell'attacco è quello di indurre la vittima, spinta dalla curiosità, ad inserire il dispositivo nel proprio computer, accedendo in questo modo all'intera rete aziendale.**

[6] **Trashing: tecnica tramite la quale i criminali setacciano la spazzatura alla ricerca di documenti contenenti dati sensibili. Obiettivo degli hacker possono essere anche i sistemi che vengono dismessi, come ad esempio smartphone, laptop o dispositivi USB guasti che, se non opportunamente resettati, possono essere fonte di preziose informazioni.**

I programmi di creazione di awareness

Per mitigare i rischi legati alla sicurezza informatica, le aziende non devono quindi soltanto dotarsi di sistemi tecnologici, ma anche introdurre iniziative volte a educare e rendere consapevoli i propri dipendenti rispetto alle possibili minacce. Benché non sia possibile annullare completamente il rischio informatico, un adeguato programma di sensibilizzazione degli utenti, congiuntamente a policy e soluzioni di sicurezza, può aiutare a minimizzarlo.

Generalmente i programmi di formazione messi in atto dalle aziende si pongono un triplice obiettivo:

1) Ridurre il rischio legato a possibili attacchi informatici, facendo sì che i dipendenti siano maggiormente consapevoli delle possibili minacce e delle tecniche per evitarle;
2) Aumentare l'empowerment delle risorse, rendendo ogni singolo utente responsabile della protezione delle informazioni aziendali;
3) Rinforzare policy e procedure comportamentali definite dall'organizzazione (policy sull'uso dei computer o di Internet, policy sugli accessi, ecc.), informando ed educando i dipendenti al rispetto delle stesse.

Secondo quanto emerge dalla Ricerca 2017 sulle grandi imprese condotta dall'Osservatorio, le azioni maggiormente diffuse all'interno delle aziende per la creazione di awareness sono l'invio di comunicazioni periodiche ai dipendenti aziendali in forma di mail e newsletter (presenti nell'80% delle organizzazioni intervistate) e le iniziative di formazione, sia in aula (69%) sia online (67%).

Lo scopo è quello di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire al massimo i rischi legati alla sicurezza e sapere come reagire e comportarsi di fronte ad eventuali criticità, con il risultato ad alto livello di provocare un cambiamento radicale nella cultura e nell'approccio dei dipendenti dell'azienda rispetto ai temi della sicurezza e della privacy.

Un'ulteriore tipologia di iniziativa per lo sviluppo della consapevolezza degli utenti, ancora poco diffusa nelle aziende italiane, è il training informale, che si basa su un approccio meno strutturato e più "amichevole". Le attività di questa categoria possono riguardare la distribuzione di materiale informativo come poster o volantini e lo svolgimento di test di auto-valutazione del proprio livello di awareness (pratiche diffuse nel 37% delle imprese del campione), l'organizzazione di incontri informali (31%) come per esempio gli Hacker lunch, pranzi in cui vengono invitate figure specialistiche come gli Ethical Hacker, che danno testimonianza concreta di quali attacchi sia possibile mettere in atto ai danni delle aziende, la creazione di piattaforme social di confronto, come blog e forum (24%), l'erogazione di formazione tramite attività di gamification (10%) o ancora l'istituzione di attività a premi (3%).

La simulazione di attacchi informatici rappresenta un ulteriore strumento formativo basato sull'esperienza diretta e può essere utile da un lato a misurare il livello di consapevolezza dei dipendenti, mettendone alla prova la resistenza agli attacchi informatici, dall'altro a testare l'efficacia delle iniziative già portate avanti.

Secondo i dati della Ricerca, le campagne di phishing simulato sono un'iniziativa messa in atto dal 39% delle aziende intervistate.

In aggiunta, un utile elemento può essere l'istituzione in azienda di un "contact point" per la segnalazione di eventi anomali, che rappresenti un punto di riferimento per gli utenti per la verifica di email sospette o per fornire supporto e chiarimenti rispetto alle buone prassi comportamentali. Tale figura, presente nel 56% dei casi, può essere individuata ad esempio nel CISO, o, se presente, nel CERT (Computer Emergency Response Team) dell'organizzazione.

Le iniziative di sensibilizzazione devono inoltre essere customizzate rispetto al target di riferimento: è ugualmente importante educare i dipendenti a tutti i livelli dell'organizzazione, qualsiasi sia la loro funzione di appartenenza, ma le attività formative devono essere in linea con le caratteristiche e con le esigenze degli utenti. Tra le azioni citate, quelle che vengono maggiormente indirizzate ad uno specifico e selezionato target all'interno delle aziende sono gli incontri informali (che risultano essere "customizzati" nel 66% dei casi) e la formazione in aula (57%). Relativamente a quest'ultimo aspetto, dovrebbero per esempio essere previsti programmi specifici per i nuovi assunti, piuttosto che sessioni specialistiche per le funzioni aziendali più tecniche, o ancora iniziative dedicate al Top Management o attività indirizzate ai dipendenti che lavorano costantemente a contatto con il pubblico.

Al contrario, le iniziative che vengono più spesso indirizzate all'intera azienda, senza alcuna distinzione di target, sono l'invio di comunicazioni periodiche (93%) e la distribuzione di materiale informativo (79%).

Per ottenere i risultati desiderati, la formazione non dev'essere erogata come un'iniziativa spot, una tantum, ma al contrario prevedere attività periodiche e continuative in logica pluriennale. Vista la rapidità di evoluzione delle tecnologie e delle minacce, infatti, è fondamentale che la popolazione aziendale sia sempre il più possibile aggiornata e consapevole rispetto a ciò che la circonda.

Sebbene sia evidente come le attività formative inizino a diffondersi nelle aziende italiane, è doveroso sottolineare come talvolta si tratti ancora di attività spot, e non di programmi strutturati che prevedano attività periodiche.

A titolo esemplificativo, anche le più diffuse iniziative di formazione online o in aula sono effettuate in maniera ricorrente e strutturata soltanto dal 31% delle organizzazioni, mentre nel 37% si tratta di attività spot, erogate una tantum.

Gli approcci alla gestione del rischio cyber

In continuità con lo scorso anno, l'Osservatorio ha rivolto l'attenzione al tema del rischio cyber ed in particolare al mercato emergente dell'assicurazione del rischio cyber. Anche a livello internazionale, il Report OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) che affronta lo scenario del mercato della cyber insurance[7] pone l'attenzione sull'importanza del quadro normativo nel favorire la quantità di dati disponibili per gestire il rischio cyber. La mancanza di dati, infatti, rappresenta secondo OCSE il principale ostacolo nella diffusione di una cultura sul tema. È auspicabile quindi un ruolo importante delle aziende dell'industria assicurativa nello spiegare le possibili coperture e opportunità di trasferimento del rischio cyber per favorire la crescita del mercato.

Per approfondire al meglio la tematica, quest'anno è stato realizzato dall'Osservatorio un filone di Ricerca dedicato, con una specifica Survey indirizzata ai Responsabili del Risk Management di grandi aziende, che ha visto il coinvolgimento di 106 grandi realtà, e un Workshop di approfondimento sul tema, con 61 partecipanti tra Risk Manager, CISO e rappresentanti del mondo dell'offerta.

[7] Si fa riferimento al Report "Enhancing the Role of Insurance in Cyber Risk Management", Dicembre 2017.

Con riferimento alla definizione dell'Institute of Risk Management, quando parliamo di rischio cyber intendiamo qualsiasi rischio di perdita finanziaria, distruzione o danno alla reputazione di un'organizzazione derivante da un malfunzionamento del proprio sistema informativo.

La gestione del rischio cyber può essere condotta seguendo due vie principali. La prima, generalmente di competenza del CISO, riguarda la *mitigazione del rischio* e ha come principale obiettivo, sebbene non esclusivo, quello di ridurre la *frequenza di accadimento* degli incidenti mediante metodi e strumenti tipici del suo ruolo. La seconda riguarda il *trasferimento del rischio* e in questo caso è necessario il coinvolgimento di altre figure aziendali in aggiunta al CISO, come il Finance ed il Risk Management, con l'obiettivo di *ridurre l'impatto* di possibili incidenti cyber.

Il rischio cyber è solo uno degli scenari di rischio che un'organizzazione, specie se di grandi dimensioni, deve prendere in considerazione. Dalla rilevazione emerge come oggi il cybercrime e le violazioni di sicurezza rappresentino comunque lo scenario di rischio ritenuto più rilevante, seguito dal danno di immagine, i cambiamenti normativi, le interruzioni di business e le crisi economiche.

Le organizzazioni si sentono più preparate ad affrontare i rischi relativi al cybercrime e alle violazioni di sicurezza rispetto a scenari di rischio quali disordini politici, sociali, catastrofi naturali e danno di immagine, ma meno preparate rispetto ad altri temi rilevanti come cambiamenti climatici, mancanza di risorse e competenze, interruzioni di business e innovazione tecnologica solo per citarne alcuni.

Questo scenario testimonia *l'esistenza di un gap tra necessità di governare il rischio e conoscenza degli strumenti* per raggiungere l'obiettivo, oltre che evidenziare un'attenzione notevole sul tema del rischio cyber, che si sta facendo strada tra le priorità aziendali in materia di gestione del rischio.

Le evidenze della nostra Ricerca trovano riscontro anche a livello internazionale: nella classificazione "Global Risk Landscape 2017" del World Economic Forum, gli attacchi cyber si collocano tra i rischi con una maggiore probabilità di accadimento e con un indice di impatto superiore al valore medio degli impatti di tutti gli scenari di rischio considerati[8].

[8] Si fa riferimento alla pubblicazione "The Global Risk Report 2017 – 12th Edition" del World Economic Forum, 2017, in collaborazione con Marsh & McLennan Companies e Zurich Insurance Group.

A fronte di un interesse crescente nei confronti della cybersecurity, la responsabilità della gestione del rischio cyber è ancora in larga parte demandata alla funzione IT, nel 48% dei casi. Solo nel 24% è in carico ad un presidio Security, ancora meno al Risk Management (10%) o al Board aziendale (8%). Nei restanti casi è in capo ad altre funzioni aziendali.

In termini di competenze a supporto della gestione del rischio cyber, il 41% delle organizzazioni dichiara di non avvalersi di nessun soggetto esterno. Nei casi in cui si sceglie di rivolgersi al mercato sono coinvolte società di consulenza (33%), provider di soluzioni tecnologiche o servizi informatici (28%), broker assicurativi (11%), società assicurative (10%), società di consulenza legale (7%).

L'assessment del rischio cyber viene realizzato sulla base di uno standard internazionale (quali ad esempio ISO 27000, NIST, COBIT/ISACA, ecc.) solo dal 45% delle organizzazioni, mentre nel 16% dei casi viene utilizzato un framework sviluppato internamente e nel 25% si fa affidamento a buone prassi senza un framework formalizzato. Infine, il 14% delle aziende non svolge alcun assessment.

La quantificazione degli impatti finanziari derivanti da un eventuale incidente di sicurezza viene svolta dal 44% delle organizzazioni. Per l'8% delle imprese che effettuano la quantificazione, la perdita potenziale viene stimata superiore al 20% del fatturato, dato che evidenzia ancora una volta l'estrema rilevanza strategica della gestione del rischio cyber.

Le componenti considerate nella quantificazione riguardano i costi legati ad interruzioni del servizio (92%), costi legati al ripristino (85%), danno di immagine (62%), penali e sanzioni (62%), risarcimento danni a terzi (59%), assistenza legale o informatica post incidente (44%), richiesta di riscatto (5%).

La Ricerca ha identificato molteplici asset aziendali come possibile oggetto di attacco cyber e ha indagato rispetto a quali di questi i rischi vengano accettati, ignorati, mitigati o trasferiti a terzi. È emerso che il bene per il quale si ricorre maggiormente a metodologie e strumenti per la mitigazione del rischio è rappresentato dai dati sul personale dell'organizzazione, mentre l'asset per il quale si ricorre di più al trasferimento è quello delle infrastrutture critiche. Il rischio reputazionale è quello che viene maggiormente accettato: è un tema ben noto e conosciuto, ma per il quale le aziende ritengono di non possedere strumenti sufficientemente maturi per mettere in atto eventuali azioni di mitigazione o protezione. Infine, il rischio legato alla proprietà intellettuale è quello che viene maggiormente ignorato dalle organizzazioni, perché eccessivamente complesso da analizzare e approfondire o perché ritenuto di minore rilevanza.

In termini di impatto e di probabilità di accadimento degli scenari di rischio cyber, emerge come la proprietà intellettuale, rischio maggiormente ignorato, risulti essere anche quello considerato di minor impatto e probabilità di accadimento. Per contro, il rischio reputazionale, che viene maggiormente accettato, è anche tra quelli per cui si prevedono probabilità

di accadimento e conseguenze maggiori. Tra gli altri rischi esaminati, dal più grave al meno grave come impatto e probabilità di accadimento, emergono l'interruzione del servizio, il furto o la perdita di dati dei clienti, l'alterazione di dati o software, i danni materiali alle infrastrutture.

Il quadro che emerge sulla gestione del rischio cyber mostra una situazione a luci e ombre, che potremmo definire "artigianale", considerato il fatto che stiamo parlando di grandi realtà strutturate. Tuttavia l'interesse nei confronti del tema è crescente, così come la progressiva presa di coscienza del rischio da parte delle organizzazioni, e gli strumenti a disposizione sono più maturi rispetto al passato. Tra questi, vi è la possibilità di trasferire parte del rischio residuale a soggetti terzi tramite opportune soluzioni assicurative.

Le soluzioni assicurative per la gestione del rischio cyber

Il mercato dell'assicurazione del rischio cyber prevede oggi svariate possibilità di copertura riguardanti la perdita o la divulgazione di dati personali e sensibili. Inoltre è possibile tutelare avvenimenti che riguardano la compromissione del sistema informativo e la sua interruzione di servizio. Le soluzioni assicurative possono tutelare danni causati a terzi, così come danni riguardanti l'azienda stessa.

Con riferimento al campione analizzato, il 27% delle organizzazioni ha già stipulato polizze assicurative per trasferire il rischio cyber (15%) o che lo coprono parzialmente (12%). Il 35% si trova in una fase di valutazione, il 27%, nonostante sia informato della possibilità, non ha intenzione di stipulare alcun tipo di copertura, mentre il restante 11% non ne conosce

l'esistenza. Rispetto allo scorso anno si registra una maggior diffusione: secondo i dati registrati dall'Osservatorio, nel 2016 solo il 15% delle organizzazioni affermava di avere già attiva una polizza assicurativa per coprire il rischio cyber, integralmente o parzialmente.

Se, come visto precedentemente, la responsabilità della valutazione e della gestione del rischio cyber è in mano al Risk Management solo nel 10% dei casi, nella fase di acquisto della polizza emerge invece come il ruolo di tale figura sia centrale. Il Risk Management è infatti responsabile del processo di acquisto per il 64% delle organizzazioni intervistate, seguito dall'IT (58%), dal Board aziendale (43%), dal Finance (40%), dalla Security (38%) e dal Legal (32%).

In termini di aree di copertura, l'84% delle organizzazioni che ha stipulato una polizza cyber gode di una copertura riguardante i danni subiti direttamente, il 71% riguardante i danni in seguito a richieste di terze parti, il 39% relativa alla gestione delle istruttorie.

Entrando nel merito, le polizze stipulate si attivano in seguito alla violazione di dati personali di terzi (82%), ad azioni cyber di tipo estorsivo (69%), al furto di informazioni operative interne (49%), a omesso o errato trattamento dei dati (49%), a downtime di rete o interruzione del servizio (45%), a danni materiali a infrastrutture fisiche (39%) e a danni d'immagine (37%).

Le motivazioni che guidano l'acquisto di una polizza cyber sono molteplici: al primo posto figura ancora una volta il Regolamento europeo per la data protection (42%), a seguire l'adeguamento alle direttive aziendali di tipo nazionale ed internazionale (34%), la convenienza economica (24%) e le richieste delle società di Audit (8%).

Dall'altro lato, per le organizzazioni che dichiarano di non avere intenzione di ricorrere all'adozione di tali strumenti i freni sono legati ad un mercato della cyber insurance ritenuto ancora scarsamente maturo (48%), alla difficoltà nel valutare costi e benefici (26%), al costo troppo elevato delle polizze (17%), alla scarsa rilevanza del problema in azienda (17%), all'asimmetria informativa spesso riscontrata tra assicuratore ed assicurato (4%) e alla scarsa adeguatezza delle polizze proposte (4%).

L'analisi delle PMI

Le piccole e medie imprese rappresentano più del 99% del tessuto produttivo italiano[9] e generano da sole il 69% del valore aggiunto. La Ricerca 2017 dell'Osservatorio ha visto il coinvolgimento di un campione di 947 PMI (aventi un numero di addetti compreso tra 2 e 249) rappresentative della totalità delle microimprese e delle piccole e medie aziende italiane[10] e, coerentemente con quanto indagato nelle realtà di grandi dimensioni, ha analizzato la diffusione di soluzioni di information security, le principali motivazioni che guidano le scelte delle imprese, i trend di maggiore impatto e le scelte organizzative. La rilevazione ha poi indagato il livello di conoscenza del General Data Protection Regulation (GDPR) e l'approccio con il quale le PMI si pongono davanti a uno degli aspetti più critici in tema di sicurezza aziendale: il fattore umano.

Il livello d'adozione delle soluzioni di information security aumenta al crescere della dimensione aziendale, raggiungendo circa il 93% nelle medie imprese. Nello specifico, circa il 44% di quest'ultime dispone di soluzioni tecnologiche ritenute sofisticate, quali sistemi di Intrusion Detection o di Identity and Access Management. Nelle piccole imprese sono

[9] Nello specifico, le microimprese rappresentano il 95,4% del totale delle aziende attive italiane. Il restante 5% si divide tra piccole imprese (4%), medie imprese (0.5%) e grandi aziende (0,1%). (Imprese attive, dati Istat 2015).

[10] L'adozione di una strategia di campionamento stratificato ha permesso, attraverso opportuni pesi, di ricondurre il campione di aziende intervistate alla popolazione delle micro, piccole e medie imprese attive in Italia (dati Istat). Per approfondire, vedere la Nota Metodologica.

particolarmente diffusi strumenti di base quali ad esempio Antivirus e Antispam mentre le microimprese si mostrano le più esposte agli attacchi, con un 30% che non adotta alcun tipo di soluzione.

Vi è un gap importante tra lo stato d'adozione di soluzioni di cybersecurity, sofisticate o di base, tra Nord e Sud Italia. Il Nord mostra un utilizzo che si muove tra il 40% del Nord-Ovest e il 30% del Nord-Est. Le regioni del Centro e del Mezzogiorno, per contro, non superano il 20%, attestandosi rispettivamente al 19% e al 15%.

La motivazione principale che spinge le PMI ad investire in sistemi di information security è rappresentata dalla necessità di tutelare i dati dei clienti. Seguono a distanza le aziende che dichiarano di essere guidate nella spesa da esigenze di adeguamento normativo e realtà che affermano di aver effettuato investimenti in seguito ad attacchi informatici subìti.

Dall'indagine emerge inoltre come, nello scenario della trasformazione digitale, il Cloud rappresenti il trend tecnologico che impatta maggiormente sull'evoluzione della spesa in sicurezza informatica delle PMI italiane. Seguono per le medie imprese i Big Data, per le piccole imprese il Mobile, mentre le microimprese vedono come seconda tematica rilevante i Social Network.

La consapevolezza dell'importanza dell'information security passa anche attraverso le scelte organizzative. Nello specifico, nella maggior parte delle piccole e delle microimprese il responsabile della sicurezza informatica è direttamente l'imprenditore stesso o il direttore generale. Al contrario nelle medie imprese la funzione è ricoperta principalmente da un vero e proprio responsabile IT. La figura di un responsabile della sicurezza è presente in meno

del 30% della totalità delle PMI, mentre il 15% non colloca nessuna figura a presidio della tematica.

La Ricerca evidenzia come le PMI sembrino sottovalutare la tematica della creazione di consapevolezza tra i propri dipendenti. Mentre la maggioranza delle imprese di medie dimensioni ha adottato policy e piani di formazione strutturati (anche se si tratta comunque di una maggioranza risicata), le piccole e microimprese si affidano prevalentemente al buon senso e alla responsabilità dei propri dipendenti. La rilevanza attribuita alle attività di formazione cresce con l'aumentare della dimensione aziendale, sebbene si tratti principalmente di iniziative sporadiche.

La nuova regolamentazione europea sulla protezione dei dati crea molte preoccupazioni alle piccole e medie aziende che necessitano di cambiare modalità e modelli di gestione della data protection, spesso senza avere la possibilità di mettere in campo un progetto articolato di adeguamento alla normativa. La consapevolezza di questa urgenza non è però diffusa tra le aziende di minori dimensioni. Sono decisamente poche le piccole e microimprese che hanno in corso un processo strutturato di adeguamento, mentre la percentuale cresce leggermente nelle medie imprese. Un dato tanto rilevante quanto preoccupante, che emerge dall'indagine, è quello per cui più della metà delle piccole e delle microimprese dichiara di non conoscere per nulla il GDPR, nonostante ci si stia ormai avvicinando all'inderogabile scadenza del 25 maggio.

Un percorso impervio… a trazione integrale

Il percorso verso una gestione matura della sicurezza informatica e della privacy si presenta sempre più impervio, difficile da percorre con gli strumenti tradizionali. Tuttavia, l'evidenza dei fatti mostra nel nostro Paese un quadro tutto sommato ottimistico rispetto al passato, sebbene le minacce continuino ad aumentare e a essere sempre più sofisticate. I dati di mercato mostrano chiaramente un crescente interesse verso le tematiche legate alla gestione della sicurezza e della privacy. Emerge inoltre come alcuni dei principali trend dell'innovazione digitale, come il Cloud ed il Mobile, rappresentino oggi elementi concreti nel mix di spesa in gestione della sicurezza delle organizzazioni. Le imprese, in particolare le più grandi, adottano misure per rispondere ai requisiti richiesti dal GDPR, con investimenti consistenti e progettualità di ampio respiro. La figura del Chief Information Security Officer acquisisce maggior rilevanza rispetto al passato e si assiste a una progressiva strutturazione delle funzioni preposte alla gestione della sicurezza, con nuovi ruoli di responsabilità. Il tema della data protection risulta rilevante all'interno delle organizzazioni e si auspica l'introduzione di nuovi percorsi formativi per i professionisti di questo settore. Il fattore umano diviene centrale, con iniziative eterogenee che cercano di stare al passo con le nuove minacce. La gestione del rischio cyber inizia ad entrare nelle strategie aziendali, sebbene i meccanismi di trasferimento del rischio, come le polizze di cyber insurance, siano ancora lontani dall'essere uno strumento largamente diffuso. Infine, per quanto riguarda le PMI, vengono utilizzate soluzioni più sofisticate rispetto al passato, sebbene non siano chiare le implicazioni derivanti dal GDPR.

Aumentano le sfide, ma sta progressivamente mutando anche l'approccio delle organizzazioni: assistiamo all'adozione di nuovi strumenti che permettono un cambio di prospettiva, un boost differente rispetto al passato.

Ricorrendo alla metafora automobilistica possiamo parlare dell'*attivazione di una trazione integrale*, che apre nuove possibilità di fronteggiare un percorso complesso e mutevole: la vera sfida che le aziende dovranno porsi per il futuro sarà quella di trasformare le competenze introdotte e gli investimenti effettuati in cambiamenti strutturali e di lungo periodo, che permettano di far evolvere l'approccio nei confronti della gestione della sicurezza e non rappresentino soltanto un'azione estemporanea compiuta in ottica di mera compliance.

Mariano Corso

Gabriele Faggioli

Alessandro Piva

I Rapporti

I Rapporti con i risultati completi della Ricerca scaricabili da www.osservatori.net

L'innovazione digitale e le implicazioni sulla Security

Il Report risponde all'obiettivo di analizzare le implicazioni sulla security introdotte dai trend che stanno guidando la trasformazione digitale in atto nelle organizzazioni: i Big Data Analytics, il Cloud Computing, il Mobile e l'Internet of Things.
Temi correlati:
Information Security, Compliance, Big Data, Analytics, Cloud, Mobile, Internet of Things

Il quadro normativo di riferimento per la Data Protection

Il Report mira ad approfondire le principali innovazioni introdotte dal nuovo Regolamento europeo sulla protezione dei dati personali e di fornire un possibile piano di adeguamento per le imprese, individuando le azioni che le organizzazioni dovrebbero intraprendere per conformarsi ai nuovi obblighi introdotti dal GDPR.
Temi correlati:
Information Security, Compliance, GDPR, DPO, Data Protection

Le competenze ed i ruoli dell'Information Security & Privacy e l'importanza del fattore umano

Il Report mira ad analizzare la progressiva evoluzione del ruolo del Chief Information Security Officer (CISO) e del mix di competenze che tale figura deve possedere per una corretta gestione dell'information security & privacy. Viene inoltre analizzato il tema del fattore umano, variabile chiave nella progettazione di un sistema di information security.
Temi correlati:
Information Security, Compliance, Governance, Privacy, CISO, Fattore umano

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Information Security & Privacy: lo scenario di mercato in Italia

Il Report mira ad analizzare le principali aree di investimento e le strategie di gestione della sicurezza e della privacy definite dalle imprese, analizzando le dinamiche del mercato delle soluzioni di information security e dei servizi necessari per adempiere ai requisiti richiesti dal General Data Protection Regulation (GDPR).

Temi correlati:
Information Security, Privacy, Compliance, Governance, GDPR, Mercato

La gestione del Rischio Cyber e la Cyber Insurance

Il Report analizza le principali modalità di gestione e valutazione dei principali scenari di rischio cyber all'interno delle imprese e approfondisce le scelte delle organizzazioni rispetto alla possibilità di trasferire il rischio residuo ricorrendo ad apposite soluzioni assicurative.

Temi correlati:
Information Security, Governance, Risk, Cyber Insurance

Esperienze aziendali in ambito Information Security & Privacy

Il Report presenta alcune rilevanti esperienze aziendali selezionate durante la Ricerca dell'Osservatorio. I casi di studio approfonditi costituiscono esempi di successo per quanto riguarda aspetti come la gestione del fattore umano all'interno delle aziende, la capacità di cogliere le opportunità offerte dai trend dell'innovazione digitale e il percorso di adeguamento al General Data Protection Regulation.

Temi correlati:
Information Security, Governance, GDPR, Data Protection, Fattore Umano, Cloud, Internet of Things

I risultati completi della Ricerca sono consultabili su www.osservatori.net

La Nota Metodologica

La Ricerca 2017

La Ricerca 2017 è stata condotta con lo scopo di monitorare lo stato dell'arte di tecnologie e strategie per l'information security e privacy, coinvolgendo le principali organizzazioni end user e fornitrici di servizi e soluzioni di information security del panorama italiano.

Nella Ricerca sono state coinvolte diverse figure professionali che si occupano di security e di privacy, da diversi punti di vista: CISO (Chief Information Security Officer), CSO (Chief Security Officer), CIO (Chief Information Officer), Compliance Manager, Risk Manager, Chief Risk Officer e DPO (Data Protection Officer) di grandi imprese italiane, con focus maggiore sulle prime 1.000 aziende per fatturato e Pubbliche Amministrazioni operanti in Italia. Sono stati inoltre coinvolti i Responsabili dei Sistemi informativi di piccole e medie imprese italiane.

La rilevazione è avvenuta utilizzando diversi strumenti:

- una Survey online volta a monitorare lo stato di adozione di sistemi di Information Security e Privacy aziendale, analizzare i principali modelli di governance adottati dalle imprese e dalle istituzioni per la gestione dell'Information Security & Privacy e a indagare il percorso di adeguamento delle aziende al General Data Protection Regulation (GDPR);
- una Survey online volta ad indagare le modalità di gestione e valutazione dei principali scenari di rischio cyber e le scelte delle organizzazioni rispetto alla possibilità di trasferirli tramite apposita insurance;

- una Survey online volta ad indagare l'interesse verso il tema della Data Protection;
- una Survey online e telefonica rivolta ai Responsabili dei Sistemi informativi di piccole e medie imprese italiane;
- alcuni studi di caso svolti mediante approfondimenti de visu, telefonici o da fonti secondarie con alcune aziende utenti e i principali player dell'offerta, con l'obiettivo di analizzare approfonditamente le iniziative più significative.

I risultati ottenuti dalla rilevazione empirica sono stati discussi e validati attraverso tre incontri a porte chiuse:

- *Il fattore umano e la sua gestione* (30 Maggio 2017) – Il primo Workshop del piano 2017 dell'Osservatorio Information & Privacy ha coinvolto 47 partecipanti (32 appartenenti ad aziende end user e 15 afferenti al mondo dell'offerta). Durante l'incontro sono state studiate le dinamiche relative alla gestione del fattore umano all'interno delle aziende, attraverso un'attività interattiva che ha coinvolto i partecipanti al fine di stimolare il confronto tra le imprese. È infatti noto come spesso azioni inconsapevoli dei dipendenti, dettate da una scarsa conoscenza delle policy aziendali, così come da comportamenti ingenui, espongano le organizzazioni a potenziali attacchi. I partecipanti sono stati suddivisi in gruppi, all'interno dei quali è stata utilizzata una metodologia di lavoro innovativa che prevedeva una mappatura della realtà della propria azienda su un framework di gioco e una successiva discussione all'interno del team di lavoro.
- *I trend tecnologici e gli impatti sulla security* (20 Settembre 2017) – Il secondo Workshop ha coinvolto 45 partecipanti (28 appartenenti ad aziende end user e 17 afferenti al mondo dell'offerta). L'incontro ha indagato l'impatto dei nuovi trend dell'innovazione digitale (Cloud, Internet of Things, Mobile, ecc.) sulla gestione dell'information

security e della privacy all'interno delle aziende. Anche in questa occasione è stata svolta un'attività interattiva che ha visto i partecipanti, suddivisi in gruppi, mappare la propria realtà aziendale su un framework di gioco. Successivamente ampio spazio è stato dedicato alla discussione all'interno di ciascun team di lavoro.

- *La gestione del rischio cyber* (30 Novembre 2017) – Il terzo Workshop ha coinvolto 61 partecipanti (41 appartenenti ad aziende end user e 20 afferenti al mondo dell'offerta). L'incontro ha indagato le modalità di gestione e valutazione dei principali scenari di rischio cyber e ha esplorato le scelte delle organizzazioni rispetto alla possibilità di trasferirli tramite apposita insurance.

La Ricerca 2017 si è focalizzata sui seguenti obiettivi:

- Quantificare il mercato della sicurezza informatica in Italia;
- Comprendere l'impatto del Regolamento UE sulla protezione dei dati e sulle nuove professionalità;
- Indagare come i trend dell'innovazione digitale impattano sulla gestione dell'information security e della privacy;
- Identificare le competenze e i ruoli coinvolti nella gestione dell'information security e le modalità di gestione del fattore umano;
- Analizzare le modalità di gestione del rischio Cyber;
- Monitorare lo stato di adozione di sistemi di information security e privacy nelle organizzazioni italiane;
- Studiare gli impatti sulle grandi imprese e sulle PMI;
- Identificare i casi di successo.

Il Gruppo di Lavoro Data Protection Impact Assessment (DPIA)

Durante la Ricerca 2017 è stato istituito un Gruppo di Lavoro di approfondimento verticale sul tema "Valutazione d'impatto sulla protezione dei dati". Il Gruppo di lavoro si è posto l'obiettivo di definire una metodologia e una linea guida operativa di attuazione del Data Protection Impact Assessment nel contesto del nuovo General Data Protection Regulation (GDPR), che possa essere applicabile nel mondo delle grandi imprese.

L'iniziativa ha visto il coinvolgimento di circa 30 organizzazioni, tra aziende end user e realtà fornitrici di servizi e soluzioni di information security & privacy operanti sul panorama italiano.

Al fine di organizzare il lavoro e consolidare i risultati si sono tenuti tre incontri di condivisione:

- 26 Ottobre 2017 – Durante il primo incontro di condivisione sono stati formati sulla base delle candidature volontarie i gruppi di lavoro incaricati della stesura delle varie sezioni del documento. Per ognuno di essi è stata individuata una persona di riferimento che ha assunto il ruolo di team leader. I singoli gruppi sono poi stati invitati a partecipare a una cartella Dropbox, al fine di condividere il proprio lavoro e monitorarne lo stato di avanzamento.
- 21 Dicembre 2017 – Durante il secondo incontro di condivisione sono stati analizzati i contributi per la stesura della linea guida caricati nella cartella condivisa dai partecipanti ed è stata assemblata una prima bozza del documento. Successivamente è stata richiesta ad ognuno una revisione del proprio contributo, sulla base dei feedback recepiti.
- 06 Febbraio 2018 – In occasione del Convegno finale di presentazione dei risultati della Ricerca dell'Osservatorio sarà presentato il lavoro svolto e condiviso il documento di linee guida nella sua versione finale.

Le Survey

A partire da un modello comune di indagine, sviluppato in funzione degli obiettivi della Ricerca, sono stati definiti i questionari che sono stati sottoposti ai CISO, CSO, CIO, Risk Manager e Chief Risk Officer di organizzazioni di piccole, medie e grandi dimensioni e Pubbliche Amministrazioni presenti in Italia e appartenenti a diversi settori.

Survey Information Security & Privacy – Grandi imprese

La rilevazione ha visto il coinvolgimento di 160 organizzazioni italiane di grandi dimensioni, aventi un numero di addetti superiore a 249. La Survey, volta a monitorare lo stato di adozione di sistemi di Information Security e Privacy aziendale, analizzare i principali modelli di governance adottati dalle imprese e dalle istituzioni per la gestione dell'Information Security & Privacy e a indagare il percorso di adeguamento delle aziende al General Data Protection Regulation (GDPR), è stata indirizzata ai Chief Information Security Officer e ai Chief Information Officer.

ll panel della rilevazione sulle grandi imprese ha la seguente composizione settoriale:

- Manufacturing: 36%
- Retail e GDO: 15%
- Servizi: 12%
- Banche: 11%
- Utility ed Energy: 8%
- PA e Sanità: 7%
- Telco e Media: 6%
- Assicurazioni: 5%

Survey Information Security & Privacy – PMI

La rilevazione ha visto il coinvolgimento di 947 piccole e medie imprese operanti in Italia, aventi un numero di addetti compreso tra 2 e 249. Il processo di campionamento si è basato sulla stratificazione del campione, realizzata a partire dalla distribuzione delle imprese in Italia (dati ISTAT, dicembre 2015). Nel dettaglio, sono state considerate le seguenti variabili di stratificazione:

- Classe dimensionale: microimprese (2-9 addetti), piccole imprese (10 – 49 addetti), medie imprese (50 – 249 addetti);
- Area geografica: Nord-Ovest (Liguria, Lombardia, Piemonte, Valle d'Aosta), Nord-Est (Emilia-Romagna, Friuli-Venezia Giulia, Trentino-Alto Adige, Veneto), Centro (Lazio, Marche, Toscana, Umbria), Mezzogiorno (Abruzzo, Basilicata, Calabria, Campania, Molise, Puglia, Sardegna, Sicilia);
- Settore: 9 settori, riconducibili alla classificazione ATECO delle attività economiche. Finanza e assicurazioni, ICT, media e comunicazione, Commercio, Manufacturing, Turismo & Travel, Costruzioni, Servizi alla persona, Servizi alle imprese, Altro.

Il questionario è stato quindi somministrato sia online sia telefonicamente ad un campione di micro, piccole e medie imprese italiane, scelte casualmente in ogni strato. Le elaborazioni complessive sono state condotte attribuendo dei pesi a ogni unità campionaria, a partire dal rapporto tra la numerosità delle imprese italiane e il numero di rispondenti presenti in ogni specifico strato. Ciò ha permesso di rendere i risultati statisticamente rappresentativi dell'intera popolazione di piccole e medie imprese italiane.

Survey Cyber Risk & Insurance

La rilevazione ha visto il coinvolgimento di 106 organizzazioni italiane di grandi dimensioni. La Survey, volta ad indagare le modalità di gestione e valutazione dei principali scenari di rischio cyber e le scelte delle organizzazioni rispetto alla possibilità di trasferirli tramite apposita insurance, è stata indirizzata principalmente ai Chief Risk Officer e ai Risk Manager.

Il campione considerato nelle analisi comprende tutti i settori aziendali. Il panel della rilevazione ha la seguente composizione settoriale:

- Manufacturing: 29%
- Servizi: 27%
- Finance: 19%
- Retail e GDO: 6%
- Offerta ICT: 5%
- Utility: 4%
- PA: 4%
- Telco e Media: 4%
- Sanità: 2%

Survey sul ruolo della Data Protection

La rilevazione, volta ad indagare l'interesse nei confronti della Data Protection, ha visto il coinvolgimento di 313 professionisti del settore appartenenti a organizzazioni operanti in Italia. Il campione considerato nelle analisi comprende tutti i settori aziendali. Il panel della rilevazione ha la seguente composizione settoriale:

- ICT: 33%
- Manufacturing: 10%
- PA: 10%
- Telco e Media: 10%
- Bancario e assicurativo: 9%
- Consulenza di direzione: 9%
- Università/Formazione/ Centri di ricerca: 6%
- Utility: 6%
- Retail e GDO: 4%
- Servizi: 3%

La quantificazione del mercato

La metodologia di stima del mercato ha seguito un approccio caratterizzato da una triplice prospettiva:

- top-down, tramite il coinvolgimento dei principali vendor del settore: in particolare sono stati analizzati tramite interviste dirette, telefoniche o fonti secondarie, oltre 100 organizzazioni operanti nel territorio italiano;
- bottom-up, tramite la rilevazione della spesa in soluzioni e servizi di information security da parte delle organizzazioni italiane end-user stratificate per classe dimensionale e settore di mercato;
- fonti secondarie, analizzando ricerche e studi dei principali vendor e analisti internazionali.

Gli studi di caso

Sono stati effettuati 40 approfondimenti dettagliati attraverso la conduzione di interviste telefoniche o de visu ai Chief Information Security Officer di alcune grandi aziende ritenute particolarmente rilevanti. Gli studi di caso hanno indagato in particolare gli ambiti seguenti:

- Posizionamento e organizzazione della funzione information security all'interno dell'azienda;
- Impatto dei nuovi trend tecnologici (Cloud, Mobile, Big Data, Internet of Things) sulla sicurezza aziendale e relativa gestione;
- Iniziative di awareness sviluppate;
- Impatto e percorsi di adeguamento al Regolamento europeo sulla protezione dei dati.

Il Gruppo di Lavoro

Mariano Corso
Responsabile Scientifico

Gabriele Faggioli
Responsabile Scientifico

Alessandro Piva
Direttore

Giorgia Dragoni
Ricercatrice Senior

Luca Dozio
Ricercatore

Andrea Antonielli
Ricercatore Junior

Irene Di Deo
Ricercatrice Junior

Martina Broggi
Program Management Office

Si ringrazia inoltre per il supporto specialistico:

Luca Bechelli
Consiglio Direttivo, CLUSIT

Raoul Brenna
Responsabile della Practice Information Security & Infrastructures, CEFRIEL,
Co-direttore Corso Information Security Management

Guglielmo Troiano
Senior Advisor

Per qualsiasi commento e richiesta di informazioni:
alessandro.piva@polimi.it | giorgia.dragoni@polimi.it

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

La Community dell'Osservatorio Information Security & Privacy

Giorgio Alchieri,
Information and IT Security Manager, Prysmian Group

Valentino Angeletti,
Referente Cyber Security OT, Enel

Moreno Baldini,
IT Information System Manager, Butali

Luciano Bearzi,
System & Network Manager, Same Deutz – Fahr Group

Michele Bona,
Responsabile Information Security Audit, Italiaonline

Alberto Borgonovo,
CISO,
Gruppo Mediobanca

Barbara Brunetti,
CIO,
Varvel

Marco Caleri,
Responsabile Sicurezza Sistemi, Autostrade per l'Italia

Simone Campera,
Corporate IT Security & Compliance Manager, Amplifon

Mauro Capitanio,
IT Security & Compliance Manager, Gruppo Percassi

Salvatore Carrino,
Senior Vice President, Eni

Roberto Castagnetti,
IT Risk Executive, Banca Popolare dell'Emilia Romagna

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Carlo Causio,
Chief Risk Officer,
Telespazio

Daniele Cavagnero,
Senior Manager IT Infrastructure
Europe & Middle East,
Johnson Electric

Massimiliano Chiardoni,
Responsabile Cyber Security,
Sogin

Andrea Chittaro,
Head of Global Security & Cyber
Defence Department, Snam

Corradino Corradi,
Head of ICT Security & Fraud
Management, Vodafone

Massimo Cottafavi,
Information & Cyber Security
Manager, Snam

Marco Destro,
Group CIO,
Afv Acciaierie Beltrame

Massimo Di Lauro,
IT Security Manager,
Kering

Antonio Durante,
Responsabile Compliance IT,
Italgas

Maurizio Freschi,
ICT Manager,
Alia Servizi Ambientali

Sara Galbiati,
Corporate Legal Affairs Specialist,
Comifar Distribuzione

Elisa Garavaglia,
Chief Information Security Officer,
Axa Global Direct

Paolo Grigoletto,
Sicurezza delle informazioni
e privacy, Infocamere

Cristina Guffanti,
Data Security Partner,
Robert Bosch

I risultati completi della Ricerca sono consultabili su www.osservatori.net

Alberto Iacop,
Head of IS Europe and Italy,
ABB

Sergio Leonardo Insalaco,
Responsabile Standard – Continuità e Sicurezza dei Servizi Informatici,
UnipolSai Assicurazioni

Gianfranco Labonia,
Supply Chain & Merchandising IT Area Manager, La Rinascente

Roberto Maraglino,
Data Protection Officer,
Randstad

Gianluca Martinuz,
Head of Information Security & Fraud Management, FinecoBank

Sergio Mattioli,
Information Security and Data Privacy Director, Robert Bosch

Domenico Nilo Mazza,
Responsabile Sistemi Informativi,
IZSLER

Vinicio Mazzei,
IT Risk, Security and Compliance Manager, Saipem

Filippo Morosini,
ICT Corporate Infrastructure and Security Project Manager, Tenova

Omar Moser,
Group CIO,
Gnutti Carlo Group

Antonio Mura,
Risk Manager,
Ilva

Sara Pagani,
Data Security Partner,
Robert Bosch

Ignazio Parrinello,
Information Security and Data Privacy Specialist, Robert Bosch

Stefano Pastori,
Information Security & Data Privacy Specialist, Ikea Italia Retail

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Emanuele Patrini,
Head of Risk Manager & Antifraud,
AmTrust Europe Limited

Michele Pavan,
Responsabile Information Security,
Banca IFIS

Vincenzo Pensa,
Direttore Sistemi Informativi
e Innovazione, ACI Global

Fabrizio Pizzo,
Chief Technology Officer, Fondazione
Don Carlo Gnocchi

Ruggero Platolino,
Information Security Officer,
Luxottica

Laura Quaroni,
Responsabile Servizio Security
Management, Banca IFIS

Riccardo Roncon,
Responsabile Sicurezza IT, Gruppo
ITAS Assicurazioni

Enrico Maria Rossi,
CSO, Gruppo bancario
Credito Valtellinese

Corrado Salvemini,
Responsabile Sicurezza delle
informazioni – Direzione Sistemi
Informativi, Carrefour

Gian Luigi Sangermani,
CIO,
Silvano Chiapparoli Logistica

Simone Santini,
CISO,
Cnp Unicredit Vita

Giampaolo Tacchini,
CISO e Responsabile Infrastrutture
e Servizi ICT, Edison

Sandra Teri,
Insurance Specialist,
Boehringer Ingelheim

Marco Terzago,
Head of Group Risk Engineering
– Area Risk Managers Global
Coordinator, SKF Industrie

I risultati completi della Ricerca sono consultabili su www.osservatori.net

Enrico Luigi Toso,
IT Regulatory Risk and Control Specialist, Deutsche Bank

Mario Trovato,
IT Manager,
LVMH Italia

Ileana Vanzini,
Information Security Expert,
Bayer

Maria Gaia Vinciguerra Frezza,
Data Protection, Security & Compliance Manager, Europcar

Andrea Volponi,
Information Technology – Security Operation & Monitoring Manager,
Alitalia

Gabriele Zavaroni,
Infrastructure & Communication Manager – ICT Department,
Comer Industries

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

GDPR e Security: un percorso impervio… a trazione integrale

Il Convegno

Febbraio 2018

L'Agenda del Convegno

6 Febbraio 2018

8.45 **Registrazione e Welcome Coffee**

9.15 **Benvenuto**

Mariano Corso
Responsabile Scientifico
Osservatorio Information Security & Privacy

9.30 **Presentazione dei risultati della ricerca**

Gabriele Faggioli
Responsabile Scientifico
Osservatorio Information Security & Privacy e presidente, CLUSIT

Alessandro Piva
Direttore
Osservatorio Information Security & Privacy

Giorgia Dragoni
Ricercatrice
Osservatorio Information Security & Privacy

10.25 **Competenze per la gestione della sicurezza e della data protection**

Ne discutono:

Andrea Bignozzi
General Manager, Nest2

Elisa Garavaglia
Chief Information Security Officer, Axa Global Direct

Vinicio Mazzei
IT Risk, Security and Compliance Manager, Saipem

Giuliano Merlo
Responsabile IT Risk and Security, Generali

Paolo Rossi
Ground Segment Engineering Manager and ISMS Security Manager, Skylogic

11.00 **Commento ai risultati della Ricerca**

Raoul Brenna
Responsabile della Practice Information Security & Infrastructures, CEFRIEL, Co-direttore Corso Information Security Management

11.10 **Nuove metodologie di difesa e di trasferimento del rischio**

Ne discutono:

Valentino Angeletti
Referente Cyber Security OT, Enel

Andrea Bono
General Manager, Marsh SpA

Alessandro Cosenza
Chief Information Security Officer, BTicino

Alessandro Gioso
Senior Principal System Engineer, Symantec

Andrea Mercurio
Responsabile Security Operations and Products, AlmavivA

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

11.45 GDPR: esperienze e strumenti

Ne discutono:

Mariangela Fierro
Accenture Security Senior Manager, Application Security Lead in ICEG (Italy, Central Europe and Greece)

Gianluca Giaccardi
Chief Product Officer, TESISQUARE

Fabio Gianotti
Chief Security Officer | Resp.Direzione IT Security & Business Continuity, UBI Sistemi e Servizi

Daniele Sangion
Head of Group ICT Security for GDPR, Unicredit

12.15 Il Gruppo di Lavoro Data Protection Impact Assessment

Luca Bechelli
Consiglio Direttivo, CLUSIT

12.25 GDPR: la roadmap di adeguamento

Ne discutono:

Sonia Crucitti
Partner, Spike Reply

Riccardo Roncon
Responsabile Sicurezza IT, Gruppo ITAS Assicurazioni

Renato Sesana
Partner BRS, Grant Thornton Financial Advisory Services

Enrico Luigi Toso
IT regulatory risk and control specialist, Deutsche Bank

13.00 Cybersecurity Certification Framework: il contributo dell'Osservatorio

Gabriele Faggioli
Responsabile Scientifico Osservatorio Information Security & Privacy e presidente, CLUSIT

13.15 Executive lunch

Sul sito **www.osservatori.net** è possibile rivedere le riprese integrali del Convegno **"GDPR e Security: un percorso impervio… a trazione integrale"**

Visita **www.osservatori.net** e seguici sui nostri **social network**

I risultati completi della Ricerca sono consultabili su www.osservatori.net

I Relatori

Valentino Angeletti
Referente Cyber Security OT,
Enel

In Enel dal 2010, ricopre il ruolo di referente per il laboratorio di Cyber Security allestito dall'azienda per eseguire sperimentazioni su tecnologie industriali ed ICS. Nel 2016, a valle di una forte ristrutturazione del gruppo e della trasformazione della divisione Cyber Security in Global ICT Cyber Security direttamente a staff della direzione, partecipa alla definizione ed applicazione del nuovo "Framework" di Cyber Security. È coordinatore su progetti tecnologici di Cyber Security OT e definizione di policy e linee guida per la medesima area.

Luca Bechelli
Consiglio Direttivo,
CLUSIT

Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni. Dal 2007 è membro del Consiglio Direttivo e del Comitato Tecnico Scientifico del Clusit.

Andrea Bignozzi
General Manager,
NEST2

Laureato in ingegneria elettronica, nel 2015 ha conseguito un M.B.A presso il MIB di Trieste. Vanta una carriera nel mondo IT di oltre 20 anni ed è attualmente socio e general manager di NEST2, di cui ha curato l'impostazione strategica, ampliato il NOC e creato la BU di Service Management. Sotto la sua guida NEST2 è cresciuta costantemente e, nel 2017, si è posizionata tra le prime 70 aziende italiane di servizi informatici (fonte IDC).

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Andrea Bono
General Manager,
Marsh

Andrea Bono è General Manager di Marsh Spa dal giugno 2015, Membro del CdA di Marsh Spa e Presidente di Marsh Risk Consulting Services Srl. Entrato in Marsh nel 2010 come responsabile del segmento Risk Management, ha iniziato la sua carriera come Lloyd's Broker a Londra nel 1996 ricoprendo ruoli di crescente responsabilità che nel 2001 lo hanno riportato in Italia. Nato a Torino dove si è laureato, è sposato con due figli.

Raoul Brenna
Responsabile della Practice Information Security & Infrastructures,
Co-direttore Corso Information Security Management,
CEFRIEL

In CEFRIEL, Centro di Eccellenza del Politecnico di Milano per la Digital Innovation, si occupa di sicurezza informatica da oltre 10 anni, affrontando la tematica sia da un punto di vista "tradizionale" (tecnologico e di processo), sia esplorando ambiti innovativi (sicurezza del fattore umano, nuovi assessment efficaci, IoT/ICS security e sicurezza nei paradigmi emergenti, come Industry 4.0). Su questi temi collabora attivamente, oltre che con MIP, anche con AIEA, CLUSIT e altre associazioni di settore.

Alessandro Cosenza
Chief Information Security Officer,
BTicino

He is responsible for maintaining the enterprise vision of ITC department. He manages the team in order to develop, implement and maintain processes across the organization to reduce information technology (IT) risks. He works to help company to develop the implementation and ongoing monitoring of General Data Protection Regulation (GDPR). He supports the Company Group, key business units and executive leadership in demonstrating compliance with data protection principles across a range of customer facing and internal activities. He holds the ISACA certification, Certified Information Security Auditor (CISA) and he is also member of CLUSIT.

Partner di Spike Reply, società di consulenza del Gruppo Reply specializzata in Cyber Security, Risk Management & Data Protection, opera da più di 18 anni nel campo della security. Nel 2004, dopo alcune esperienze in primarie realtà italiane dell'information security, approda in Spike Reply per avviare la divisione di Information Risk Management e Compliance ricoprendo nel corso degli anni ruoli sempre di maggior rilievo. Dal 2017 guida il gruppo di lavoro sul GDPR, all'interno della Practice Cyber Security di Reply.

Sonia Crucitti
Partner,
Spike Reply

Mariangela is a Security Senior Manager with more than 13 years of experience in design and governance of ICT security projects, with a focus on Telco and Financial Services industry. She started her carrier as Security Architect and Engineer in Telco companies with a focus on Infrastructure Security and Security Compliance. In 2010 she joined Accenture and she has now the responsibility for the Application and Data Security & Privacy offering for ICEG region.

Mariangela Fierro
Security Senior Manager,
Application Security Lead in ICEG (Italy, Central Europe, and Greece),
Accenture

Laureata in Economia presso l'Università Cattolica del Sacro Cuore di Milano, inizia un percorso decennale in una primaria società di consulenza, lavorando nel mondo ITC con particolare attenzione ai processi di business assicurativi e quelli contabili. Nel 2008 si unisce al team della nascente Compagnia Diretta del Gruppo Axa, Quixa, con il ruolo di Demand Manager. Dal 2013, in risposta al Programma Axa di Trasformazione in ambito Security, assume il coordinamento e la leadership di tale programma all'interno della Compagnia. Viene nominata Chief Information Security Officer nel 2014. Oltre alla Security, è attualmente responsabile dell'IT Governance e della Business Continuity.

Elisa Garavaglia
Responsabile Security, BCM e IT Governance,
Axa Global Direct

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Gianluca Giaccardi
Chief Product Officer,
TESISQUARE®

Gianluca Giaccardi inizia la propria esperienza professionale nell'ambito della consulenza informatica. Nel 1995 è tra i soci fondatori di Tesi e da allora è direttamente coinvolto nella direzione aziendale. Da oltre 15 anni segue clienti di medio-grandi dimensioni, proponendo software orientati al miglioramento dell'efficienza dei processi HR e di quelli legati a normative e policy interne. È Responsabile della Direzione di Prodotto.

Fabio Gianotti
Chief Security Officer | Resp. Direzione IT Security & Business Continuity,
UBI Sistemi e Servizi

Fabio Gianotti is a Security professional with more than 20 years on ICT and Information Security. He currently covers position of CISO for UBI.S (part of UBI Banca) leading IT Security and Business Continuity department. As UBI.S CISO, Fabio's responsibilities is mainly to drive UBI security business strategy, covering cyber security, logical security and ICT security infrastructure aspects, ensuring adequate level of security for UBI, as required by ECB and local regulators within and outside the European Community, where UBI Banca is present.

Alessandro Gioso
Senior Principal System Engineer,
Symantec

Alessandro Gioso dopo gli studi comincia a lavorare nel campo delle telecomunicazioni dopo uno stage di un anno a Amsterdam, nel 1997 passa alla sicurezza informatica e diventa esperto di firewall, ids e endpoint protection. Passato a Symantec come Presales Specialist South Europe realizza importanti progetti in aziende a copertura globale. Grazie agli studi di giurisprudenza segue le normative applicate all'ambito cyber security privacy e Cloud.

Laureato in Ingegneria Chimica, ha iniziato la sua carriera come ingegnere di processo nella progettazione di raffinerie. Dopo aver conseguito l'Executive NBA passa nell'ICT per occuparsi di governance. Certificato CRISC e Lead Auditor ISO 27001 e ISO 20000, dal 2006 nel Gruppo Saipem ha acquisito il ruolo dapprima di responsabile dell'IT Compliance e in seguito anche dell'IT Risk and Security. È il PM del progetto di adeguamento al GDPR.

Vinicio Mazzei
IT Risk, Security and Compliance Manager,
Saipem

Laureato in Fisica, opera da quasi 30 anni nel settore ICT e da oltre 15 anni nell'aera della sicurezza informatica. Attualmente è responsabile dell'area Operations and Products della Cybersecurity Practice di Almaviva. Ha collaborato con istituti universitari quali La Sapienza e LUISS di Roma e UNICAL di Cosenza come docente e relatore di tesi di master in sicurezza. Certificato CISA, CISM, CRISC, ISO27001 auditor, è membro di diversi gruppi di lavoro tecnici ed istituzionali di settore e socio ISACA.

Andrea Mercurio
Responsabile Security Operations and Products,
AlmavivA

Ha maturato un'esperienza in ambito sicurezza informatica di oltre 15 anni passando dalla consulenza informatica a responsabile della sicurezza IT prima in una realtà assicurativa internazionale e oggi presso il Gruppo ITAS Assicurazioni dove ha coordinato la definizione e l'implementazione di un sistema di governo della sicurezza delle informazioni (ISMS) e del modello di gestione "Business Continuity Management". Possiede conoscenze in ambito tecnico, gestionale e normativo nell'ambito della sicurezza IT. Ha conseguito una serie di certificazioni quali ISO 27001 e ITIL.

Riccardo Roncon
Responsabile Sicurezza IT,
Gruppo ITAS Assicurazioni

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Paolo Rossi
Ground Segment Engineering Manager and ISMS Security Manager, Skylogic

Paolo Rossi è Ground Segment Engineering Manager and ISMS Manager presso Skylogic Spa, società del gruppo Eutesat SA, operante nel settore dei servizi di broadband satellitare. Laureato in Ingegneria delle Tlc nel 2002, è approdato a Skylogic nel 2005 come Network Manager e nel corso degli anni ha visto crescere le proprie responsabilità; nel 2009 diventa KA-SAT Ground Segment Design Manager e dal 2015 ricopre anche il ruolo di ISMS Manager.

Renato Sesana
Partner BRS, Grant Thornton Financial Advisory Services

Consulente con vasta esperienza nella Information Security, Cybersecurity, Privacy e, più in generale, nel mondo del Risk Advisory, nel corso della propria carriera professionale ha ricoperto il ruolo di Information Security Manager in diverse realtà di primaria importanza nonché ruoli di sempre più elevata responsabilità nel mondo della consulenza. Ricopre ora il ruolo di Partner Business Risk Services in Grant Thornton Financial Advisory Services.

Enrico Luigi Toso
IT Regulatory Risk and Control Specialist, Deutsche Bank

Già auditor di terza parte sulla sicurezza delle informazioni e della qualità, dal 2001 ha ricoperto ruoli di responsabile della sicurezza e del rischio informatico, di analista e di project manager in Deutsche Bank SpA. Ha maturato competenze di Governance, Risk e Compliance con impatto sull'ICT. Oggi segue progetti di antifrode sui pagamenti, di gestione del rischio e di adeguamento al GDPR e alla PSD2, in particolare su SCA e su CSC con i TPP.

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Gli obiettivi dell'Osservatorio

OSSERVATORI.NET digital innovation

- Quantificare il mercato della sicurezza informatica in Italia
- Comprendere l'impatto del Regolamento UE sulla protezione dei dati e sulle nuove professionalità
- Indagare come i trend dell'innovazione digitale impattano sulla gestione dell'information security e della privacy
- Identificare le competenze e i ruoli coinvolti nella gestione dell'information security e le modalità di gestione del fattore umano
- Analizzare le modalità di gestione del rischio Cyber
- Monitorare lo stato di adozione di sistemi di information security e privacy nelle organizzazioni italiane
- Studiare gli impatti sulle grandi imprese e sulle PMI
- Identificare i casi di successo

GDPR e Security: un percorso impervio... a trazione integrale 06.02.18 #OISP18 Network Digital360 · Events

I risultati completi della Ricerca sono consultabili su www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

I risultati completi della Ricerca sono consultabili su www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Il campione – Survey Information Security & Privacy

OSSERVATORI.NET digital innovation

La scomposizione per dimensione

Grandi imprese (da 250 addetti)

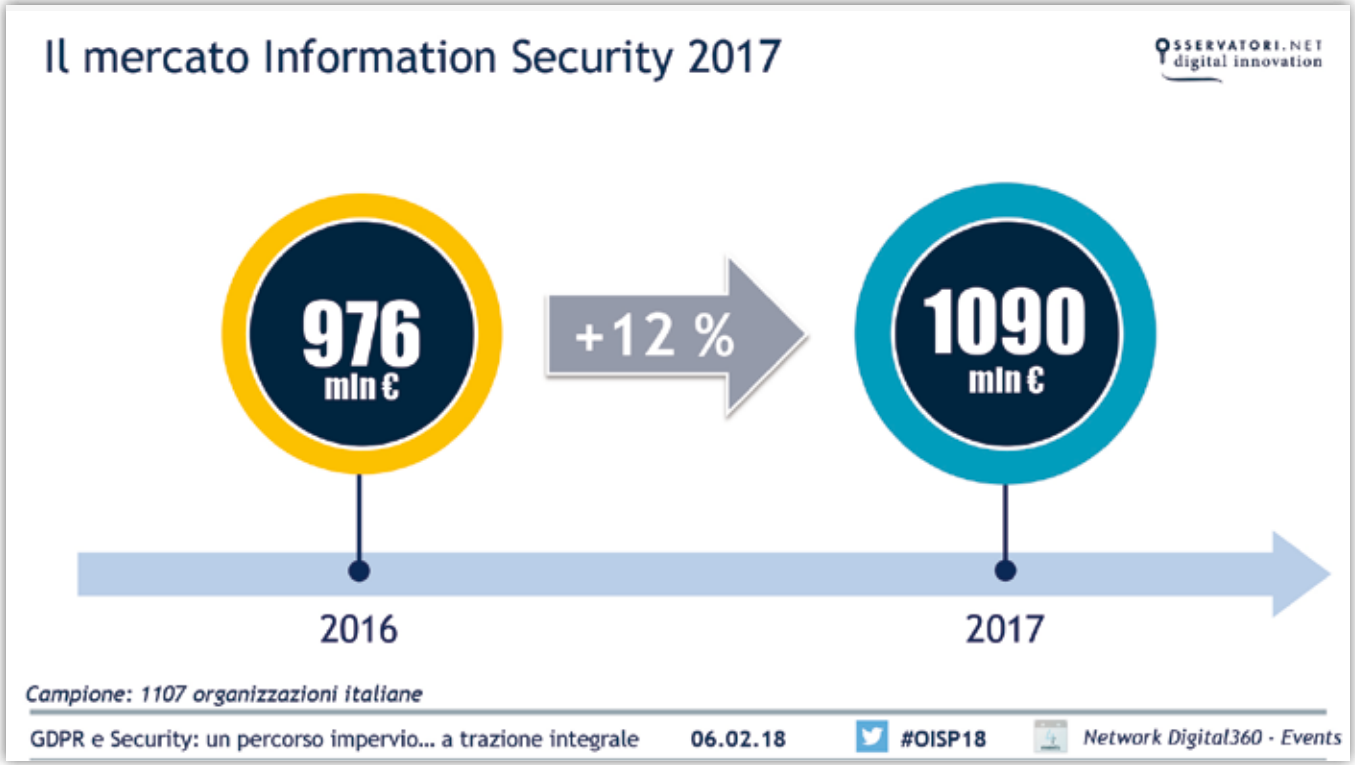
Medie imprese (59-249 addetti)

Piccole imprese (2-49 addetti)

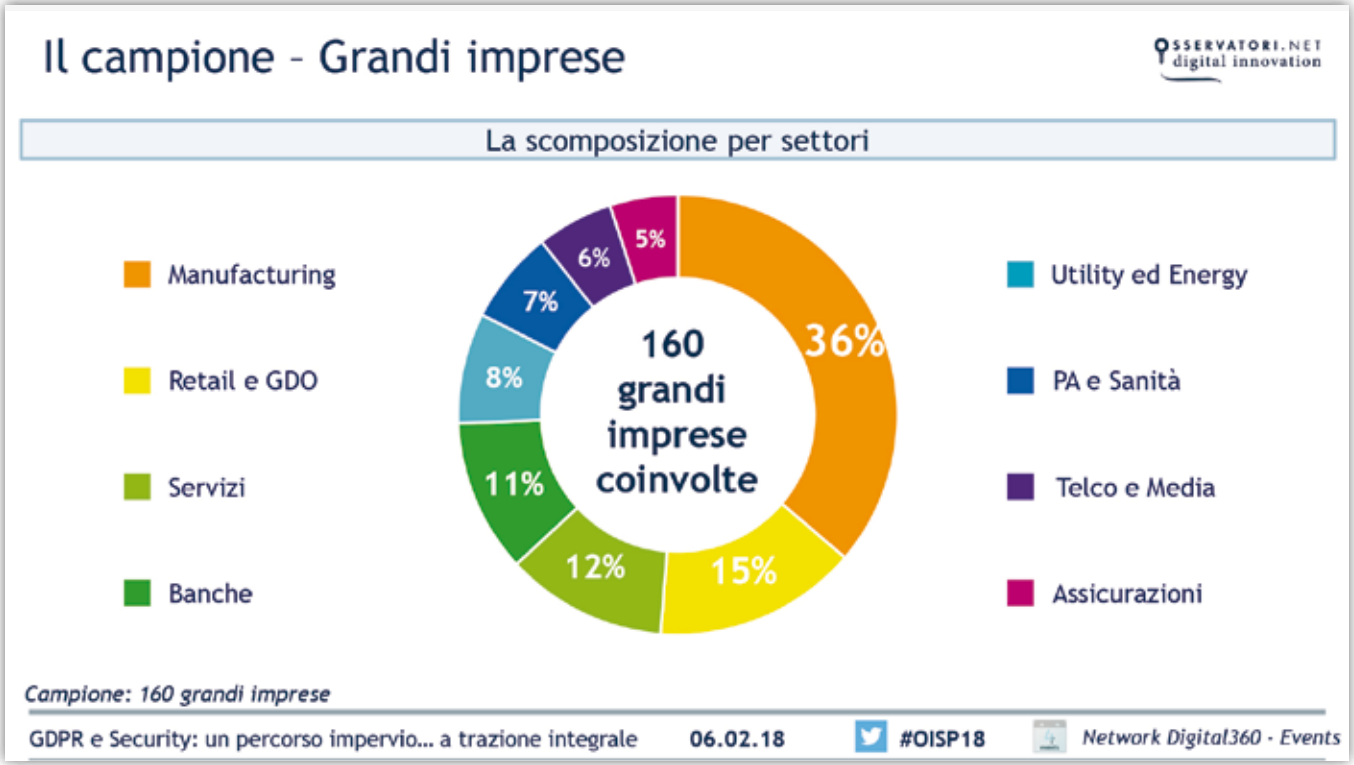
Campione: 1107 organizzazioni italiane

GDPR e Security: un percorso impervio... a trazione integrale **06.02.18** **#OISP18** *Network Digital360 - Events*

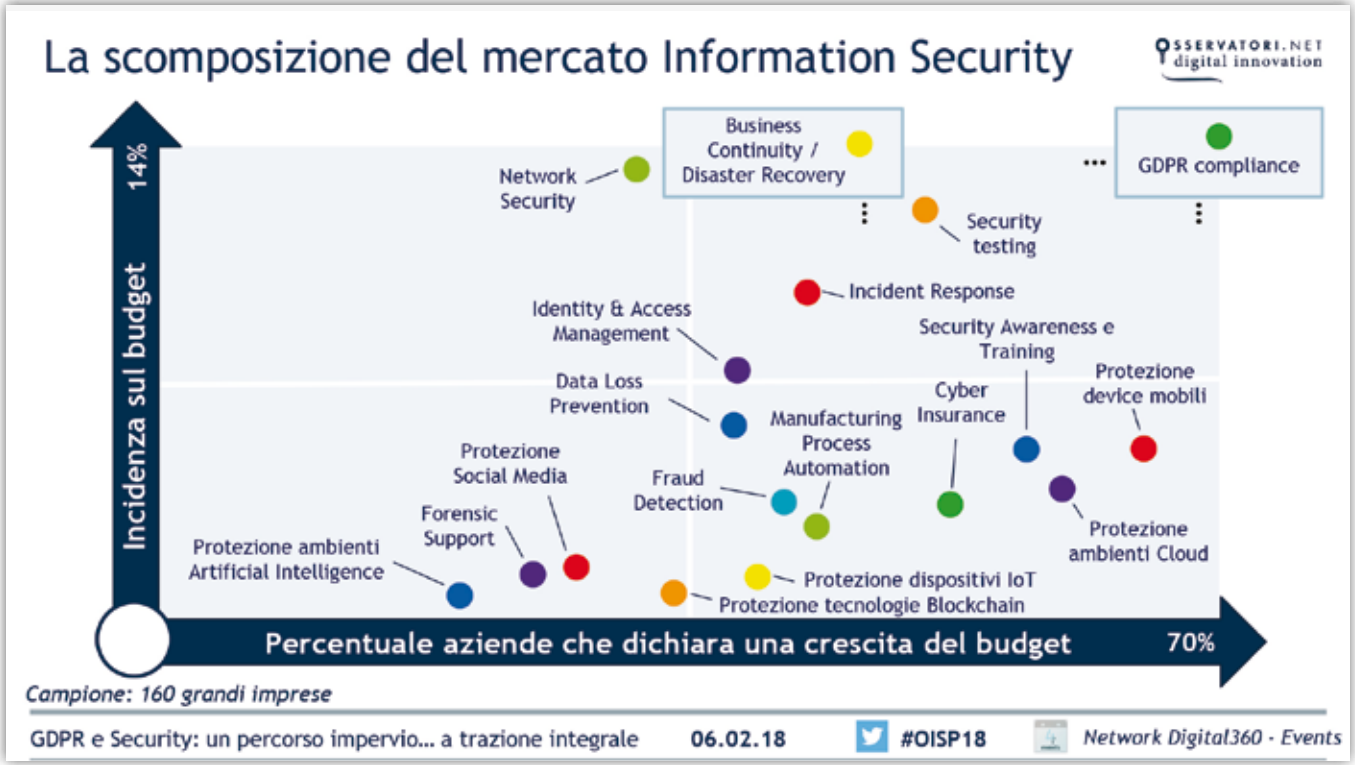
I risultati completi della Ricerca sono consultabili su www.osservatori.net

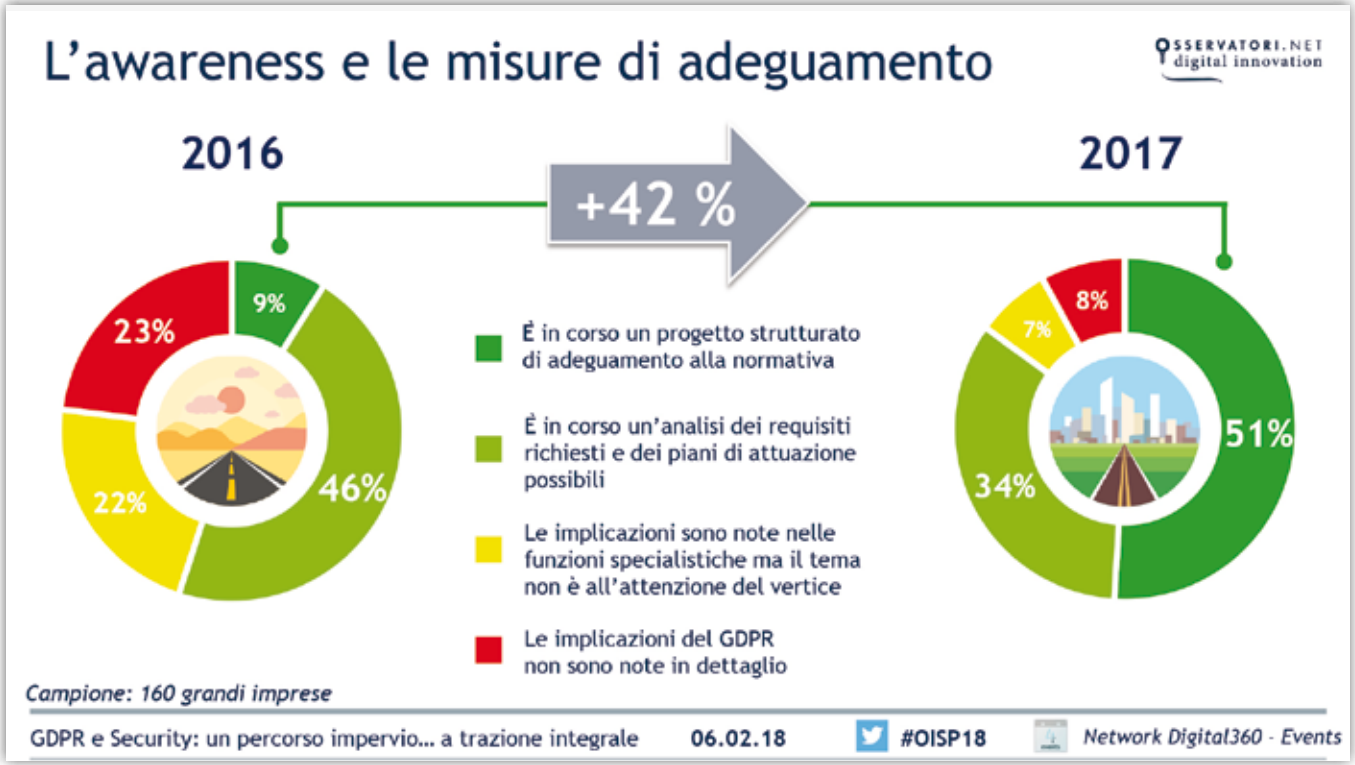


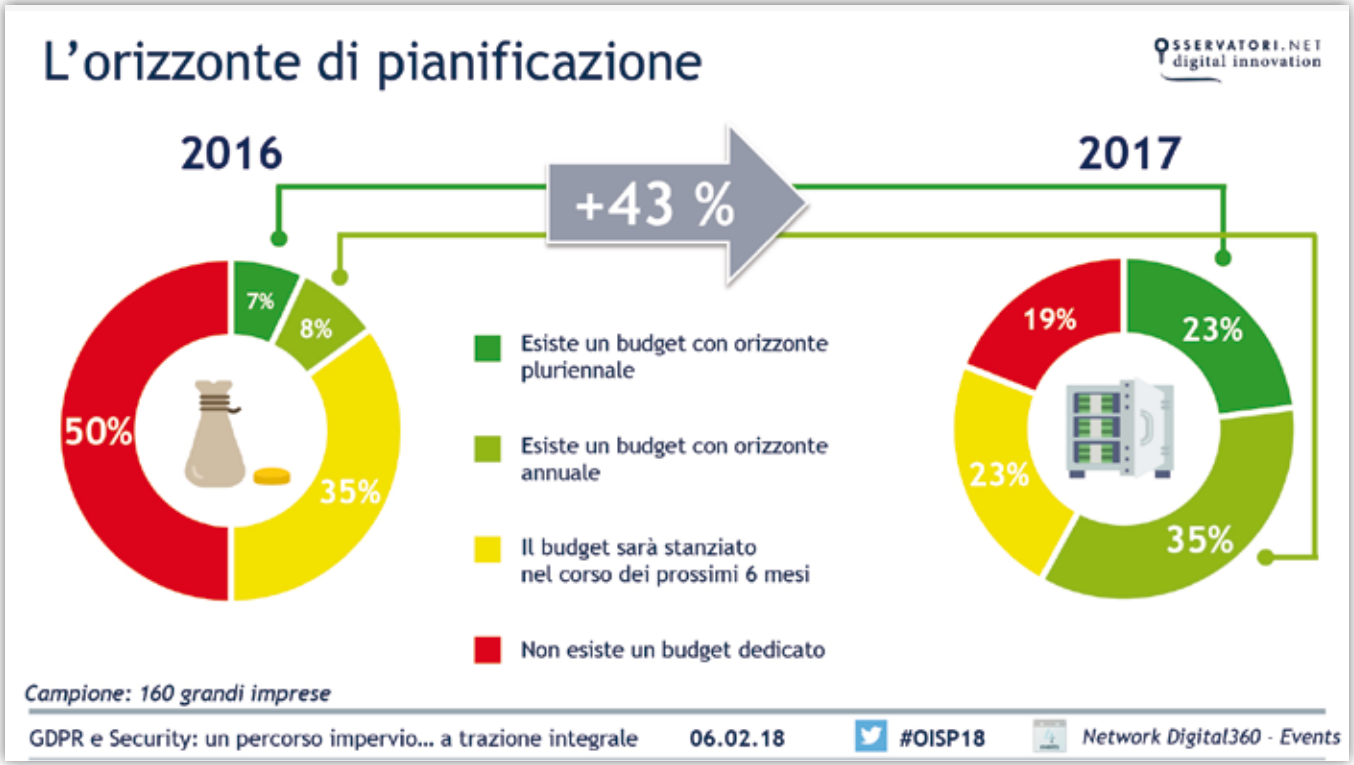
Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net



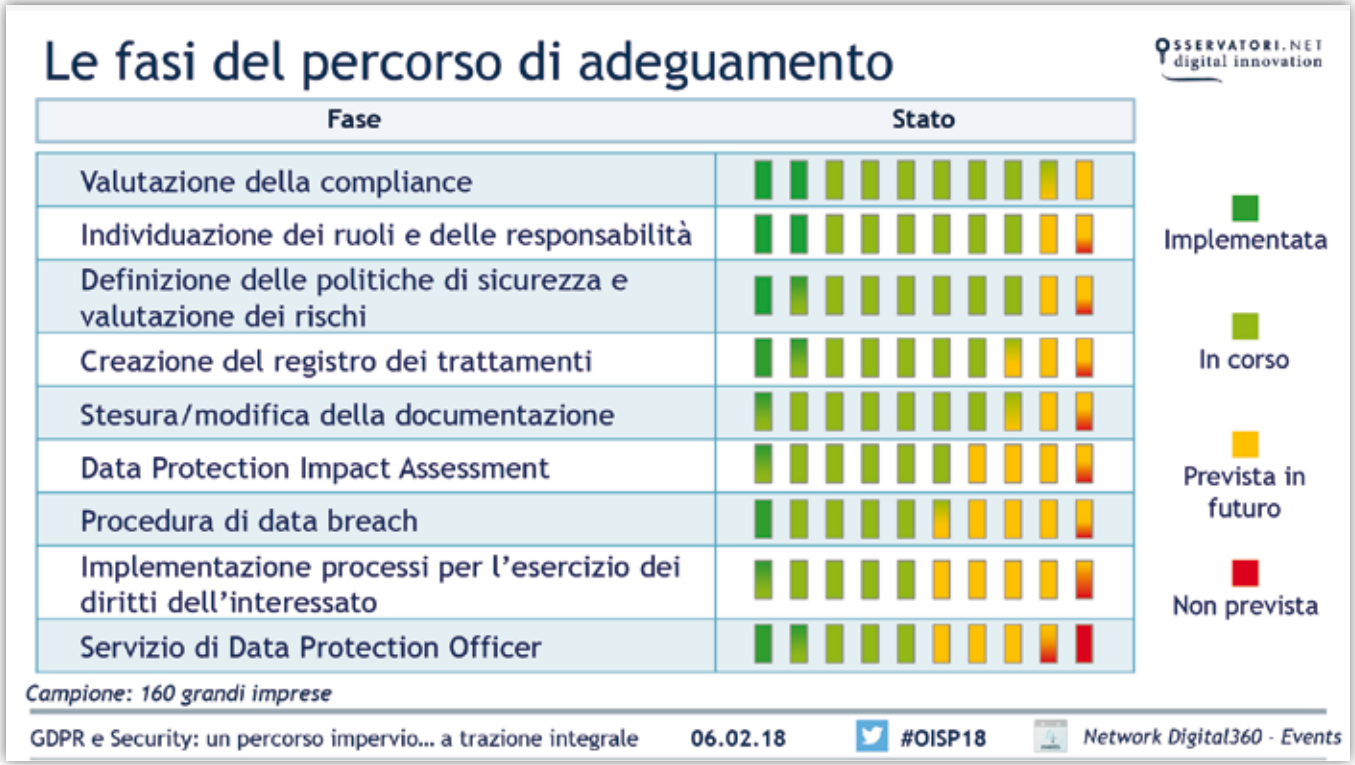
I risultati completi della Ricerca sono consultabili su www.osservatori.net





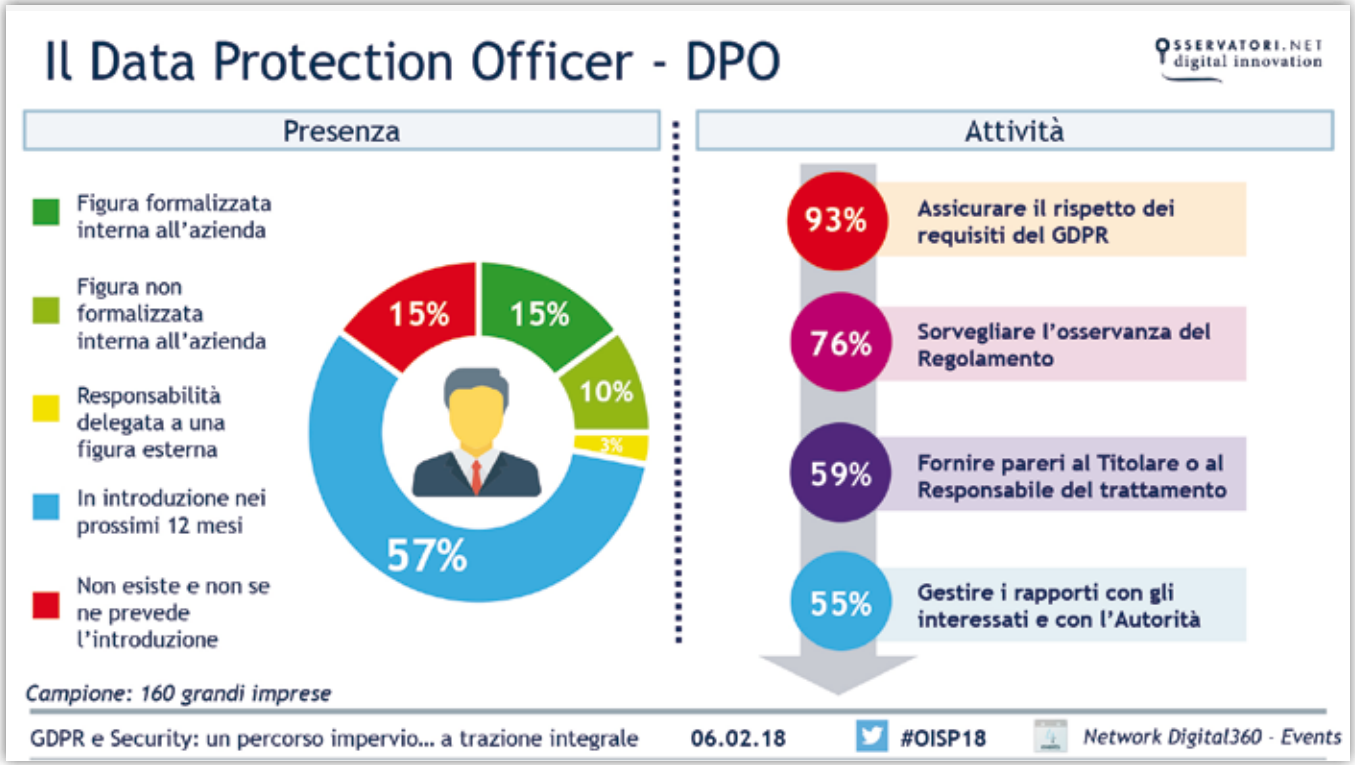


I risultati completi della Ricerca sono consultabili su www.osservatori.net



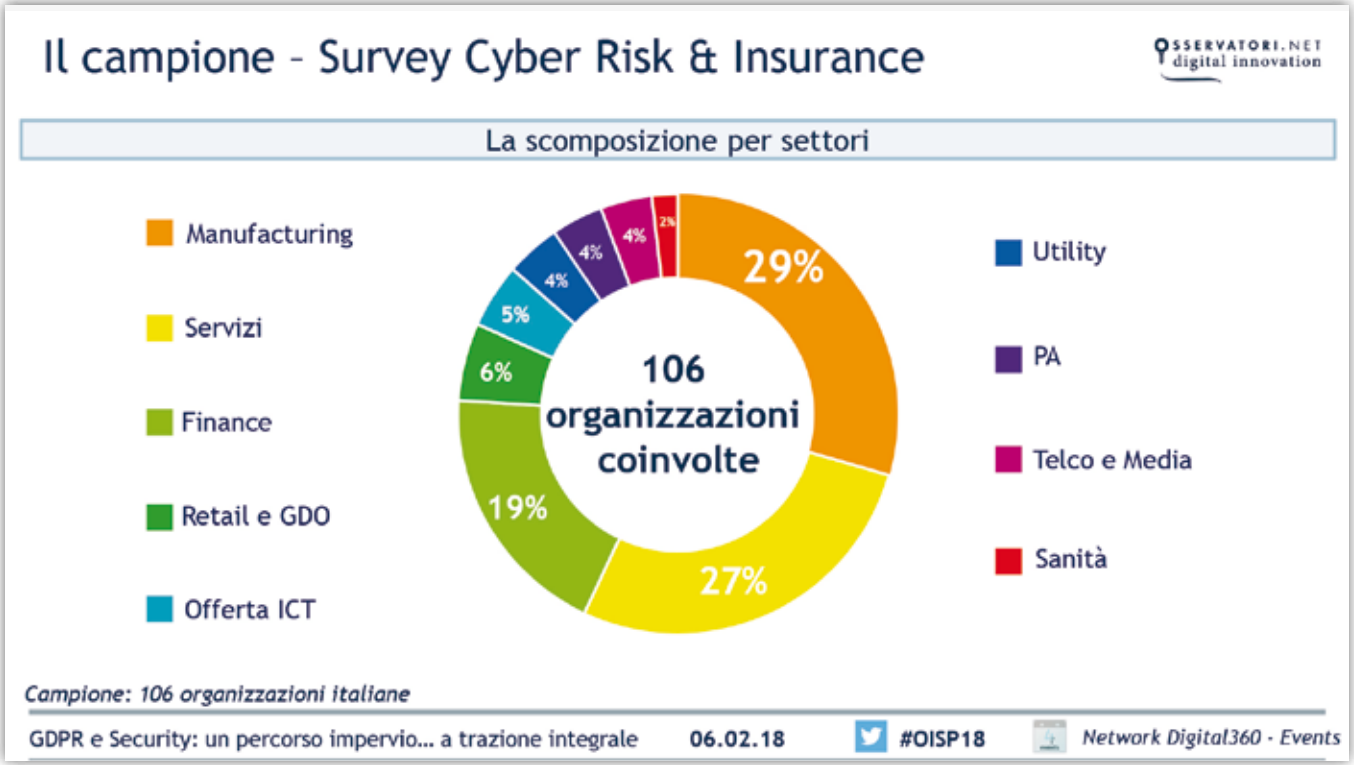
I risultati completi della Ricerca sono consultabili su www.osservatori.net

I risultati completi della Ricerca sono consultabili su www.osservatori.net



I risultati completi della Ricerca sono consultabili su www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net



I risultati completi della Ricerca sono consultabili su www.osservatori.net

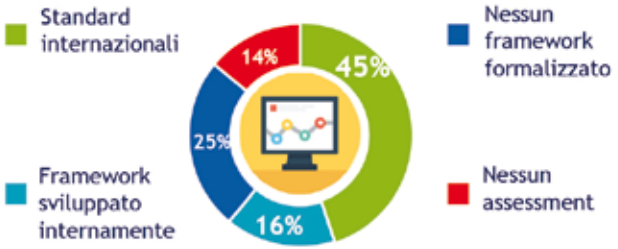
La responsabilità e l'assessment del rischio cyber

OSSERVATORI.NET digital innovation

La responsabilità del rischio cyber

Nel **48%** dei casi
la responsabilità della valutazione e della gestione del rischio cyber è demandata alla **funzione IT**

L'assessment del rischio cyber



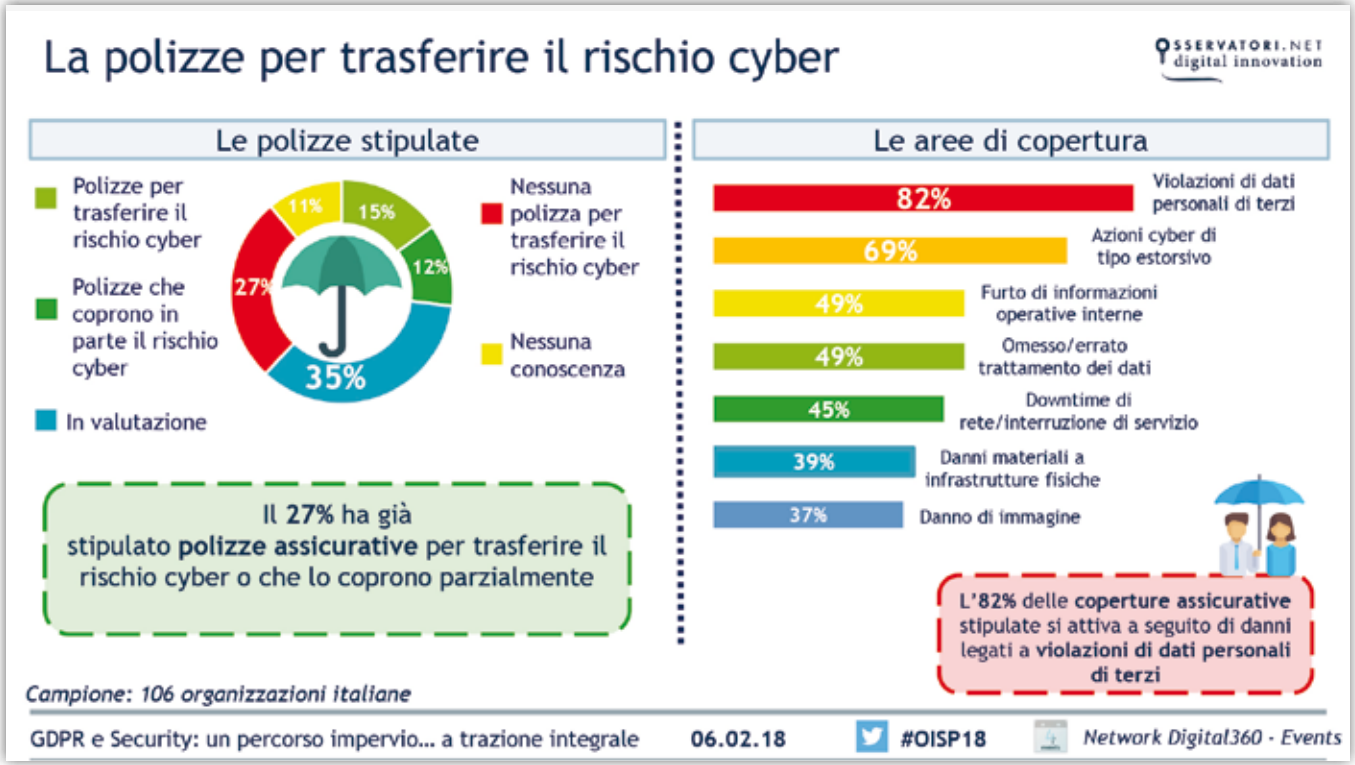
Il **45%** utilizza un **framework** di assessment del rischio cyber basato su **standard internazionali**
(es. ISO 27000, NIST, COBIT/ISACA)

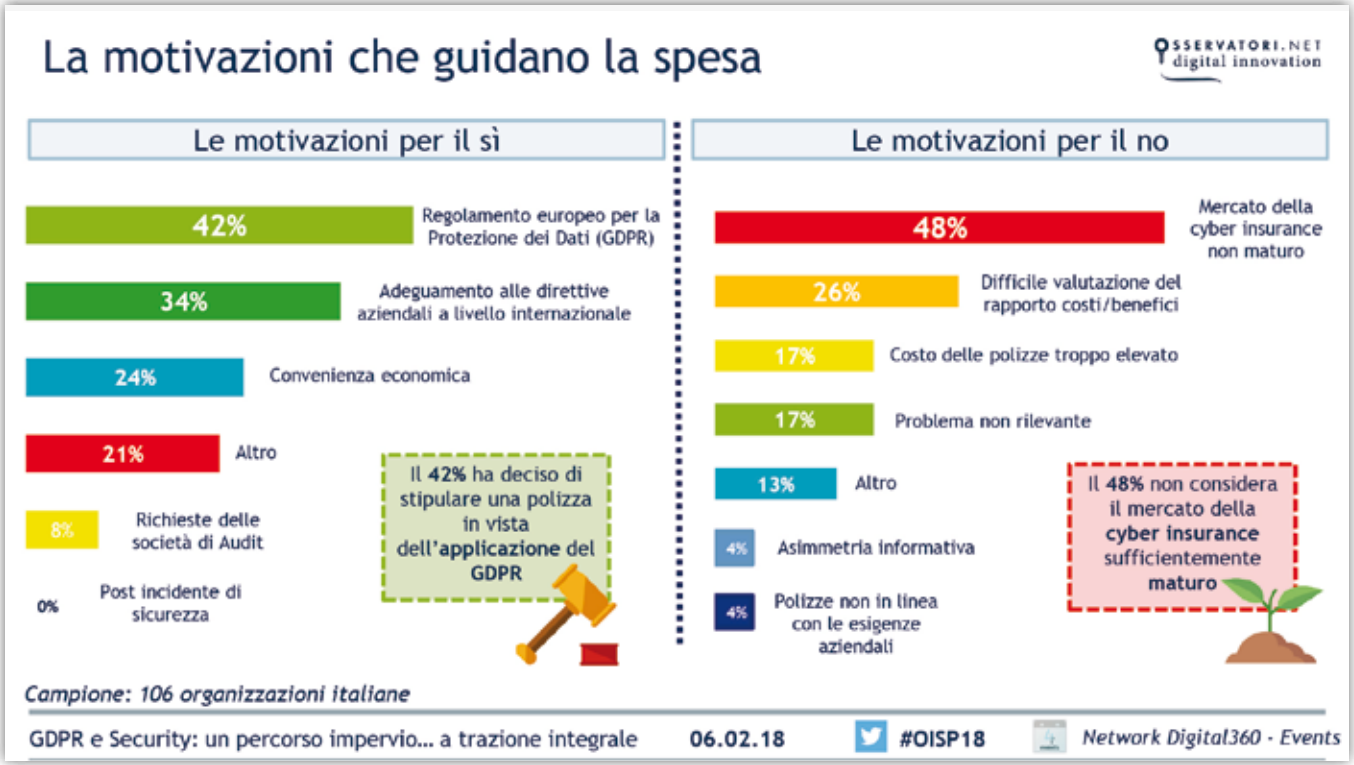
Campione: 106 organizzazioni italiane

GDPR e Security: un percorso impervio... a trazione integrale **06.02.18** **#OISP18** *Network Digital360 - Events*

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

I risultati completi della Ricerca sono consultabili su www.osservatori.net





I risultati completi della Ricerca sono consultabili su www.osservatori.net

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

Il campione: le PMI

OSSERVATORI.NET digital innovation

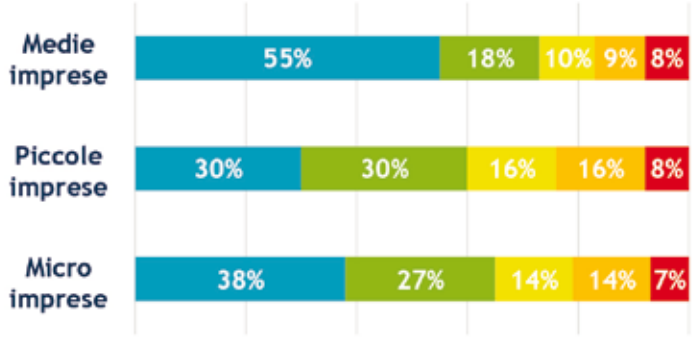
La scomposizione per settori

Campione: 947 piccole e medie imprese (addetti compresi tra 2 e 249)

GDPR e Security: un percorso impervio... a trazione integrale 06.02.18 #OISP18 Network Digital360 - Events

I trend tecnologici e l'impatto sulla Security

OSSERVATORI.NET digital innovation



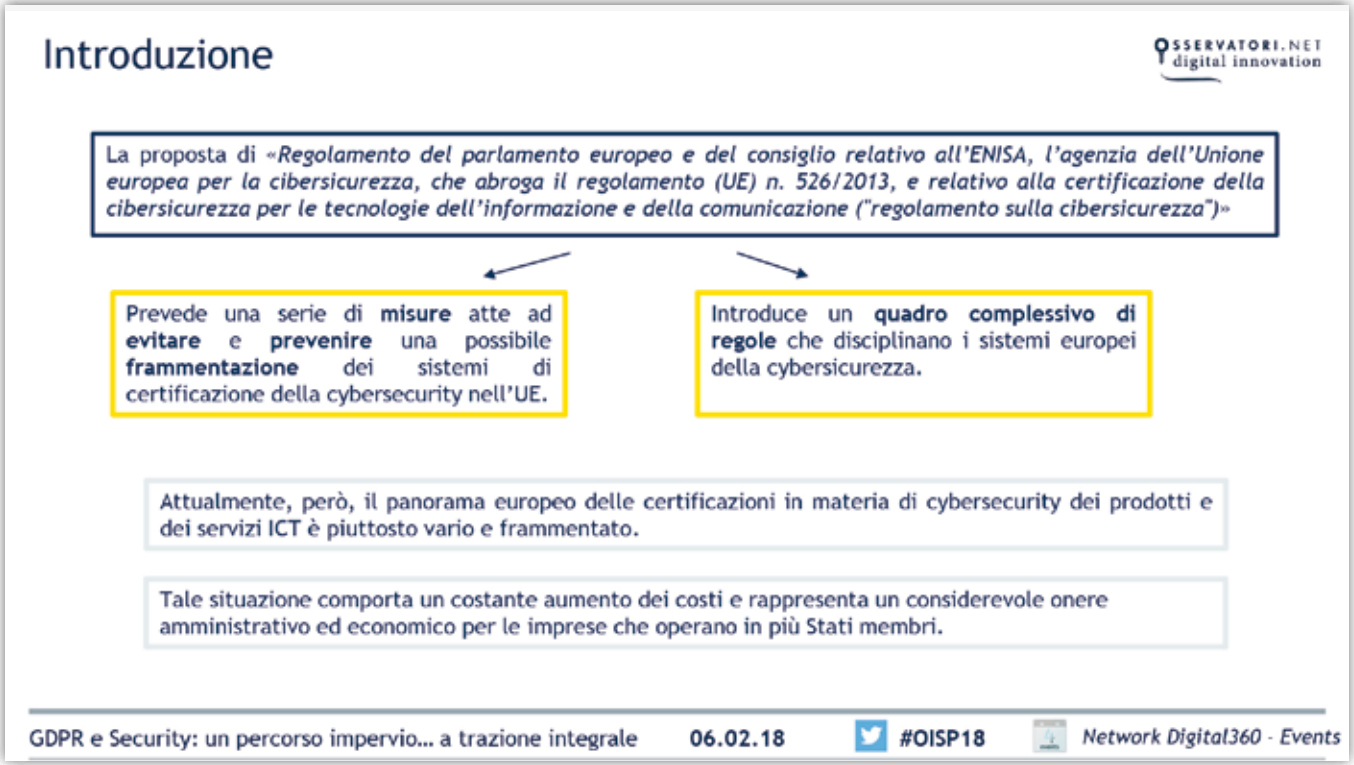
Principale trend che influenza le scelte di security:

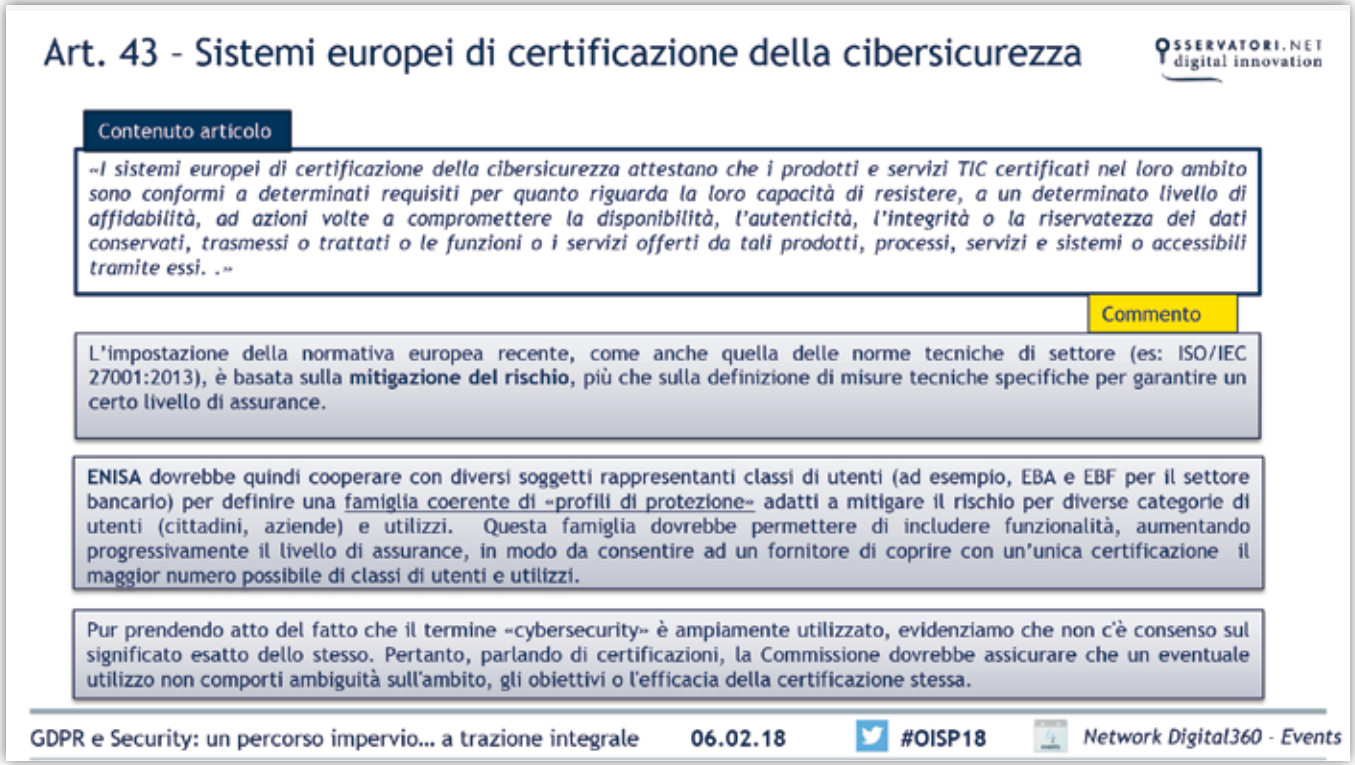
Cloud | Big Data | Social | Mobile | Internet of Things

Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

GDPR e Security: un percorso impervio... a trazione integrale 06.02.18 #OISP18 *Network Digital360 - Events*

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net





Art. 44 – Preparazione e adozione di un sistema europeo di certificazione della cibersicurezza

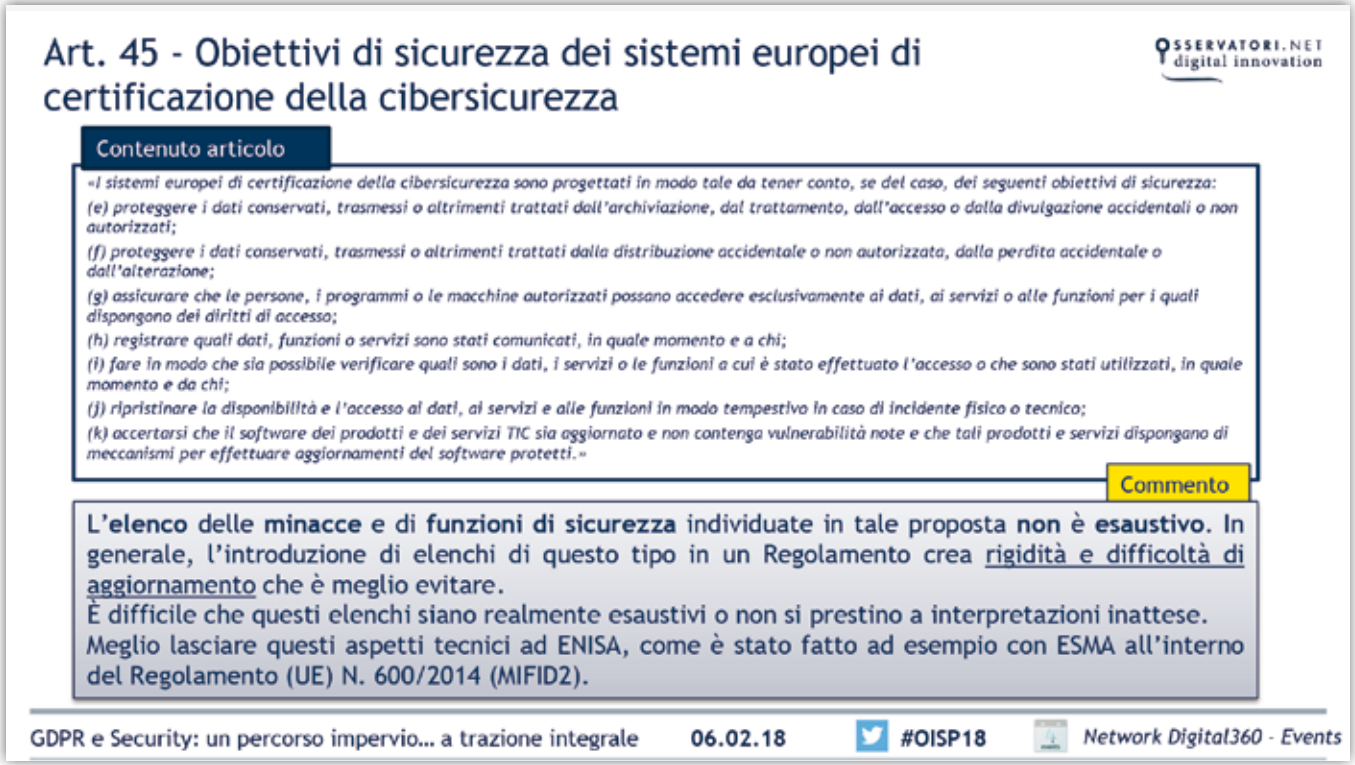
OSSERVATORI.NET digital innovation

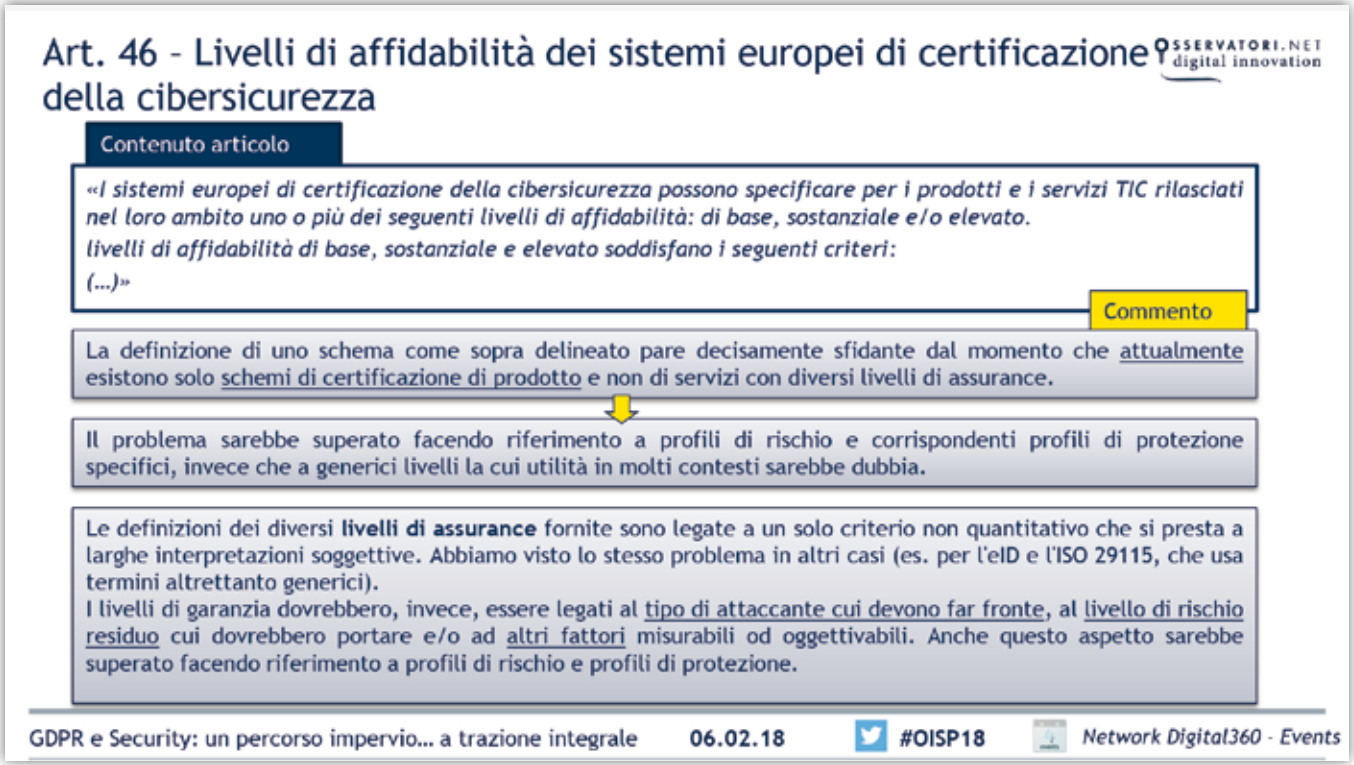
Contenuto articolo

«A seguito di una richiesta della Commissione, l'ENISA prepara un sistema europeo di certificazione della cibersicurezza che soddisfa i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento. Gli Stati membri o il gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza. (...)»

Commento

Risulta essere poco chiaro come **ENISA** possa preparare uno «schema» utilizzando le norme tecniche e le best practice esistenti; forse da questi si potrebbero ricavare quelli che per i **Common Criteria** sono dei «profili di protezione» da adottare per profili di rischio associati a diverse tipologie di utenti e utilizzi.





Art. 47 – Elementi dei sistemi europei di certificazione della cibersicurezza

OSSERVATORI.NET digital innovation

Contenuto articolo

«Un sistema europeo di certificazione della cibersicurezza comprende i seguenti elementi:

(o) l'oggetto e l'ambito di applicazione della certificazione, compresi il tipo o le categorie di prodotti e servizi TIC coperti;

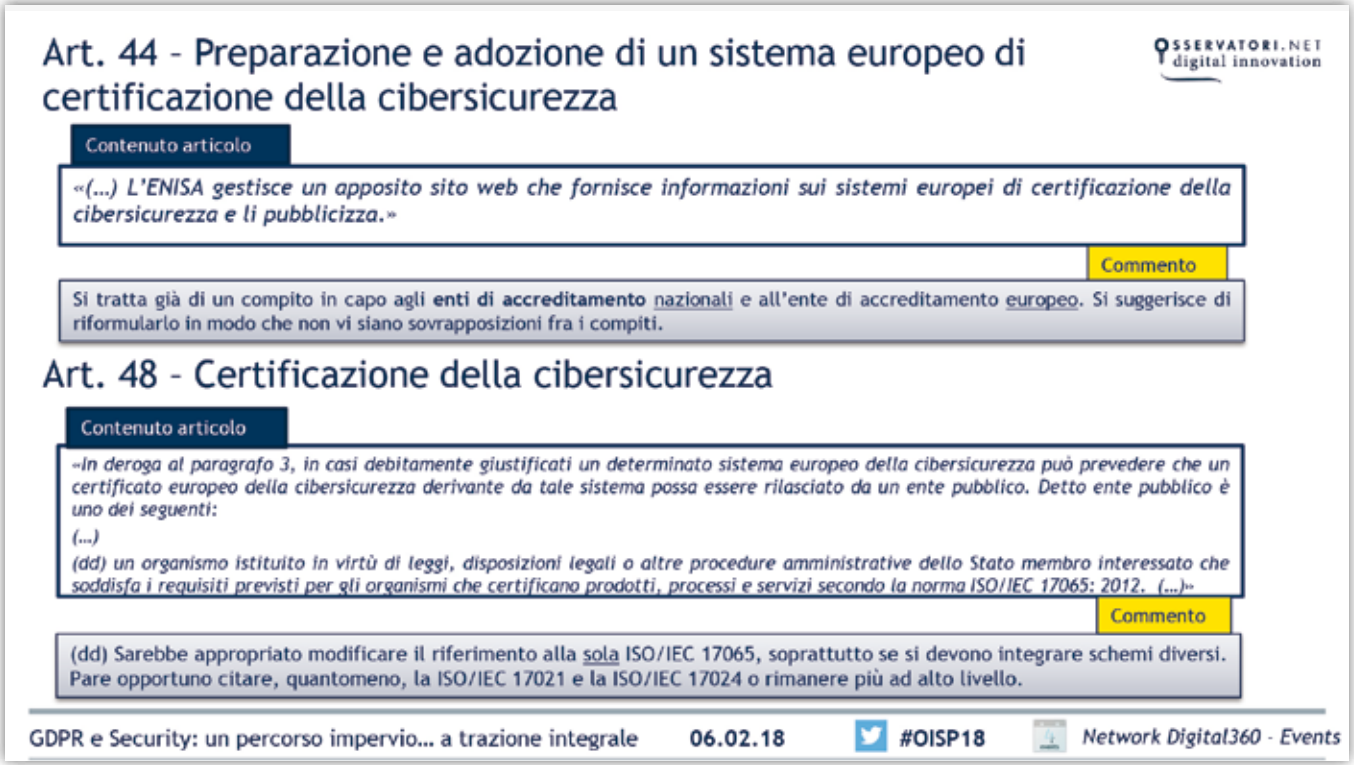
(...)»

La capacità di supportare le attività di «Identify, Protect, Detect, Respond and Recover» degli utenti del servizio o utilizzatori del prodotto (Framework for Improving Critical Infrastucture Cybersecurity - NIST, National Institute of Standards and Technology).

Commento

- (o) Poiché si parla di prodotti, è necessario contemplarne anche la versione.
- È opportuno includere nel perimetro di certificazione la capacità di integrarsi con i processi di gestione degli incidenti dei clienti, seppure con modalità diverse a seconda della tipologia di servizio o prodotto.

GDPR e Security: un percorso impervio... a trazione integrale 06.02.18 #OISP18 Network Digital360 - Events



Art. 49 – Sistemi nazionali di certificazione della cibersicurezza e certificati nazionali della cibersicurezza

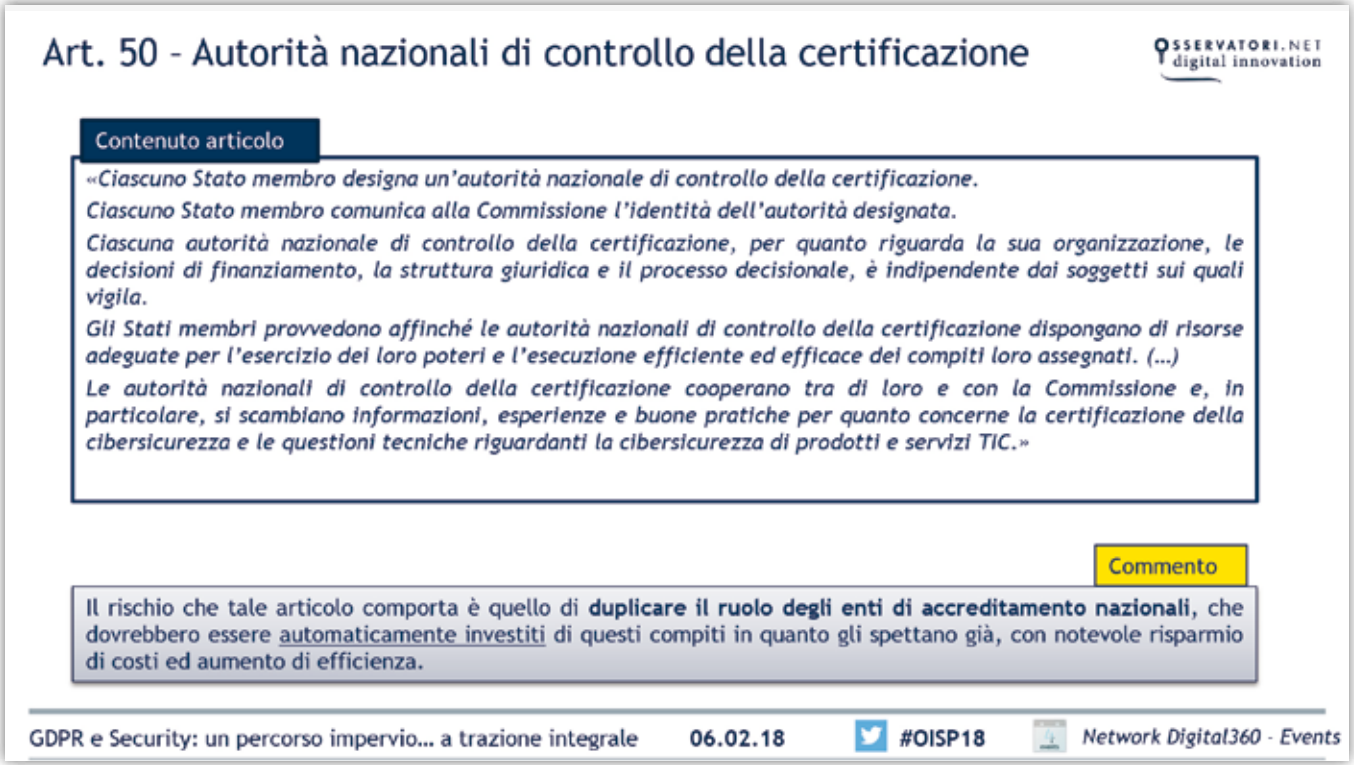
OSSERVATORI.NET digital innovation

Contenuto articolo

«Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.»

Commento

Sarebbe opportuno **rivedere** o **eliminare** l'articolo in quanto andrebbe a minare quanto disposto dalle certificazioni esistenti (v. ISO/IEC 27001) e per le organizzazioni certificate. Inoltre, prevarica le prerogative istituzionali degli enti nazionali di accreditamento.



Conclusioni

OSSERVATORI.NET digital innovation

In conclusione, il contenuto elaborato dai legislatori europei della proposta di Regolamento analizzata è da ritenersi, senza alcun dubbio, elogiabile.

Ma alla luce di quanto fin qui esposto, si reputa necessario apportare alcune modifiche al testo della proposta di Regolamento e, in particolare, in merito ai seguenti aspetti:

- adottare una **differente impostazione** fondata sulla mitigazione del rischio anziché sulla definizione di misure tecniche specifiche, per garantire un certo livello di *assurance*;
- definire dei **livelli di garanzia degli schemi di certificazione** non generici, ma che facciano riferimento a specifici profili di rischio e a relativi profili di protezione;
- sotto il **profilo sanzionatorio**, sarebbe opportuno chiarire «cosa e chi» debba essere sanzionato, prevedendo almeno che le stesse siano rivolte ai soggetti certificatori;
- prevedere che **ENISA** possa effettuare un'**attività di audit** sui prodotti e i servizi certificati a cui anche i soggetti per i quali è stato pensato il profilo di autorizzazione possano partecipare.

GDPR e Security: un percorso impervio... a trazione integrale **06.02.18** **#OISP18** *Network Digital360 - Events*

I risultati completi della Ricerca sono consultabili su www.osservatori.net

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

GDPR e Security: un percorso impervio… a trazione integrale

Approfondimenti

Febbraio 2018

Studi di caso

Sul sito www.osservatori.net, saranno scaricabili in formato elettronico tutti i casi di studio oggetto di approfondimento della Ricerca 2017.

Di seguito si riportano i casi aziendali presenti nelle pagine successive del Report:

- BAYER
- CARREFOUR
- DUCATI MOTOR HOLDING
- EDISON
- EUROPCAR
- GRUPPO BOSCH ITALIA
- GRUPPO ITAS ASSICURAZIONI
- IKEA
- SNAM

BAYER

Bayer è un'azienda globale, con sede a Leverkusen (Germania), che ha competenze chiave nei settori delle Life Sciences, Salute e Agricoltura.
In Italia conta 3 siti produttivi con impianti fra i più avanzati al mondo, circa 2.100 collaboratori e un fatturato 2016 di 1.046 milioni di Euro.
Bayer in Italia attualmente è costituita da società che consentono al Gruppo di essere presente e operare in diversi ambiti strategici e di primaria importanza: da Pharmaceuticals a Consumer Health, a Crop Science ed Animal Health.

All'interno dell'Information Technology è presente la funzione Information Security, guidata dall'Information Security Officer. Le linee guida su cui si focalizza la funzione IT Security vengono definite dalla casa madre, che le sviluppa basandosi sulle esigenze di business, trend di mercato e potenziali rischi.
Tra le principali progettualità condotte recentemente dall'Information Security rientrano le iniziative di Information Classification e Awareness Campaign.
Il progetto di Information Classification è stato portato avanti con l'obiettivo di identificare le informazioni sensibili trattate in ognuna delle aree di business aziendali, analizzarne il rischio potenziale e pianificare l'implementazione di adeguate misure di sicurezza, al fine di garantire una gestione sostenibile delle informazioni stesse.
L'attività, messa in opera da un team di progetto di 15 diversi gruppi con esperti IT e di business, ha portato all'identificazione di diversi cluster di informazioni suddivisi in 3 tipologie, ognuno con caratteristiche ben definite, e alla definizione di una roadmap di misure di protezione comportamentali, organizzative e tecniche. All'interno di ogni funzione aziendale coinvolta è stata individuata una figura a cui è stata assegnata la responsabilità di garantire la sostenibilità del processo di Information Classification.

Rispetto al piano Awareness Campaign, nel corso degli anni sono state svolte diverse iniziative con l'obiettivo di sensibilizzare gli utenti e creare consapevolezza sul tema della sicurezza e della protezione dei dati a tutti i livelli aziendali.
Nel 2015 è stato realizzato l'Information Security Awareness Workshop, preceduto dalla distribuzione di flyer informativi sui "Sette principi chiave della sicurezza", raccomandazioni che invitano i dipendenti ad adottare comportamenti responsabili nelle proprie azioni quotidiane, dalla gestione prudente delle informazioni e dei dispositivi aziendali alla protezione della propria identità digitale.
L'attività, svolta con l'obiettivo di trasmettere i principi generali sulla sicurezza, ha seguito un approccio top-down: la formazione è stata inizialmente somministrata ai manager, dapprima ingaggiati come partecipanti ai corsi, che hanno poi assunto il ruolo di moderatori all'interno dei workshop con il proprio team di riferimento, e così via per i progressivi livelli gerarchici. Questo approccio ha permesso di sottolineare come ogni team e ogni singola persona all'interno di essi abbia un ruolo fondamentale nel garantire la sicurezza delle informazioni.

È stata successivamente promossa una Campagna AntiPhishing, che ha previsto, previo annuncio, la simulazione di un attacco rivolto agli utenti. Il finto attacco è avvenuto tramite una mail customizzata, con richiamo al flyer informativo divulgato già in fase di annuncio della campagna, contenente una checklist di elementi utili per individuare e-mail di phishing e la procedura corretta da seguire per gestire comunicazioni sospette. A questo proposito è stato implementato il servizio "CheckMail", che permette ai dipendenti di segnalare in automatico e-mail di dubbia provenienza perché possano essere esaminate e verificate.

Un'ulteriore iniziativa facente parte del piano Awareness Campaign è il Cyber Security Day, una sessione a partecipazione libera organizzata per la prima volta a marzo 2017. Durante l'evento sono stati toccati argomenti relativi a Phishing e Social Engineering, ma anche tematiche di attualità che hanno

▸

Le riprese dell'evento sono disponibili in video on demand su www.osservatori.net

messo in relazione sicurezza aziendale e protezione dei dati personali nella vita quotidiana, quali per esempio cyberbullismo, legalità digitale, utilizzo consapevole di Internet e dei social network. I vari interventi che si sono susseguiti hanno visto la partecipazione di esperti esterni all'organizzazione e di figure aziendali di riferimento sul tema della sicurezza, sia a livello di Corporate Security sia di Information Security, che hanno raccontato alcuni casi concreti di tentativi di attacco informatico subiti dall'organizzazione.

Le attività di sensibilizzazione vengono portate avanti con logica continuativa e pluriennale, poiché sono considerate da Bayer un fattore fondamentale per assicurare la corretta protezione dei dati: oltre all'adozione di difese tecnologiche, alla pubblicazione di regolamenti, alla definizione di processi, l'azienda ritiene infatti che non sia possibile raggiungere un adeguato livello di sicurezza senza considerare anche l'elemento umano. Lo scopo delle iniziative è quello di educare i dipendenti, affinché ogni singolo collaboratore abbia un comportamento sicuro sia in azienda sia nella vita quotidiana, dando ad ognuno la responsabilità di salvaguardare il successo dell'organizzazione.

CARREFOUR

Carrefour è una delle maggiori catene della grande distribuzione a livello mondiale. Fondata nel 1958, è presente in Europa, America, Asia e Africa, per un totale di circa 30 Paesi. La casa madre si trova in Francia, nei pressi di Parigi. Il Gruppo è presente in Italia con 1.073 punti vendita dislocati in 18 regioni e oltre 20.000 collaboratori. Nel 2015 Carrefour Italia ha ottenuto un fatturato di circa 5 miliardi di Euro.

In tema di cyber security, le strutture dei singoli Paesi sono misurate rispetto a una serie di indicatori,

stabiliti dalla casa madre principalmente in base allo standard ISO/IEC 27001, che hanno la funzione di valutare il livello di performance e il raggiungimento degli obiettivi anno per anno. Tali indicatori costituiscono intrinsecamente una linea guida, in quanto indirizzano le attività delle varie unità operative nazionali, sebbene non sia formalmente imposto il loro rispetto.

Anche l'Italia ha nominato formalmente un Chief Information Security Officer (CISO) al quale sono state attribuite le responsabilità di indirizzo e definizione dei temi di cyber security, di analisi e valutazione del cyber risk, di definizione dei piani di awareness e, non meno importante, la definizione del corpo documentale della sicurezza. Il CISO è collocato nella Direzione Sistemi Informativi che riporta alla Divisione Amministrazione, Finanza e Controllo. Gli aspetti di sicurezza fisica sono invece gestiti da una direzione diversa a riporto del CEO (Direzione Risk & Compliance).

Carrefour Italia è attiva sul tema del fattore umano, poiché ritiene che sia necessario non solo dotarsi di sistemi tecnologici avanzati, ma anche introdurre iniziative volte ad educare, sensibilizzare e rendere consapevoli i propri dipendenti rispetto ai temi di cyber security, con un focus particolare sulle possibili minacce informatiche. Per questo motivo l'azienda ha intrapreso, a partire dal 2010, un programma pluriennale di formazione in materia di cyber security, optando per un modello "a chiocciola", concentrandosi inizialmente sulla Direzione Sistemi Informativi per poi estendere progressivamente le attività formative, opportunamente adattate, alle altre funzioni e alle altre sedi.

Il training, svolto sia in aula che online e supportato da comunicazioni periodiche effettuate via e-mail o sfruttando il periodico interno, viene annualmente rilanciato ed arricchito.
Il programma rivolto alla Direzione Sistemi Informativi prende il nome di "Security Week": le varie attività formative vengono concentrare nell'arco di una settimana, interamente dedicata al tema della protezione delle informazioni.

La Security Week viene organizzata come un convegno a sessioni parallele in cui ogni persona si può costruire il proprio percorso formativo. La settimana inizia con una sessione introduttiva di inquadramento del problema e termina con una seduta finale in cui si raccolgono le impressioni ed i commenti di tutti i partecipanti. Quest'anno è stato aggiunto un ulteriore elemento che riguarda la valutazione dell'efficacia della formazione: a tutti i partecipanti viene proposto un questionario online a risposta chiusa per la valutazione delle competenze prima della formazione; lo stesso questionario viene quindi riproposto dopo la fine della Security Week. L'incremento del numero di risposte esatte dirà in modo concreto ed immediato quanto l'attività formativa sia stata utile.

A completamento e supporto della formazione precedente, Carrefour Italia effettua periodicamente dei test sui dipendenti, con lo scopo sia di valutare la capacità di reazione a possibili minacce, sia di creare un'ulteriore forma di apprendimento. Per garantire la credibilità e l'efficacia di tali iniziative vengono utilizzate tecniche di social engineering e attività di assessment di volta in volta diversificate: sono state ad esempio effettuate simulazioni di attacchi di phishing, tramite l'invio ai dipendenti di e-mail contenenti link sospetti, oppure sono stati realizzati finti attacchi con la tecnica del baiting, avvenuti disseminando alcune chiavette USB incustodite in zone frequentate dagli utenti dell'organizzazione.

Le attività di sensibilizzazione vengono proposte anche al Top Management, tramite l'elaborazione di percorsi formativi specifici per Direzione. Carrefour Italia è infatti consapevole che la necessità di creare attenzione rispetto ai temi della cyber security deve coinvolgere tutti i livelli dell'organizzazione e che l'esempio del management aziendale è di fondamentale importanza per creare comportamenti virtuosi in azienda.

DUCATI MOTOR HOLDING

La Ducati Motor Holding S.p.A. è una casa motociclistica italiana con sede nel quartiere Borgo Panigale a Bologna. Nel 2012 l'azienda è stata acquisita da AUDI AG ed è entrata quindi a far parte del Gruppo Volkswagen. Ducati distribuisce i propri prodotti in più di 90 Paesi e nel 2016 ha venduto 55.451 moto fatturando 731 milioni di euro.
L'offerta di Ducati non si focalizza soltanto sul prodotto: l'azienda punta infatti a fornire un'esperienza, che sia allo stesso tempo emozionante, performante e sicura, in una costante volontà di innovazione.
Oltre alla produzione di motoveicoli, Ducati si dedica al mondo delle competizioni attraverso il Reparto Corse, partecipando a numerosi campionati, quali Superbike e MotoGP.

All'interno del Gruppo Volkswagen i temi della sicurezza e della protezione delle informazioni sono trattati con estrema attenzione: la struttura del Gruppo, un network di imprese distribuito e costituito da diversi nodi, aumenta le vulnerabilità da affrontare, ampliando la superficie d'attacco potenziale e i punti di ingresso per un eventuale aggressore.
Ducati stessa viene inoltre sottoposta ad una costante copertura mediatica, che genera grandi opportunità ma allo stesso tempo ha come conseguenza una forte esposizione a minacce di sicurezza.

L'azienda è molto sensibile agli stimoli, in termini di regole di sicurezza, provenienti dalla Capogruppo, che coniuga con il rispetto delle normative nazionali e internazionali (regolamenti e direttive europee tra le quali il GDPR) e ponendo attenzione alle specifiche esigenze dell'organizzazione.

Per garantire la massima sicurezza possibile assicurando allo stesso tempo un alto livello di sensibilità alleesigenze del Business, è stato creato un **ISMS (Information Security Management System)**, che

si avvale di due componenti fondamentali: una di metodo, processo, governance, che va dalla definizione dei ruoli alla scrittura delle procedure, e una tecnologica, che mira a ricercare continuamente le tecnologie migliori in relazione al budget disponibile. Il framework creato ha l'obiettivo di proteggere i dati strategici dell'azienda, minimizzare i rischi e garantire la business continuity qualora si verifichino data breach o situazioni di crisi in generale.

Il tema della sicurezza informatica in azienda è gestito da un CISO, collocato all'interno della funzione IT, che riporta al CIO. Il CISO si avvale sia di competenze di specialisti interni, soprattutto per la gestione dell'area Networking e della sicurezza perimetrale (VPN, Firewall, ecc.), sia di competenze reperite esternamente: l'azienda si rivolge sia per la parte tecnologica, sia per la parte normativa, contrattuale e organizzativa, ad alcuni partner, tra i quali, in particolare, è preziosa la collaborazione con Sinergy.

Il tema della sicurezza informatica non interessa soltanto la funzione IT, ma è pervasivo a livello aziendale: Ducati ritiene fondamentale l'aspetto legato alla gestione del fattore umano e ha quindi previsto numerose iniziative di sensibilizzazione del personale, tra cui corsi interni, programmi di comunicazione e "pillole" informative via mail, con l'obiettivo di coinvolgere l'intera popolazione dell'organizzazione. È in fase di progettazione un'iniziativa che prende il nome di "Digital Fridays": si tratterebbe di un appuntamento mensile serale, in logica informale, con il coinvolgimento di alcuni speaker di rilievo volto alla creazione di awareness sui temi del digitale.

Ducati è un'azienda dinamica e attenta all'innovazione e, di conseguenza, pone molta cura al tema della gestione del cambiamento. Grande importanza è dunque data alla disciplina del **Change Management**, che punta ad assicurare un opportuno bilanciamento tra la necessità di cambiamento e la gestione degli effetti generati, in termini di rischi, impatti economici, di processo, di sicurezza, tramite la definizione di ruoli e responsabilità e il coinvolgimento del Business.

Dalla collaborazione con Sinergy è nato anche un framework di analisi dei workflow sui diversi processi per la gestione dei privilegi (**Privileged User Management**), con l'obiettivo di tracciare e controllare gli accessi che possono essere concessi agli utenti, specialmente qualora si tratti di amministratori di sistema o di rete. Ad ogni utente aziendale devono essere messi a disposizione esattamente i dati e i processi necessari per lavorare, al fine di prevenire eventuali violazioni dei dati strategici o comunque confidenziali o accesso a informazioni per le quali non si dispone l'autorizzazione.
In tale contesto si colloca anche la valutazione della conformità in termini di **Segregation of Duties**, con l'obiettivo di impedire la commissione di frodi ed errori attraverso l'analisi automatica dei profili.

Ducati effettua periodicamente controlli automatici su una serie di vulnerabilità (**Vulnerability Management**), oltre a controlli esterni tramite penetration test più approfonditi atti a verificare lo stato di sicurezza di un determinato sistema o di una rete.
Il tema della gestione delle vulnerabilità riguarda anche i prodotti finali. L'azienda si sta infatti muovendo per la creazione di una moto connessa, con interazioni anche al di fuori dalla vettura in un ecosistema di oggetti IoT. Nell'affrontare questo progetto, Ducati sta valutando non solo il coinvolgimento di attori primari del settore dell'automotive, ma anche quello di soggetti più vicini al mondo hacker, che aiutino l'azienda nella scoperta di vulnerabilità nascoste.

EDISON

Edison S.p.A. è un'azienda italiana attiva nei settori dell'approvvigionamento, produzione e vendita di energia elettrica, gas e olio grezzo con oltre un milione di clienti. È la più antica società europea nel settore dell'energia e oggi opera, attraverso i suoi oltre 3.000 dipendenti, in più di 10 Paesi nel mondo, con una potenza installata di 6,5 GW. Il Gruppo è composto da 74 aziende, 14 delle quali sono loca-

lizzate fuori dall'Italia: le società estere sono prevalentemente petrolifere e dedite alla produzione di gas naturale.
L'azienda ha ottenuto nel 2016 un fatturato di oltre 11 miliardi di Euro.

La funzione di Information Security dell'azienda ha portato avanti negli ultimi anni diversi progetti sul tema del "fattore umano", volti a sensibilizzare il personale sui rischi e sulle minacce informatiche. In particolare, Edison ha sviluppato tre tipologie di iniziative:

- Hacker lunch: in primo luogo sono stati organizzati degli incontri informali, aventi ad oggetto i comportamenti da tenere al fine di evitare incidenti di sicurezza. In sede di programmazione si è deciso di trattare non solo tematiche attinenti alle policy e alle procedure lavorative, ma anche relative alle consuetudini nei comportamenti degli utenti nella vita quotidiana, come per esempio l'utilizzo consapevole degli smartphone e la gestione delle password.
- Nel corso del 2016 la formazione è stata impartita attraverso una decina di sessioni. Una serie di queste è stata organizzata in forma di hacker lunch, tramite il coinvolgimento di un giornalista esperto di informatica che, attraverso "provocazioni" e filmati incentrati ad esempio sui furti di identità, ha tentato di stimolare i dipendenti anche da un punto di vista emotivo, al fine di far loro comprendere l'importanza della cyber security nella vita di tutti i giorni. Tali incontri, sebbene limitati alla sola sede principale dell'azienda, che ospita circa il 60% del personale, hanno registrato una buona partecipazione.
- In secondo luogo, allo scopo di raggiungere l'intera popolazione aziendale, Edison ha puntato sul tradizionale corso di e-learning. Nel 2016 il corso, sviluppato in logica tradizionale, si è focalizzato sull'importanza di gestire in maniera ottimale le password e sulle modalità di segnalazione di incidenti informatici e di riconoscimento delle e-mail di phishing.
- A partire dal 2017, invece, per aumentare il livello di engagement dei dipendenti, l'azienda ha fatto ricorso ad una logica di gamification, impostando la formazione su un corso on-line imperniato su una

serie di nozioni a difficoltà crescenti (ad esempio come riconoscere i virus e quali sono le azioni da compiere per rimuoverli), con l'obiettivo di verificare l'effettivo apprendimento dei concetti trasmessi e poter incrementare così il livello di gioco sino a potersi cimentare con il livello Hacker Professional.
- Infine, sempre nel 2016, la società ha distribuito un libro sulla sicurezza, sviluppato da un esperto esterno all'azienda con il coinvolgimento di CISO di alcune società fra cui Edison, che è stato successivamente consegnato a circa 600 dipendenti.

Le iniziative sono state proposte dalla funzione Security, in collaborazione con la funzione Human Resources. Le attività hanno poi coinvolto anche la Comunicazione, che si è occupata degli aspetti relativi all'organizzazione degli eventi, dello sviluppo delle locandine, dell'invio delle e-mail e dell'aggiornamento della Intranet aziendale.

Per verificare l'efficacia delle iniziative messe in atto e l'effettivo livello di apprendimento dei dipendenti, sono stati successivamente effettuati dei test. Per quanto riguarda il corso di e-learning basato sul modello "gamification", ad esempio, sono stati previsti degli appositi momenti di verifica, in cui sono stati accuratamente analizzati i punteggi ottenuti dagli utenti durante lo svolgimento dei giochi online.

L'identificazione e la definizione delle azioni in tema di sicurezza si basa sulla revisione annuale dei rischi. Edison ha sviluppato negli anni un apposito strumento, un framework di valutazione dei rischi strutturato in riferimento ai dati della lista dei controlli della ISO27001, da cui è emerso in particolare che il rischio connesso al fattore umano era sopra la soglia consentita, suggerendo la necessità di un intervento in tal senso.
Dall'assessment sui rischi scaturiscono anche le scelte relative alle soluzioni tecnologiche da implementare: la società ha recentemente adottato una nuova piattaforma anti APT e anti malware, poiché nel processo di analisi del rischio era stata riscontrata l'esistenza di un problema in tale ambito.

EUROPCAR

Nata in Francia oltre 65 anni fa, Europcar è leader europeo nel noleggio di autoveicoli, oltre che uno dei principali attori nel mercato della mobilità. Il Gruppo Europcar, attivo in oltre 140 Paesi con i marchi Europcar ed InterRent, offre ai suoi clienti uno dei più grandi network di autonoleggio del mondo tramite società interamente controllate, nonché franchising e partner. Oltre all'attività core del noleggio di auto, furgoni e scooter, il Gruppo Europcar ha ampliato negli ultimi anni la propria gamma di soluzioni in risposta alla crescente domanda del mercato, abbracciando la sfida di proporre nuovi modelli di mobilità a 360°.

Europcar, che vanta numerosi premi "World Travel Awards" relativi all'offerta di mobilità ed alla soddisfazione del cliente, consta di 6000 dipendenti e nel 2016 ha fatturato 2,151 miliardi di Euro.

Da un punto di vista organizzativo, la società operante sul territorio nazionale Europcar Italia S.p.A., è soggetta alla direzione ed al coordinamento di Europcar Groupe S.A., situata a Parigi. I progetti legati alla sicurezza delle informazioni, in termini sia di adeguamenti tecnologici sia di compliance dei processi verso gli standard di settore, vengono pianificati e coordinati direttamente dalla casa madre in Francia e messi in atto dalle singole Country.

Sin dalla pubblicazione del General Data Protection Regulation ed in vista della sua prossima entrata in vigore, Europcar si è immediatamente attivata per strutturare il processo di adeguamento alla normativa in materia di tutela dei dati personali. Il percorso è iniziato conducendo una gap analysis e proseguirà con una serie di investimenti strategici, con l'obiettivo di presentarsi sul mercato nel 2018 come azienda non solo in grado di assicurare un'adeguata protezione ai numerosi dati dei propri clienti, ma anche perfettamente rispondente ai requisiti imposti dalla nuova normativa.

Il GDPR è un tema che diventa particolarmente complesso in contesti multinazionali: è un dato di fatto che ogni Stato membro dell'Unione europea, infatti, risponde in maniera differente a determinati stimoli legali, in particolare per quanto riguarda la protezione dei dati. L'Italia, così come la

Germania ad esempio, è più propensa a reagire al nuovo Regolamento europeo in modo efficace, sia in termini di tempi che di modalità, a differenza di altri Paesi la cui normativa interna in questo campo non ha la stessa maturità e sensibilità di quella italiana. In una multinazionale, dunque, la sfida è attivarsi in modo armonico così da garantire un approccio comune, sincrono e virtuoso al fine di raggiungere il comune obiettivo dell'aderenza ai nuovi requisiti previsti dal GDPR.
Volgendo lo sguardo ad uno dei principali compiti che le aziende facenti parte di un gruppo devono affrontare per l'entrata in vigore della nuova normativa, ovvero quello di definire il perimetro di responsabilità rispetto al trattamento dei dati, troveremo ben poche organizzazioni pronte; infatti tali responsabilità non sempre sono già chiaramente definite negli atti societari. Esistono diversi problemi pratici sui quali si dovrà lavorare per capire dove inizia e dove finisce la propria responsabilità ed uno di questi è quello di tipo tecnologico: Europcar Italia, infatti, utilizza da un lato applicativi locali per far fronte a esigenze tipiche del mercato italiano, ma allo stesso tempo fa riferimento a diversi mezzi e strumenti centralizzati la cui responsabilità è in seno alla Holding. Un esempio riguarda il sito Internet, in parte gestito centralmente da Europcar International e in parte, per quanto riguarda il content management e la gestione del database per l'invio delle newsletter, in Italia.

Una ulteriore criticità introdotta dal GDPR riguarda l'applicazione del meccanismo dello "sportello unico". Infatti, secondo quanto previsto dalla normativa, qualora un'organizzazione vantasse più stabilimenti all'interno dell'Unione europea, potrà avere un'unica Autorità sovrintendente riconosciuta come "Autorità principale" (o capofila), sulla base dell'ubicazione del proprio "stabilimento principale" (ossia il luogo dove avvengono le più significative attività di trattamento). L'Autorità principale agirà quale "sportello unico" per supervisionare tutte le attività di gestione dei dati personali effettuate dall'azienda a livello complessivo che abbiano carattere transfrontaliero. Essendo Europcar una multinazionale con casa madre situata a Parigi, se si adottasse tale meccanismo, l'Authority di riferimento (in merito alla maggior parte dei trattamenti posti in essere) sarebbe quella francese. Paradossalmente, anche se "la

soluzione" dello "sportello unico" nasce con l'obiettivo di semplificare i processi per le aziende presenti in più Paesi, di fatto potrebbe risultare addirittura più gravoso: esso, infatti, non esclude che per i casi regolati specificatamente dalla normativa locale (come ad esempio i diversi Provvedimenti del Garante che non decadranno in forza del GDPR) o aventi stretta connotazione territoriale (come reclami o violazioni) ci si dovrà sempre confrontare con l'Autorità di Controllo nazionale, dovendo quindi sostenere i processi per mantenere sempre aperti i due "canali", quello locale e quello internazionale.

Un ulteriore punto di attenzione è relativo all'applicazione del principio della "Data Protection by Default", un approccio che richiede l'attuazione di misure tecniche ed organizzative adeguate al fine di proteggere efficacemente i dati. Tali misure, come ad esempio la crittografia, dovranno essere predisposte in modo nativo su tutti i servizi, ridisegnandoli ed effettuando un periodico censimento dei dati personali; dovranno inoltre definire i tempi di conservazione dei dati stessi ed attivare apposite procedure che permettano, in automatico, di cancellarli quando non sono più necessari.

Infine, in Europcar, particolare attenzione è dedicata al processo di sensibilizzazione del fattore umano per prevenire, quanto più possibile, i rischi. Per questo, sempre in vista dell'entrata in vigore del GDPR, sono in programma due principali tipologie di formazione: la prima prevede la realizzazione di corsi dedicati, nello specifico, a temi connessi alla privacy, in modo da rendere edotti i dipendenti sulla nuova normativa europea; la seconda mette a fuoco aspetti di tipo tecnico e, cioè, i diversi pericoli nei quali i dipendenti possono incorrere durante lo svolgimento della normale mansione lavorativa (tentavi di phishing, diffusione di malware e ransomware).

Europcar Italia si sta impegnando molto per far sì che la formazione raggiunga ogni dipendente all'interno dell'organizzazione: le attività sono indirizzate a tutto il personale aziendale dal top management ai dipendenti dei tanti uffici di noleggio disseminati sul territorio.

GRUPPO BOSCH ITALIA

La Robert Bosch GmbH nasce nel 1886 a Stoccarda come "Officina di meccanica di precisione ed elettrotecnica". Attualmente Bosch è una delle più grandi aziende tedesche, con un fatturato pari a circa 73 miliardi di Euro nel 2016, ed è presente in oltre 150 paesi nel mondo.
In Italia e Grecia conta una ventina di entità legali, tra sedi commerciali, sedi produttive (power tools, diesel, pneumatica/idraulica, attrezzatura d'officina) ed entità di ricerca e sviluppo, per un totale di circa 6000 collaboratori.
Il Board di Bosch è particolarmente attento e sensibile alle implicazioni del General Data Protection Regulation (GDPR), che prevede sanzioni consistenti – fino al 4% del fatturato globale annuo – in caso di mancato adempimento.
Nell'ambito Sicurezza Dati e Informazioni, l'organizzazione prevede, a livello di Regione, un Data Security Officer (DSO), coadiuvato da circa 30 collaboratori nelle varie sedi, chiamati Professional Data Security Partners (DSP). I DSP sono coloro che hanno direttamente a che fare con i vari collaboratori sul territorio e si occupano di sensibilizzazione, formazione e raccolta informazioni. Il DSO riporta direttamente al Board della Regione e di conseguenza la funzione Sicurezza Dati e Informazioni è indipendente da IT, Finance o Legal.
Dal momento della pubblicazione del GDPR, la funzione Sicurezza Dati e Informazioni si è immediatamente attivata per definire un percorso di adempimento.
Il primo passo effettuato è stato chiedersi quanto la situazione dell'azienda fosse "lontana" dai requisiti imposti dal nuovo Regolamento. Il documento è stato analizzato nel dettaglio per arrivare alla stesura di una lista puntuale delle richieste del GDPR (informative, notifiche, registro dei trattamenti, implementazione TOMs (Technical and Organisational Measures), analisi dei rischi, Data Protection Impact Assessment, misure IT, ecc.) composta da 70 punti.

A seguito della redazione della lista, si è passati all'individuazione delle persone coinvolte. Sono state definite 4 categorie di riferimento: società di consulenza informatica, supporto informatico interno all'azienda, supporto legale esterno e collaboratori interni. Questi ultimi sono stati individuati sia tra i Professional Data Security Partners, sia tra i collaboratori responsabili di vari enti commerciali, di servizi e di produzione.

Successivamente, l'azienda si è dedicata alla valutazione dell'impegno connesso ad ognuna delle attività richieste dal GDPR in termini di tempistiche, per ogni categoria di persone coinvolte, seguita da un censimento sul territorio di tutti i trattamenti dei dati personali, che ha portato all'individuazione di circa 200 trattamenti (es. trattamento dati previdenziali dei collaboratori; trattamento dati per incidenti sul lavoro; trattamento dati salariali, ecc.).
Per rendersi effettivamente conto del gap esistente e misurare l'impatto e l'impegno che il percorso di adeguamento avrebbe richiesto all'azienda, la lista di attività da svolgere è stata dapprima applicata su 30 trattamenti. Ciò ha permesso di stimare i tempi medi di implementazione, poi applicati a tutti i 200 trattamenti, per ottenere una valutazione dell'impegno totale delle risorse coinvolte, sia interne che esterne.
Questo impegno è stato poi tradotto in costi, per definire l'ammontare del budget necessario all'adeguamento per tutte le entità legali italiane e greche. Al costo per lo svolgimento delle attività per le 4 categorie di responsabilità è stato aggiunto il costo della formazione, ottenendo una stima complessiva che è stata poi suddivisa sui 2 anni di riferimento, 2017 e 2018.
Il budget calcolato ammonta in totale a circa 2 milioni di Euro, ovvero in media intorno a 10.000 Euro per ognuno dei trattamenti identificati.

Il percorso di formazione delle risorse all'interno dell'organizzazione è un passaggio fondamentale nella roadmap di adeguamento al GDPR. Bosch ha ritenuto indispensabile la formazione di tutti i

Responsabili di ente e dei capi ufficio e, per alcune funzioni (come per esempio l'HR), di tutti i collaboratori per sensibilizzare a tutti i livelli l'organizzazione.
Per assicurare che la formazione fosse adeguata al target dei diversi soggetti, sono state definite 4 aree tematiche:

- Trattamento dati dei collaboratori
- Trattamento dati personali con applicazioni IT
- Trattamento dati di clienti/fornitori
- Trattamento dati personali tramite prodotti

In Italia attualmente non vengono realizzati prodotti che raccolgono dati personali, a differenza di quanto avviene in altre nazioni. Questa tipologia di prodotti viene però commercializzata anche sul territorio italiano ed è quindi necessario che venga affrontato anche questo ambito.
Ogni sessione di formazione è tenuta da un legale esterno e ha una durata di mezza giornata.
Una volta terminata la formazione ai Responsabili, per tutti gli altri collaboratori che trattano dati personali sono previste sessioni di aggiornamento da un'ora ciascuna, in cui verranno illustrate le novità introdotte dal nuovo Regolamento europeo rispetto all'attuale legge vigente. La formazione specifica sulla nuova regolamentazione si affianca alle tradizionali sessioni relative al tema della privacy che vengono veicolate da anni agli utenti dell'organizzazione.

A seguito della formazione verrà effettuata una revisione dell'analisi preliminare. Infatti quando tutti i Responsabili saranno a conoscenza dei requisiti del GDPR, potrebbero emergere trattamenti non considerati precedentemente o valutazioni differenti dello stato del trattamento rispetto alle esigenze di adeguamento. Di conseguenza, potrebbe essere necessaria una revisione delle attività con relativo riesame del budget stimato.
A valle della rifinitura, verranno stabilite con l'ausilio del supporto legale le priorità d'azione sui trat-

tamenti censiti, in base ai rischi ad essi connessi.
L'attività entrerà poi nel vivo e sarà coordinata a livello globale, attraverso incontri per tematica e teleconferenze con le medesime funzioni nelle varie sedi, con l'obiettivo di creare degli standard a livello di Gruppo applicabili nei diversi Paesi. Analizzare in contemporanea sulle varie sedi trattamenti analoghi permetterà infatti una standardizzazione sia nei processi che nella documentazione, ottimizzando così i costi di consulenza esterna.

Le maggiori difficoltà incontrate ad oggi riguardano la raccolta dei dati, poiché spesso le informazioni ottenute non sono del tutto coerenti e richiedono un continuo coordinamento, la definizione in dettaglio delle attività da svolgere, in termini di processi, tecnologie, tool di supporto da implementare e la stima dell'impegno, dei costi e dei tempi necessari.
La mole di lavoro derivante dal percorso di adeguamento è molto consistente, ma rappresenta al tempo stesso un'importante opportunità per l'azienda. Studiando a fondo i trattamenti sarà infatti possibile ottimizzare processi, snellire procedure e aumentare l'efficienza.

GRUPPO ITAS ASSICURAZIONI

Fondata a Trento nel 1821, ITAS (Istituto Trentino-Alto Adige per Assicurazioni) è la Compagnia Assicuratrice più antica d'Italia.
Proteggere contro gli incendi è stato il primo servizio offerto ai soci assicurati. Nel tempo, ITAS ha sviluppato la propria attività ed esteso la propria presenza sul territorio, conservando integra la sua natura mutualistica e la sua indipendenza.
Il Gruppo ITAS, una delle poche mutue presente nel territorio italiano, vanta una rete di circa 650 agenti: insieme ai collaboratori e al personale di agenzia danno vita a una famiglia di 4.500 persone,

dislocate in oltre 750 uffici e agenzie sul territorio italiano, che operano a tutela dei soci assicurati secondo i principi mutualistici della Compagnia.
Tra i primi 10 gruppi assicurativi italiani, ITAS mette quotidianamente al centro del proprio operato la sicurezza e la mutualità, i valori fondanti della Compagnia, che si concretizzano anche nel sostegno di iniziative rivolte alle imprese sociali impegnate nello sviluppo della comunità.

Il Gruppo ITAS ha recentemente introdotto un sistema piramidale di policy valido per tutte le società del Gruppo per mantenere alti i livelli di sicurezza sulle informazioni, con particolare attenzione ai dati inerenti i soci assicurati. Questa attenzione si applica a tutti i dati presenti sia presso le sedi ITAS sia presso terze parti che trattano dati per conto dell'azienda.
La Compagnia adotta un sistema di gestione della sicurezza delle informazioni atto a salvaguardare e preservare l'integrità, la disponibilità e la confidenzialità di tutti i dati trattati. Per ottenere questo scopo sono stati implementati processi tecnici e organizzativi volti a contrastare minacce interne ed esterne e a minimizzare danni diretti e indiretti, sia economici che di reputazione.
Il Gruppo ITAS si impegna a soddisfare i requisiti specificati in queste policy e si impegna a garantire un continuo miglioramento del sistema di gestione della sicurezza delle informazioni, per far fronte a eventuali incidenti nell'organizzazione e per rispondere ai continui cambiamenti in atto, legati, ad esempio, all'innovazione tecnologica, alle relative nuove minacce, alle variazioni normative.

La Divisione Servizi Informatici stabilisce un quadro di riferimento gestionale per attuare ed esercitare un sistema di governo della sicurezza delle informazioni all'interno dell'organizzazione aziendale. Il sistema di gestione è ispirato alla normativa internazionale ISO/IEC 27001 ed è volto a disciplinare aspetti relativi alla sicurezza logica, fisica e organizzativa, tenendo conto anche delle disposizioni di legge e regolamentari. Uno dei principali obiettivi del sistema è quello di analizzare ed evidenziare,

con approccio basato sulla valutazione del rischio, eventuali criticità all'interno dell'organizzazione su temi inerenti la sicurezza delle informazioni attraverso specifiche policy.

Per aumentarne l'efficacia all'interno dell'organizzazione, le policy sono state concepite su tre livelli:

- "Information Security Policy" apicale, che ha come obiettivo quello di definire la politica aziendale in merito alla gestione della sicurezza delle informazioni;
- "Disposizioni", che definiscono le azioni necessarie al fine di soddisfare quanto richiesto dalla "Information Security Policy" e disciplinano temi quali: sistema di gestione delle policy sulla sicurezza, organizzazione della sicurezza, sicurezza risorse umane, gestione degli "asset" fisici e logici, controllo accessi, crittografia, sicurezza fisica, sicurezza delle attività operative, protezione da minacce esterne, sicurezza delle comunicazioni, acquisizione, sviluppo e manutenzione dei sistemi, gestione degli incidenti relativi alla sicurezza, sicurezza della informazioni nella gestione della continuità operativa, conformità, leggi e regolamenti ecc.;
- "Standard", che sono stati creati con lo scopo di dettagliare temi inseriti all'interno delle "Disposizioni", ma che sono ritenuti particolarmente significativi ai fine della sicurezza delle informazioni. Esempi di "standard" sono documenti di dettaglio su temi quali ad esempio: la configurazione sicura di sistemi ed apparati "hardening", la gestione del patching, la gestione dell'antimalware, il dettaglio sulla gestione accessi, i processi di gestione degli incidenti di sicurezza, le clausole sulla sicurezza da inserire nei contratti stipulati con le terze parti ecc.

Le policy, al fine di essere sempre attuali, sono riviste a intervalli regolari, condivise con le funzioni preposte e divulgate alle parti interessate.

IKEA

IKEA è un'azienda multinazionale fondata in Svezia nel 1943 e specializzata nella vendita di mobili, accessori e decorazioni per l'arredamento della casa. La società ha sede legale in Olanda e opera in 48 Paesi attraverso i suoi oltre 390 negozi sparsi in tutto il mondo. Nel 2016 il suo fatturato ha superato i 34 miliardi di Euro.

In tema di sicurezza informatica, la casa madre del Gruppo IKEA definisce gli end-point da utilizzare e i sistemi di prevenzione e rilevamento, per un totale pari a circa il 70% delle scelte complessive. Il restante 30% è rappresentato da local solutions, ossia da sistemi richiesti dalle unità operative dei singoli Paesi che generalmente l'headquarter non è in grado di implementare in tempi brevi come quelli richiesti dal business della nazione. La struttura che richiede una soluzione particolare riceve pertanto dalla casa madre una "delega" allo sviluppo e all'implementazione del tool a livello locale. Le local solutions vanno tuttavia ridotte al minimo, poiché rappresentano per la casa madre stessa una fonte di rischio aggiuntiva e una perdita di controllo.

Per valutare gli aspetti di sicurezza delle local solutions che le Countries hanno intenzione di implementare, sono stati recentemente introdotti i penetration test. Tale approccio ha un impatto in termini di budget, ma permette una valutazione completa dell'affidabilità della soluzione e della credibilità del fornitore. I penetration test vengono effettuati periodicamente anche sui sistemi già esistenti.

Ogni struttura nazionale ha la facoltà di creare figure locali che possono rappresentare una sorta di progetto pilota da replicare eventualmente a un livello superiore. È il caso, ad esempio, della figura del CISO, introdotta in Italia nel 2011 e divenuta in seguito "internazionale", tanto che ogni Paese

è spinto dalla casa madre ad istituirla. Al momento dell'introduzione di tale figura in ambito locale non esistevano linee guida, obiettivi o attività di riferimento e la direzione da seguire è stata definita da zero, anche in seguito a consulenze esterne.
A livello mondiale va rilevata l'esistenza di un Global Retail Information Security Manager con cui l'IS Responsible italiano si relaziona periodicamente all'occorrenza. Tale figura fornisce la direzione, le policy e gli standard da seguire.

La funzione Information Security in IKEA Italia è inserita all'interno della funzione Risk Management. Il CISO risponde pertanto al Risk Manager anche e soprattutto nell'ottica di garantire l'indipendenza e l'autonomia della figura. Sullo stesso livello di IS si collocano Security & Safety, Internal Audit e Compliance.
L'approccio si è evoluto nel tempo: se in passato l'informazione veniva concepita come un bene aziendale che andava salvaguardato per motivi legati al business, successivamente si è passati a considerare il dato personale come un'informazione da proteggere anche per ragioni di compliance normativa. Nel 2015 è stata pertanto associata a Information Security la funzione di Data Privacy.

Un tema importante per IKEA Italia è quello relativo alla creazione di consapevolezza. La società ha svolto un programma di formazione, indirizzato al management dei vari store, relativo ai rischi legati al mondo IT; in esso sono stati forniti esempi di casi concreti di incidenti cyber particolarmente rilevanti ed è stato distribuito a tutti i dipendenti un booklet contenente raccomandazioni di base (in materia di gestione password, chiusura sessioni, ecc.).
Per quanto riguarda la Data Privacy si è invece tenuto un corso dedicato, rivolto alle figure manageriali e specialistiche aventi normalmente a che fare con i dati personali dei clienti (ad esempio il customer service), in cui sono state approfondite le tematiche della L. 196/03 ("Codice della Privacy").

Particolare attenzione è stata dedicata ai cambiamenti normativi: provvedimenti del Governo Monti, normativa sui cookies e GDPR. Proprio in vista dell'entrata in vigore del Regolamento europeo, la casa madre si sta riorganizzando e sta creando un canale con le Countries al fine di sfruttare il know-how e le competenze locali e di comprendere le normative interne.

In generale, essendo ormai ben sviluppato un team anche a livello globale, le linee guida sono sempre più chiare e ben delineate. Attualmente le sfide maggiori sono rappresentate da social network e device mobili.
Per IKEA l'attenzione al brand è massima, e quello che succede sui social network viene monitorato costantemente. La sfida è quella di essere pronti e reattivi nel momento in cui dovessero verificarsi particolari situazioni.

SNAM

Snam è il leader europeo nella realizzazione e gestione integrata delle infrastrutture del gas naturale. Con le sue 3.000 persone, gestisce la rete di gasdotti più estesa e accessibile d'Europa (lunga oltre 32.500 km), un sistema di stoccaggio del gas tra i più importanti a livello continentale (con una capacità di 16,5 miliardi di metri cubi) e il primo terminal GNL costruito in Italia. È inoltre presente attraverso sue partecipate in Austria, Francia e Regno Unito.
Gli investimenti di Snam sono finalizzati a sostenere lo sviluppo delle infrastrutture italiane e la loro interconnessione con quelle europee, rafforzando la sicurezza, la flessibilità e la liquidità dell'intero sistema gas.
Nel 2016 ha registrato un fatturato pari a circa 2,5 miliardi di Euro.
In qualità di Infrastruttura Critica e Strategica per il Paese, Snam gestisce con la massima attenzione

e con senso di responsabilità le tematiche connesse alla security, un settore in rapida evoluzione in cui si fondono e intersecano problematiche estremamente diversificate e di natura geopolitica, sociale, e tecnologica, solo per fare alcuni esempi. Snam è profondamente convinta della necessità di adottare un modello integrato di indirizzo e governo della security; solo in questo modo è possibile, da un lato, garantire l'adozione di principi generali e logiche di intervento operative uniformi ad ogni livello, e dall'altro supervisionare nella maniera più completa e affidabile le fonti di minaccia, a prescindere da come le stesse si manifestano sul piano pratico. In altre parole, deve essere superato il paradigma della sicurezza "a silos"; la sicurezza fisica, la sicurezza logica, la cyber security, la travel security e la security intelligence sono le anime di un unico e complesso ecosistema che integra i contributi e le competenze di tutte le funzioni aziendali.

In Snam, tutti questi temi sono affidati alla Direzione Global Security & Cyber Defence che ha la responsabilità di definire la strategia complessiva e gli interventi tattici conseguenti, monitorandone i risultati al fine di identificare gli eventuali margini di miglioramento. In quest'ambito le competenze da mettere in campo sono così vaste e variegate da richiedere il coinvolgimento simultaneo di numerosi attori appartenenti a diverse funzioni. Un ruolo centrale, da questo punto di vista, risulta essere quello della Direzione ICT, al quale viene richiesto, da un lato, di garantire l'implementazione e la gestione di soluzioni coerenti con le esigenze di sicurezza della Società, e dall'altro di vigilare sull'evoluzione delle minacce in un ambito assai pervasivo come quello tecnologico.

Al contempo, la consapevolezza che i rischi di security costituiscono solo una parte, seppur di rilevanza crescente, dei rischi complessivi che Snam deve monitorare e gestire, ha portato la funzione preposta alla Security a realizzare un significativo programma di razionalizzazione delle proprie metodologie di lavoro, specie quelle afferenti l'analisi dei rischi, al fine di garantire l'adozione di tassonomie e algoritmi coerenti con quelli utilizzati dall'unità di Enterprise Risk Management. L'obiettivo è favorire la definizione di un modello di governo del rischio onnicomprensivo, mettendo gli specialisti del Risk Management nella condizione di comprendere anche un ambito (la security) con peculiarità

specifiche e spesso molto diverso dagli altri.
In questo modello di governo della sicurezza a 360 gradi rientrano inoltre tutti i dipendenti e collaboratori ai quali viene chiesto, ciascuno nei limiti del proprio ruolo e mansioni, di partecipare attivamente al mantenimento di livelli di sicurezza adeguati e coerenti con le esigenze della Società. Dal punto di vista pratico ciò si traduce in due richieste: rispetto dei comportamenti attesi e sviluppo della capacità di identificare i segnali deboli.
Per raggiungere questo obiettivo, Snam ha predisposto un programma pluriennale di sensibilizzazione e formazione articolato in varie iniziative specifiche, che fanno ricorso a molteplici metodologie didattiche e si rivolgono a target differenziati che spaziano dall'intera popolazione aziendale fino a specifiche categorie professionali.
Nella consapevolezza, infine, che un adeguato governo della security passi anche attraverso l'applicazione trasparente e continuativa di logiche di infosharing, Snam sta facendo sistema con il mondo istituzionale (attraverso la formula del Partenariato Pubblico Privato), con le Associazioni di categoria e con i peer di mercato per migliorare i livelli di competenza e la tempestività di risposta alle minacce secondo un modello di governo della security il più possibile esteso ed efficace.

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Osservatorio Information Security & Privacy

GDPR e Security: un percorso impervio… a trazione integrale

Gli Attori

Febbraio 2018

La School of Management del Politecnico di Milano

La **School of Management del Politecnico di Milano**, costituita nel 2003, accoglie le molteplici attività di ricerca, formazione e alta consulenza, nel campo dell'economia, del management e dell'industrial engineering che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili.

La Scuola ha ricevuto, nel 2007, il prestigioso accreditamento **EQUIS**. Nel 2009 è entrata per la prima volta nel **ranking del Financial Times** delle migliori Business School europee, e oggi è in classifica con *Executive MBA*, *Full-Time MBA*, *Master of Science in Management Engineering*, *Customised Executive programmes for business* e *Open Executive programmes for managers and professionals*. Nel Marzo 2013 ha ottenuto il prestigioso accreditamento internazionale da **AMBA** (*Association of MBAs*) per i programmi **MBA** e **Executive MBA**. La Scuola può contare su un corpo docente di più di duecento tra professori, ricercatori, tutor e staff e ogni anno vede oltre seicento matricole entrare nel programma undergraduate. La Scuola è membro **PRME** (*Principles for Responsible Management Education*), **Cladea** (*Consejo Latinoamericano de Escuela de Administración*) e **QTEM** (*Quantitative Techniques for Economics & Management Masters Network*).

Fanno parte della Scuola: il **Dipartimento di Ingegneria Gestionale** e il **MIP Graduate School of Business** che, in particolare, si focalizza sulla formazione executive e sui programmi Master.

Le attività della School of Management legate all'Innovazione Digitale si articolano in:
- *Osservatori Digital Innovation*, che fanno capo per le attività di ricerca al Dipartimento di Ingegneria Gestionale;
- Formazione executive e programmi Master, erogati dal MIP.

Gli Osservatori Digital Innovation

Gli *Osservatori Digital Innovation* della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di fare cultura in tutti i principali ambiti di Innovazione Digitale per favorire lo sviluppo del Paese.

La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese.

La **Mission** degli Osservatori è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di Innovazione Digitale in Italia.

Gli Osservatori sono oggi un punto di riferimento qualificato sull'Innovazione Digitale in Italia che integra attività di Ricerca, Comunicazione, Formazione e una Community sempre più ampia di professionisti.

I fattori distintivi

Le attività degli Osservatori Digital Innovation sono caratterizzate da 4 fattori distintivi.

1. La **Ricerca** sui temi chiave dell'innovazione digitale è basata su solide metodologie (studi di caso, survey, censimenti, quantificazioni di mercato, analisi bibliografiche, ...).
2. La **Community** è composta da decisori e C-Level della domanda, dell'offerta e delle Istituzioni, che collaborano e sviluppano relazioni concrete nelle numerose occasioni di interazione.
3. La **Comunicazione** è finalizzata a raggiungere, attraverso Convegni, Media e Pubblicazioni, il più ampio numero di persone, per diffondere buone pratiche, esperienze e cultura legata all'innovazione digitale.
4. La **Formazione**, attraverso pubblicazioni, webinar e workshop premium del sito Osservatori.net, rappresenta un canale unico per l'aggiornamento professionale sui temi chiave dell'innovazione digitale.

Gli Osservatori Digital Innovation (2017-2018)

Gli Osservatori Digital Innovation sono classificabili in 3 macro categorie.

1. *Digital Trasformation*, che include gli Osservatori che analizzano in modo trasversale i processi di innovazione digitale che stanno profondamente trasformando il nostro Paese.
2. *Digital Solutions*, che raggruppa gli Osservatori che studiano in modo approfondito specifici ambiti applicativi e infrastrutturali relativi alle nuove tecnologie digitali.
3. *Verticals*, che comprende gli Osservatori che analizzano l'innovazione digitale in specifici settori o processi.

Digital Transformation:
Agenda Digitale | Design Thinking for Business | Digital Transformation Academy | Startup Hi-tech | Startup Intelligence

Digital Solutions:
Artificial Intelligence | Big Data Analytics & Business Intelligence | Cloud Transformation | eCommerce B2c | Enterprise Application Governance | Fatturazione Elettronica & eCommerce B2b | Gestione Progettazione e PLM (GeCo) | Information Security & Privacy | Internet of Things | Mobile B2c Strategy | Mobile Payment & Commerce | Multicanalità | Omnichannel Customer Experience | Smart Working

Verticals:
Cloud nella Pubblica Aministrazione | Contract Logistics "Gino Marchet" | Digital Insurance | eGovernment | Export | Fintech & Digital Finance | Food Sustainability | Gioco Online | HR Innovation Practice | Industria 4.0 | Innovazione Digitale in Sanità | Innovazione Digitale nei Beni e Attività Culturali | Innovazione Digitale nel Retail | Innovazione Digitale nel Turismo | Innovazione Digitale nell'industria dello Sport | Internet Media | Mobile Banking | Professionisti e Innovazione Digitale | Smart AgriFood | Supply Chain Finance

Si segnalano di seguito gli Osservatori correlati a *Information Security & Privacy*:
Big Data Analytics & Business Intelligence | Cloud Transformation | Digital Innovation Academy | Enterprise Application Governance | Industria 4.0 | Internet of Things | Smart Working

I numeri chiave del 2017

- **Formazione:** 150 pubblicazioni con i risultati delle ricerche; 200 workshop e webinar; archivio di 800 Pubblicazioni e 300 Eventi on demand.
- **Ricerca:** 39 Osservatori; 5.000 casi; 90 Professori/Ricercatori/Analisti.
- **Network:** 350 partner e sponsor; 150.000 contatti; 8.500 contatti C-Level; 18.000 partecipanti agli Eventi.
- **Comunicazione:** 200 Eventi; 5.000 Uscite stampa; 20.000 Report cartacei distribuiti; 25 Pubblicazioni scientifiche su riviste internazionali.

Per maggiori informazioni si veda il sito **www.osservatori.net**

Seguici anche su:

MIP Politecnico di Milano Graduate School of Business

Gli *Osservatori Digital Innovation* sono fortemente integrati con le attività formative della Scuola: nel senso che rappresentano un'importante sorgente per la produzione di materiale di insegnamento e di discussione per i corsi e traggono anche spesso linfa vitale dalle esperienze di coloro che partecipano ai corsi (in particolare a quelli post-universitari erogati dal MIP) o vi hanno partecipato nel passato.

In sinergia con gli Osservatori, il MIP Politecnico di Milano Graduate School of Business ha lanciato diverse iniziative nell'ambito Digital Innovation:

- Master Executive MBA con possibilità di scegliere corsi elective focalizzati sui temi della Digital Business Transformation;
- Percorso Executive in Gestione Strategica dell'Innovazione Digitale;
- Corsi brevi Digital Innovation.

Per maggiori informazioni si veda il sito **www.mip.polimi.it**

POLITECNICO
MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

Il punto di riferimento
per l'Aggiornamento Executive sull'Innovazione Digitale

visita **www.osservatori.net** e scopri come accedere a tutti i servizi

L'innovazione digitale a portata di Click!

In un contesto in cui l'innovazione digitale ha sempre più rilevanza per la competitività delle imprese e il cambiamento incessante caratterizza le nuove tecnologie, aggiornarsi è fondamentale per tutti i professionisti a vari livelli aziendali. Dedicare tempo e risorse all'aggiornamento di skill e competenze in questo ambito è fondamentale e va fatto in modo permanente lungo tutta la vita professionale, attraverso nuovi strumenti compatibili con il lavoro quotidiano.

Osservatori.net

Gli Osservatori Digital Innovation rappresentano una fonte unica di conoscenza sull'Innovazione Digitale sviluppata da un team di 90 Ricercatori e Professori del Politecnico di Milano, che da anni punta a fornire a professionisti, manager e imprenditori una visione strategica e manageriale dell'innovazione digitale, consapevole che questa rappresenta una leva indispensabile per la competitività delle imprese e il rilancio economico e sociale del nostro Paese.

Fattori Distintivi

- Piattaforma multimediale e interattiva per un aggiornamento continuo a distanza;

- Ricerca indipendente, caratterizzata da rigore scientifico, modelli originali e basata sull'analisi dell'eccellenza;

- Analisti e esperti con un know-how unico e distintivo al servizio di manager e professionisti.

Rapporti

Osservatori.net offre la più completa raccolta di analisi e dati sull'Innovazione Digitale in Italia. I Rapporti sono caratterizzati da formati innovativi che consentono una rapida ricerca delle informazioni di proprio interesse

Workshop e Webinar Premium

Eventi Premium della durata di circa 4 ore (Workshop) e 1 ora (Webinar), durante i quali i partecipanti possono confrontarsi con gli Analisti e Esperti che approfondiscono i temi chiave dell'innovazione digitale

Percorsi

Workshop e Webinar sono organizzati in *Percorsi* focalizzati su un particolare tema:

Agenda Digitale | Big Data & Analytics Strategy | Cloud Computing Strategy & Business Model | Come Innovare il Business grazie al Design Thinking | Digital Travel Innovation | Finance Digital Revolution | eCommerce & Customer Experience Strategy | Fatturazione Elettronica e Dematerializzazione | GDPR: cosa occorre fare per arrivare in regola il 25/05/2018 | HR Innovation & Smart Working Practice | Information Security & Privacy | Internet Media Strategy | Internet of Things Application | Mobile B2c Strategy | Omnichannel Customer Experience Management | Smart AgriFood | Social Media Strategy | Startup & Innovation | Supply Chain Finance

Per maggiori dettagli visitare:
www.osservatori.net/it_it/percorsi

CEFRIEL

CEFRIEL è un Digital Innovation and Design Shop che opera dal 1988 nell'ambito dell'innovazione, della ricerca e della formazione per aziende e Pubbliche Amministrazioni. Suo obiettivo primario è rafforzare i legami tra università e imprese attraverso un approccio multidisciplinare che, partendo dalle esigenze dell'impresa, integra i risultati della ricerca, le migliori tecnologie presenti sul mercato, gli standard emergenti e la realtà dei processi industriali, per innovare o realizzare nuovi prodotti e servizi che uniscono ICT e Design.

Il capitale umano è costituito da circa 130 professionisti, ai quali si affiancano docenti e ricercatori universitari, esperti del mondo delle imprese, visiting researcher, studenti. I docenti universitari rivestono un ruolo proattivo. In particolare, essi sono i mentor scientifici per lo sviluppo delle competenze all'interno del centro e la guida scientifica nelle iniziative di ricerca. I professionisti di Cefriel sono ingegneri e laureati in discipline scientifiche con titoli accademici plurimi (master post-laurea, PhD, MBA, etc.), i più senior con oltre 10-15 anni di esperienza.

Unica azienda italiana a essere inserita da Gartner tra i "Cool Vendors in IoT Solutions 2016", Cefriel è organizzato in centri di competenza specialistici che coprono tutte le aree dell'Information and Communication Technology, dalla microelettronica alle interfacce utente più evolute, in particolare nell'ambito di API Economy and Distributed Architectures, Business and Analytics, Design, Information Security and Infrastructures, Internet of Things, Project Management, Smart Cities, Cross-channel Web, Mobile and Wearable.

Sfruttando le proprie competenze multidisciplinari distintive, CEFRIEL è in grado di sviluppare soluzioni all'avanguardia, dall'ideazione fino all'esecuzione di progetti complessi, integrando hardware, software e le più recenti tecnologie di comunicazione multimediale.

CEFRIEL è oggi una società consortile a responsabilità limitata senza scopo di lucro i cui soci sono il Politecnico di Milano, l'Università degli Studi di Milano, l'Università degli Studi di Milano-Bicocca, l'Università degli Studi dell'Insubria, la Regione Lombardia e aziende multinazionali operanti nei settori ICT, dei media e dell'energia. Inoltre, con la presenza negli USA e in Europa (in particolare UK), CEFRIEL rafforza ulteriormente il supporto alle crescenti esigenze d'innovazione delle imprese anche a livello internazionale. Dal 2014 CEFRIEL è anche affiliate partner di EIT ICT Labs, la rete di centri di ricerca leader in Europa nel campo dell'innovazione ICT, e ospita il nodo satellite di Milano.

Il Dipartimento di Elettronica, Informazione e Bioingegneria

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA

Il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB) è uno dei più grandi dipartimenti di ICT in Europa. Con circa 840 collaboratori, tra personale di ricerca strutturato, collaboratori esterni, studenti di dottorato e personale tecnico e amministrativo, il Dipartimento costituisce una realtà vitale in grado di sostenere la formazione, la ricerca di base, la ricerca applicata e l'attività di trasferimento tecnologico alle imprese.

La qualità della ricerca scientifica è l'obiettivo principale del DEIB, perseguito secondo i più elevati standard internazionali di qualità. All'interno del dipartimento sono presenti competenze eccellenti e consolidate, sia a livello nazionale che internazionale, nei settori dell'automazione, dell'informatica, dell'elettronica, della bioingegneria, dell'ingegneria elettrica e delle telecomunicazioni.

La qualità del lavoro di ricerca è testimoniata dalla vasta rete di collaborazioni con le migliori istituzioni internazionali, che fa del Dipartimento uno dei principali attori dello scenario mondiale dell'innovazione scientifica e tecnologica.

L'ambiente di ricerca del DEIB comprende anche la società consortile CEFRIEL e dodici spin-off.

Per maggiori informazioni si veda il sito **www.deib.polimi.it**

Clusit

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più autorevole associazione italiana nel campo della sicurezza delle informazioni. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Collabora con diversi Ministeri ed Agenzie Governative, con le Forze dell'Ordine, con il Garante per la Privacy, con Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Banca d'Italia, Confindustria e Confcommercio.

Tra le attività ed i progetti per il 2018: la produzione di documenti tecnico-scientifici; la formazione specialistica; il Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria, arrivato alla 13a edizione; i Security Summit, conferenze specialistiche a Milano dal 13 al 15 marzo, a Treviso il 16 maggio, a Roma il 6 e 7 giugno e Verona il 4 ottobre; il Rapporto Clusit, rapporto annuale sul Cyber-crime e sullo stato della sicurezza delle informazioni e delle reti in Italia; il Mese Europeo della Sicurezza Informatica, campagna di sensibilizzazione della Commissione Europea e dell'ENISA che si svolge ogni anno in ottobre, promossa in Italia da Clusit.

Clusit è su **www.clusit.it**

I Sostenitori della Ricerca

Partner

- Accenture
- AlmavivA
- Marsh
- Nest2
- Poste Italiane
- Spike Reply
- Symantec
- TESISQUARE©

Sponsor

- BT
- Fastweb
- Grant Thornton Financial Advisory Services
- Horizon Security
- MEGA International
- Sinergy

Supporter

- BDO Italia
- Generali Global Corporate & Commercial (GC&C)
- XL Catlin

Accenture
www.accenture.it

Accenture è un'azienda leader a livello globale nel settore dei servizi professionali, che fornisce una vasta gamma di servizi e soluzioni nei settori strategy, consulting, digital, technology, operations e security.

Combinando un'esperienza unica e competenze specialistiche in più di 40 settori industriali e in tutte le funzioni aziendali – sostenuta dalla più ampia rete di delivery center a livello mondiale – Accenture opera all'intersezione tra business e tecnologia per aiutare i clienti a migliorare le proprie performance e creare valore sostenibile per i loro stakeholder.

Con circa 435.000 professionisti impegnati a servire i suoi clienti in più di 120 paesi, Accenture favorisce l'innovazione per migliorare il modo in cui il mondo vive e lavora.

Visita il sito www.accenture.it

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations.

Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders.

With more than 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at www.accenture.com

AlmavivA
www.almaviva.it

AlmavivA è sinonimo di innovazione tecnologica. Esperienze consolidate, competenze uniche, ricerca continua e una puntuale conoscenza dei diversi settori di mercato, pubblico e privato, ne fanno il Gruppo leader italiano nell'Information & Communication Technology.

Con 41.000 persone, 10.000 in Italia e 31.000 all'estero, AlmavivA è il 5° Gruppo privato italiano per numero di occupati al mondo, con un fatturato nel 2016 pari a 739 milioni di euro. AlmavivA opera a livello globale, attraverso 39 sedi in Italia e 22 all'estero, con un'importante presenza in Brasile, oltre che negli Stati Uniti, Cina, Colombia, Tunisia, Romania e Bruxelles, centro nevralgico della UE.

Il Gruppo AlmavivA accompagna i processi di digitalizzazione e innovazione tecnologica del Paese, raccogliendo la sfida che le realtà di qualsiasi dimensione e settore dovranno affrontare nei prossimi anni per rimanere competitive, innovando il proprio modello di business, la propria organizzazione, la cultura aziendale e l'ICT.

AlmavivA si pone come System Integrator di riferimento per i propri clienti nella definizione delle strategie per una gestione efficace della Cyber Security, a protezione di business e informazioni di realtà pubbliche e private dalle nuove minacce e vulnerabilità.

Con un focus sui principali scenari legati alla sicurezza informatica in ottica security e privacy-by-design, l'offerta End-to-End AlmavivA va dalla fase di definizione all'integrazione di soluzioni e servizi di sicurezza gestiti, adeguati alle esigenze del cliente e basate sull'analisi del rischio e dell'impatto sull'organizzazione aziendale.

Marsh
www.marsh.it

Marsh, leader globale nell'intermediazione assicurativa e nelle soluzioni per il risk management, opera in team con i propri clienti per definire, sviluppare e offrire soluzioni innovative, specifiche per ogni settore, che aiutino i clienti stessi a proteggere il loro futuro e a crescere.

Dalla grande azienda internazionale alla media impresa, dalle associazioni agli enti pubblici, l'approccio di Marsh permette di definire le opportunità di riduzione del rischio, migliorare l'efficienza e contenere i costi, progettare una strategia di risk management su misura in base all'organizzazione e al suo profilo di rischio e offrire risultati che siano allineati agli obiettivi di business.

Integrità, onestà, determinazione, orientamento al risultato e mutuo rispetto sono i valori etici che, combinati alle competenze, stanno alla base del rapporto con il cliente: mettere il cliente al primo posto per noi significa mettere a sua disposizione le migliori competenze locali e internazionali e il know-how presente in azienda, proponendo soluzioni che meglio rispondono al suo interesse.

Con circa 30.000 colleghi che collaborano per fornire servizi per l'analisi e la gestione del rischio in oltre 130 Paesi, Marsh è parte di Marsh & McLennan Companies, un team di società leader nei servizi professionali nelle aree del rischio, strategia e persone. Il Gruppo ha 60.000 dipendenti nel mondo e un fatturato annuo che supera i 13 miliardi di dollari.

Oltre a Marsh, fanno parte di Marsh & McLennan Companies anche Guy Carpenter, che sviluppa strategie di gestione di rischio, capitale e riassicurazione per aiutare i clienti a crescere in modo profittevole e perseguire opportunità emergenti; Mercer, che fornisce ad aziende e organizzazioni consulenza e soluzioni tecnologiche orientate a soddisfare le esigenze di salute, benessere e carriera dei propri dipendenti; e Oliver Wyman, che offre consulenza strategica, economica e di brand ad aziende e istituzioni.

Nest2
www.nest2.com

NEST2 è un'azienda 100% a capitale italiano che progetta e realizza soluzioni informatiche su misura per aziende, pubbliche o private, di grandi o piccole dimensioni e in diversi settori.
È uno dei primi system integrator in Italia in ambito sicurezza informatica ed implementa da venticinque anni soluzioni integrate con il massimo livello di certificazioni e al più alto grado tecnologico.

In concreto:
Offre consulenza per il design di reti e architetture tecnologiche. Definisce e gestisce il ciclo completo di sistemi per la sicurezza informatica in chiave totalmente *tailor made*. Prende in carico i servizi operativi dei clienti: outsourcing completo di sistemi e business process avendo come priorità qualità e cost-effectiveness.

NEST2 opera su tutto il territorio nazionale attraverso 3 sedi – Padova, Milano, Roma.

L'offerta di NEST2 si articola in quattro aree:

- *Security* – progettazione e realizzazione di progetti di sicurezza informatica, con estremo livello di complessità, in modalità full outsourcing e secondo framework ITIL. Security Operation Center (SOC) H24 7/7 giorni, con 15 anni di esperienza, > 3000 device amministrati e 8000 ticket/anno.
- *Networking* – progettazione, realizzazione e gestione operativa di reti dati –architetture campus e reti convergenti. Approccio di qualitative full/partial outsourcing grazie al Network Operation Center (NOC) H24 7/7 giorni, con 20 anni di esperienza, > 200.000 device amministrati, > 180.000 ticket/anno, 97% tempo di risposta in 14 secondi.
- *IT* – Design e delivery di soluzioni IT destinati ad ambienti di business complessi. Integrazione di soluzioni su base cloud computing, hybrid e on premises; in ottica full outsourcing o personalizzata in base alle esigenze dei clienti. Service Desk, H24 7/7 giorni e IT Competence Center > 2000 device amministrati e > po6000 ticket/anno.
- *Compliance* – Supporto dei clienti nelle fasi di valutazione (auditing) e implementazione dei processi e dei sistemi di gestione secondo normative standard e globali (GDPR).

Filosofia dell'azienda
NEST2 si pone come il partner per l'innovazione e la trasformazione tecnologica dal DNA italiano che fa della sartorialità e della passione al fianco del cliente le parole chiave del proprio lavoro. L'obiettivo è quello di fornire servizi ICT, gestiti rigorosamente secondo i criteri di innovazione, qualità, efficienza e sicurezza.

Poste Italiane
www.posteitaliane.it

Poste Italiane è la più grande infrastruttura di servizi in Italia. Grazie alla presenza capillare su tutto il territorio nazionale, ai forti investimenti in ambito tecnologico e al patrimonio di conoscenze rappresentato dai suoi *143mila dipendenti*, Poste Italiane ha assunto un ruolo centrale nel processo di crescita e modernizzazione del Paese.

Oggi fornisce servizi logistico-postali, di risparmio e pagamento, assicurativi e di comunicazione digitale a oltre *32 milioni* di clienti.

Gli importanti investimenti in *ricerca e sviluppo* e nella *formazione* dei propri dipendenti hanno inoltre consentito a Poste Italiane di creare servizi avanzati basati sulle esigenze dei clienti e capaci di cogliere le trasformazioni sociali del nostro Paese.

Da sempre attenta al *rispetto dell'ambiente* e ai temi dello *sviluppo sostenibile*, l'Azienda è impegnata nella riduzione delle emissioni e nell'abbattimento dell'inquinamento attraverso un sempre maggiore utilizzo di energia da fonti rinnovabili e la scelta di veicoli a basso impatto ambientale.

L'attenzione all'innovazione e alle persone e la vicinanza territoriale sono alla base dei *risultati di eccellenza* raggiunti da Poste Italiane in particolare nel settore finanziario e ancor più in quello assicurativo, dove Poste Vita ha fatto registrare una crescita straordinaria che l'ha proiettata al secondo posto tra le compagnie di assicurazione attive in Italia.

Spike Reply
www.reply.eu

Spike Reply è la società del Gruppo Reply specializzata nei servizi di consulenza e soluzioni integrate di Cyber Security.

L'avvento del mondo digitale, e la crescente interconnessione di persone, dispositivi e organizzazioni, sono fonte di maggiori vulnerabilità e di nuovi rischi.

La rapida evoluzione delle esigenze di business e la continua introduzione di nuove tecnologie quali Mobilità, Consumerizzazione, Cloud, automazione industriale, Internet of Things (automotive, smart homes/cities, wearable devices, …) aumentano la possibilità di esposizione al cybercrime e all'utilizzo illecito delle risorse.

Spike Reply supporta le aziende creando e mantenendo un Programma di Cyber Security per governare, analizzare, proteggere, rilevare e rispondere al panorama delle minacce, sviluppando e implementando le protezioni adeguate.

Spike Reply is the Reply Group Company, specializing in consultancy services and integrated solutions for Cyber Security.

The advent of the digital world, and the inherent interconnectivity of people, devices and organizations, are the source of increased vulnerabilities and new risks.

The rapid evolution of business needs and the continuous introduction of new technologies such as Mobility, Consumerization, Cloud, industrial automation, Internet of Things (automotive, smart homes/cities, wearable devices, …) increase the likelihood of exposure to cybercrime and resources misuse.

Spike Reply assists enterprises creating and maintaining a Cyber Security Program to govern, assess, protect, detect and respond to the threat landscape, developing and implementing the appropriate safeguards.

Symantec
www.symantec.com/it

Symantec Corporation (NASDAQ: SYMC) is the global leader in cyber security.

Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks.

Our integrated products offer unparalleled protection and insight to reduce risk and lower costs across your entire organization. We help companies, governments and individuals secure their most important data wherever it lives.

TESISQUARE©
www.tesisquare.com

TESISQUARE® – Where IT happens è la piazza delle soluzioni software collaborative nella quale persone, tecnologie e processi vengono interconnessi.

L'azienda è protagonista da 23 anni nel mondo dell'Information Technology, con una presenza estesa a livello internazionale, un fatturato superiore ai 25 milioni di euro ed oltre 5.000 clienti, di cui 30 top brand a livello mondiale.

Le soluzioni di TESISQUARE® gestiscono ogni anno circa 139 milioni di transazioni e sono utilizzate in oltre 80 paesi da un network di 25.000 aziende; consentono di digitalizzare i processi lungo la supply chain estesa, dal produttore al consumatore finale, generando valore attraverso una piattaforma integrata di Sourcing and Procurement, Supply Chain Execution, Transportation Management, Retail and e-Commerce.

TESISQUARE® abilita inoltre la collaborazione e la visibilità in tempo reale grazie a capabilities trasversali in ambito Governance, Risk and Compliance, Digital Transformation, E2E Control Tower e Supply Chain Finance: veri e propri acceleratori che permettono alle aziende di evolvere più rapidamente nel loro percorso di innovazione.

La leadership in ambito supply chain execution e visibility è stata riconosciuta anche dalla principale società a livello mondiale di ricerca e analisi in ambito IT.

TESISQUARE® si propone come partner unico per i propri clienti, promuovendo innovazione e trasformazione attraverso competenze di business modelling, con l'obiettivo di accompagnare le aziende sin dalle prime fasi di disegno dei nuovi modelli di processo.

E lo fa attraverso un approccio "end-to-end turn-key", fornendo la soluzione pronta e funzionante, integrandola, ad esempio, con qualsiasi sistema presente in azienda.

L'obiettivo è quello di condurre il cliente nel processo di cambiamento dall'inizio alla fine, anche attraverso servizi a supporto come le attività di onboarding degli stakeholders, l'help desk e l'application maintenance.

Il tutto ormai disponibile nella più completa trasparenza offerta dalle tecnologie cloud.

BT
www.bt.com/italia

BT è tra i principali provider globali di servizi e soluzioni di comunicazione, con clienti in 180 Paesi e con 14 SOC 'follow the sun'. Presente in Italia dal 1995, BT gode di una visione privilegiata circa gli attacchi alla sicurezza delle reti, malware e violazioni ai danni delle organizzazioni in tutto il mondo.

Le soluzioni di BT oltre a garantire la compliance alle misure per la sicurezza ICT indicate dalle norme e dalla agenzie ed autorità nazionali, hanno anche l'obiettivo di mitigare il rischio rappresentato dalle nuove minacce informatiche e sono realizzate grazie all'esperienza maturata da BT Security nel proteggere sia la rete di BT sia quella dei propri clienti in Italia come in 180 paesi al mondo.

Il portfolio BT Security comprende una gamma di soluzioni puntuali e di servizi di sicurezza gestita end-to-end network-centrici, ma anche di servizi di consulenza e cyber intelligence.

BT Security si avvale di oltre 2.500 specialisti ed è uno dei membri fondatori del Cybersecurity Information Sharing Partnership (CiSP) in Gran Bretagna, è membro dell'IoT Security Foundation e di numerosi progetti internazionali sul tema.

Fastweb
www.fastweb.it

Con circa 2.4 milioni di clienti, **Fastweb** è uno dei principali operatori di telecomunicazioni in Italia.

L'azienda offre servizi voce e dati, fissi e mobili, a famiglie e imprese.

Puntando sull'innovazione Fastweb ha sviluppato una rete nazionale in fibra ottica di 45.600 chilometri e oggi raggiunge con la tecnologia fiber-to-the-home o fiber-to-the-cabinet circa 7,9 milioni di abitazioni e aziende.

Entro il 2020 Fastweb raggiungerà con la rete ultrabroadband 13 milioni di famiglie (ovvero il 50% della popolazione), di cui 5 milioni con tecnologia Ftth e velocità fino a 1 Gigabit e 8 milioni con tecnologia FttCab e velocità fino a 200 Megabit per secondo.

La società offre ai propri clienti un servizio mobile di ultima generazione 4G e 4G Plus.

Entro il 2020 il servizio mobile verrà potenziato grazie alla realizzazione di una infrastruttura di nuova generazione 5G.

Fastweb fornisce servizi di tlc ad aziende di tutte le dimensioni e alla Pa, alle quali offre connettività e servizi ICT avanzati, come l'housing, il cloud computing, la sicurezza e la comunicazione unificata.

La società fa parte del gruppo Swisscom dal settembre 2007.

Grant Thornton Financial Advisory Services
www.bgt-grantthornton.it

Horizon Security
www.horizonsecurity.it

Bernoni Grant Thornton è la member firm italiana di Grant Thornton International Ltd specializzata nei servizi di consulenza tributaria, societaria, advisory, IT ed outsourcing.

Con oltre 200 persone che operano nelle sedi di Milano, Roma, Padova, Brescia, Arezzo, Torino, Trento e Trieste garantiamo ai nostri clienti una costante presenza per un servizio più efficace e di qualità.

Il nostro approccio si basa sull'approfondimento delle specifiche esigenze di ciascun cliente, a cui rispondiamo tempestivamente ed in modo integrato, anche avvalendoci della collaborazione delle member firm estere del network Grant Thornton, presente in 130 paesi.

Con un team di 7 partners e circa 40 professionisti, Grant Thornton Financial Advisory Services Srl è la società del gruppo Bernoni Grant Thornton che fornisce servizi di Advisory, tra i quali M&A, Due Diligence, Valuation, Recovery & Reorganization, Forensic & Investigation e Business Risk Services. È quest'ultima la linea di business specializzata in servizi di Governance, Compliance e Risk Management, con un particolare focus su progetti di Cybersecurity e di adeguamento al GDPR.

Horizon Security Azienda italiana specializzata nell'erogazione di servizi di consulenza in ambito Cyber & Information Security, opera da svariati anni sui più importanti mercati nazionali ed internazionali, affiancando i maggiori Gruppi Industriali, Finanziari, Assicurativi e dei Servizi nell'affrontare le nuove sfide per la protezione del proprio business.

Attraverso una costante attività di formazione e di investimenti nella Ricerca, Horizon Security è in grado di proporre servizi e soluzioni all'avanguardia al passo con i continui mutamenti degli scenari tecnologici e normativi.

Può contare su professionisti qualificati e specializzati esclusivamente nell'ambito Cyber & Information Security al fine di identificare le soluzioni organizzative e tecnologiche più idonee a proteggere il business dei propri clienti da rischi e minacce.

Grazie alle competenze ed esperienze maturate in ambito *Data Protection, Governance Risk e Compliance, Security Assessment ed Infrastructure Security*, Horizon Security si propone come il partner ideale per soddisfare le esigenze delle aziende Enterprise.

MEGA International
www.mega.com/it

MEGA International è una società di software, presente a livello globale, che supporta le aziende nella gestione della complessità, fornendo loro una vista interattiva delle operation.

Il software HOPEX offre supporto e iniziative di IT e business transformation mediante una singola piattaforma collaborativa che gestisce i dati dell'architettura d'impresa (Processi, Servizi, Asset IT, Dati) con gli elementi di Rischio e di Compliance.

Il vantaggio per le aziende è quello di un ambiente collaborativo che supporta tutti gli stakeholder coinvolti nel processo di trasformazione e di governo: Operations, IT, C-level e Consulenti che condividono un'unica fonte attendibile per poter rafforzare il proprio sistema di decision-making, stabilendo il giusto equilibrio tra innovazione, ottimizzazione dei costi e gestione del rischio

MEGA è presente in Italia e ha una copertura mondiale attraverso le sue nove filiali e oltre 20 partner commerciali che permettono di sostenere il vostro business aziendale indipendentemente da dove si trova.

Sinergy
www.sinergy.it

Fondata nel 1994 **Sinergy** S.p.A. è tra i principali System Integrator del panorama ICT italiano e affianca oltre 600 clienti di tutti i settori fin dalla fase iniziale di assessment dell'infrastruttura. Con oltre 130 professionisti qualificati, Sinergy offre servizi di advisory "eseguibile", design, implementazione, integrazione, governo e gestione delle soluzioni dal NOC di Torino, proponendo soluzioni all'avanguardia per l'eccellenza del Data Center. Le 25 risorse dedicate in ambito Information Security e Compliance e l'offerta Cyber Security Suite personalizzata mediante servizi strategici di Security Advisoring, indirizzano tutte le componenti siano esse organizzative, procedurali o tecnologiche. La Cyber Security Suite ricopre aree multidisciplinari (Information Technology, Cyber Security, Business Continuity & Disaster Recovery, Compliance) e adotta approcci concreti utili al raggiungimento degli obiettivi dei propri clienti quali, ad esempio: analisi degli attuali livelli di sicurezza e individuazione delle vulnerabilità con attività di Ethical Hacking; definizione delle soluzioni più idonee per il cliente ed implementazione di sistemi di protezione anche integrati sui nuovi paradigmi Cloud; governo della sicurezza, monitoraggio e gestione operativa dei servizi (Flexible Managed Services). L'offerta è in linea con gli standard e best practice internazionali quali ISO 27001, ISO22301, COBIT 5.0 e ITILv3.

BDO Italia
www.bdo.it

BDO è tra i principali network internazionali di revisione contabile e di consulenza aziendale in Italia e nel mondo.

BDO è presente in oltre 160 paesi con circa 74.000 professionisti altamente qualificati.

Presenti in Italia da oltre 50 anni, siamo ad oggi oltre 700 professionisti di cui più di 60 partner e operiamo in 20 uffici, una struttura integrata e capillare che garantisce la copertura del territorio nazionale.

Offriamo servizi professionali integrati in linea con i più elevati standard qualitativi a grandi gruppi internazionali, PMI nazionali, investitori privati e istituzioni pubbliche, per affiancarli e migliorarne le performance in ogni fase del loro sviluppo, nel rispetto delle normative vigenti.

Il nostro team Data Protection & Cybersecurity è composto da esperti di information technology, IT audit, risk management, compliance, organizzazione e internal auditing, che lavorano insieme ai nostri legali, specializzati in tematiche di trattamento dei dati e sicurezza informatica, per sviluppare metodologie innovative d'intervento.

Generali Global Corporate & Commercial (GC&C)
www.generaliglobalcorporate.com

Generali Global Corporate and Commercial (GC&C) è la Business Unit del Gruppo Generali che offre soluzioni assicurative Property & Casualty ad aziende di grandi e medie dimensioni.

GC&C fornisce servizi assicurativi su scala globale e fa leva sull'approccio integrato del Gruppo Generali, coordinato da un team centrale e specifici team attivi nei singoli paesi.

GC&C si avvale di un network mondiale di professionisti per offrire un approccio congiunto verso i rischi globali e per dare ai propri clienti soluzioni rilevanti.

GC&C fornisce una gamma completa di soluzioni property, casualty e specialty lines a clienti corporate e commercial e ai loro broker in tutto il mondo.

Ad oggi, più di 1000 professionisti lavorano nei nove uffici principali di GC&C a Milano, Londra, Madrid, Parigi, Praga, San Paolo, Hong Kong, New York e Monaco di Baviera.

GC&C serve clienti e broker in più di 100 paesi, generando complessivamente una raccolta premi (GWP) di circa 2 miliardi di euro.

XL Catlin
http://xlcatlin.it

XL Catlin è il marchio utilizzato da XL Group Ltd, società quotata alla borsa di New York, che presta attività assicurativa e riassicurativa a livello globale, offrendo una vasta gamma di prodotti e servizi, inclusi Property, Energy, Construction (CAR/EAR), Casualty, Environmental, Financial Lines (Cyber, D&O, PI, etc.), Marine, Fine Art & Specie, a imprese industriali, società commerciali e di professionisti e compagnie assicurative.

Con un team di 7.300 persone in oltre 100 uffici, XL Catlin opera in più di 215 Paesi, sottoscrivendo circa 3.500 programmi globali e almeno nel 70% di questi ha il ruolo di leader.

I clienti guardano a XL Catlin per ottenere soluzioni ai rischi più complessi e per proseguire nel cammino dell'innovazione.

XL Catlin è un partner che mette a disposizione specifiche competenze per la gestione, il finanziamento e il trasferimento dei rischi, in modo che i suoi clienti si possano concentrare sul successo del loro business.

Per ulteriori informazioni, visita xlcatlin.it

Grafica: Osservatori Digital Innovation
Realizzazione: Danilo Galasso, Emanuela Micello e Stefano Erba
Stampa: Tipografia Litografia A. Scotti | www.ascotti.it

www.osservatori.net

Seguici anche su:

PARTNER

SPONSOR

SUPPORTER

IN COLLABORAZIONE CON

CON IL PATROCINIO DI