The Innovation Group

Cyber Risk Management 2018

Marzo 2018

a cura di: **Elena Vaciago**

Associate Research Manager, The Innovation Group

2018

SOMMARIO

EXECUTIVE SUMMARY 2

Cosa preoccupa maggiormente i responsabili della sicurezza 3

Far evolvere l'approccio al Cyber Risk Management 3

Come sta cambiando la percezione con riferimento a questi rischi 4

Quali sono le iniziative chiave per la Cybersecurity? 4

Gestione dei rischi associati alla supply chain 5

… e i trend di adozione della cyber insurance 6

ESPERIENZA DI ATTACCHI CYBER NELLE AZIENDE ITALIANE 7

Quali debolezze sfruttano gli attaccanti 8

A chi attribuire l'attacco 9

Quali sono state le conseguenze degli attacchi 9

EVOLUZIONE DEL PROGRAMMA PER IL CYBER RISK MANAGEMENT .. 13

Le principali iniziative per la Cybersecurity intraprese nel 2017 14

I processi di ICT Security gestiti in outsourcing 16

QUALE SARÀ IN FUTURO IL RUOLO DEL CISO 17

Information Security Governance 21

Cybersecurity Governance: il modello da adottare secondo FERMA e ECIIA 24

Misurazione e Reporting al CEO/Board 26

DATA PROTECTION E ADEGUAMENTO AL GDPR 30

Quali informazioni proteggere da eventuali data breach? 31

MISURE E PROCESSI PER LA SUPPLY CHAIN SECURITY 34

Il Cyber Risk della Supply Chain 34

I passaggi chiave per proteggere l'impresa da questo rischio 36

CYBER INSURANCE: ADOZIONE E MOTIVAZIONI 40

CONCLUSIONI 43

EXECUTIVE SUMMARY

Nessuna realtà è completamente al riparo da un attacco cyber con conseguenze catastrofiche: ma chi guida l'azienda ne è cosciente? E quanto è preparato a rispondere ad un'eventuale crisi di questo tipo?

L'indagine "Cyber Risk Management 2018", parte delle attività del Programma annuale Cybersecurity & Risk Management Program di The Innovation Group, giunge quest'anno alla sua terza edizione. È stata rivolta, tra dicembre 2017 e gennaio 2018, alla Community del Programma, composta da tutti i professionisti che si occupano di Cybersecurity, quali ad esempio CIO/Responsabili ICT, Security Manager, Chief Security Officer e Chief Information Security Officer, Risk, Audit e Compliance Manager, oltre che Professionals e Consulenti della Sicurezza coinvolti in prima persona nella definizione delle strategie per l'ICT Security.

L'indagine arriva dopo che alcuni attacchi di dimensione globale, come i ransomware (o meglio cryptoworm) WannaCry e NotPetya, hanno risvegliato l'attenzione di moltissimi su questi temi. I ransomware stanno colpendo trasversalmente e indiscriminatamente tutte le categorie, dalla grande organizzazione, all'industria manifatturiera, al piccolo studio professionale, ai singoli individui: ciò nonostante il pericolo non viene preso sufficientemente sul serio.

Oggi sappiamo che il rischio cyber differisce da altre forme di rischio per molti aspetti:

- Un sistema digitale può essere vulnerabile da più punti di vista.
- Alcuni tipologie di attacco sono facilmente realizzabili, hanno costi bassi ed elevata efficacia, e questo spiega perchè il fenomeno è in continua espansione.
- L'evenienza di un attacco cyber è difficile da prevedere.
- La probabilità di incorrere in questi incidenti è molto alta (come vedremo anche dai risultati dell'indagine), essendo le aziende e la società nel suo complesso sempre più dipendenti da sistemi digitali e da Internet.
- Nel caso in cui l'attacco cyber abbia successo, è difficile ricostruire i fatti e in particolare attribuire l'azione in modo preciso ad uno specifico attaccante.
- È una problematica che per quanto nota da decenni, sta esplodendo in questi anni. È un'emergenza ma molte aziende sono impreparate ad affrontarla: mancano sia gli skill specialistici sia anche le conoscenze di base. In caso di incidente, molti non sanno come affrontarlo e neanche a chi rivolgersi per ripristinare velocemente la situazione.
- Il problema si sta spostando anche nell'ambito geopolitico delle relazioni che intercorrono tra gli Stati. Diverse azioni in corso sono già oggi esempi di "guerra cibernetica" (cyber war), motivo per cui molti Stati stanno rafforzando con urgenza i programmi di National Security.

In linea con gli anni precedenti, anche nel 2018 gli obiettivi della Cyber Risk Management survey sono stati:

- Fornire indicazioni concrete alle aziende per aiutarle a confrontarsi con quanto stanno facendo altri (in particolar modo le aziende di grande dimensione, più attrezzate in questo campo) nella risposta alle minacce alla sicurezza, in modo da

poter prendere in considerazione modalità differenti per migliorare i propri metodi e contribuire così a ridurre i rischi.

- Fornire agli intervistati un benchmark rispetto al quale poter valutare lo stato attuale della sicurezza delle informazioni e del rischio informatico all'interno delle proprie organizzazioni.
- Verificare quali sono le aree di miglioramento, qual è la maturità del piano di Cyber Risk Management e come è andato avanzando negli ultimi 3 anni.
- Fornire al management spunti per identificare le tendenze e per supportarli nelle decisioni strategiche.

Hanno risposto all'indagine Cyber Risk Management 2018 in tutto 88 aziende, con una prevalenza di aziende medio grandi (il 60% ha oltre 500 addetti), dei diversi settori verticali. Rispetto alle survey effettuate in precedenza (relative alle scelte per la Cybersecurity effettuate dalle aziende nei 2 anni precedenti, 2015 e 2016), l'indagine propone quest'anno 2 nuovi ambiti di approfondimento, sul tema del Secure Supply Chain management e della Cyber Insurance. Di seguito riportiamo i principali risultati.

Cosa preoccupa maggiormente i responsabili della sicurezza

Guardando alla situazione attuale, con riferimento agli attacchi cyber in corso, abbiamo quasi un 90% di organizzazioni che registrano di essere state oggetto di numerose minacce. Tra le forme di attacco osservate più di frequente, attacchi di Phishing e social engineering, che colpiscono oramai oltre la metà delle aziende del campione, seguiti da malware e ransomware.

Gli attacchi sfruttano diversi vettori per colpire l'azienda – sia vulnerabilità nei suoi sistemi e applicativi, sia comportamenti errati o mancati aggiornamenti/configurazioni – ma di fatto trovano soprattutto nelle mail il veicolo principale per aprirsi un varco verso i sistemi informativi interni all'azienda. Secondo i rispondenti infatti, nel 93% dei casi gli incidenti sono stati causati originariamente da una mail contenente un allegato o un link malevolo: è una percentuale molto alta, da collegare a più tipologie di attacco (dal phishing, al malware generico, al ransomware, agli stessi APT) e conferma la preoccupazione sullo sfruttamento della "debolezza delle persone" come primo veicolo per condurre un attacco che avrà successo.

In percentuali minori ma comunque importanti appaiono le vulnerabilità che hanno permesso l'ingresso degli attaccanti (lato web server al primo posto, ma anche applicative su device endpoint, lato server o su altri device). Ulteriori debolezze sfruttate dagli attaccanti sono gli errori di configurazione e il mancato controllo sulla sicurezza delle chiavette USB, oltre alla possibilità che l'attacco sia favorito da una terza parte o da un contractor (13% delle risposte).

Un altro tema preoccupante è la crescita degli attacchi mirati alla singola azienda, ossia, ingegnerizzati in modo specifico per ottenere informazioni o causare disturbi alla singola realtà. Un 46% dei rispondenti afferma di essere a conoscenza di almento un attacco che è stato sferrato in modo mirato alla propria organizzazione.

Far evolvere l'approccio al Cyber Risk Management

L'approccio alla gestione di questo rischio deve quindi evolvere per essere più efficace. Fino ad oggi l'area della cybersecurity è stata troppo orientata a strutturarsi "a silos", in

modo separato dal resto dell'organizzazione (un limite anche all'interno dello stesso dipartimento ICT, come si vede nello scarso collegamento esistente tra sicurezza e sviluppo applicativo). Servirebbe invece un approccio più coordinato con il resto dell'organizzazione e orientato a comunicare meglio le problematiche della cybersecurity al top management/al board. Le stesse attività di misurazione e reporting sono oggi poco strutturate, qualitative invece che quantitative, in molti casi inesistenti.

Come emerge dall'indagine, il primo problema di un CISO (68% delle risposte) è rendere partecipe e ingaggiare il top management/il Board dell'azienda comunicandogli nel modo più efficace possibile le criticità della cybersecurity - che lui vede, ma che il resto del business non conosce. Ma oggi il management delle aziende è sufficientemente coinvolto in tema di cyber risk? O bisognerebbe invece incrementare i momenti di incontro e dibattito? Secondo le risposte fornite dal campione analizzato, in questo momento nel 70% dei casi il responsabile della sicurezza partecipa ad incontri con il CEO/ board "MAI o QUASI MAI".

Il secondo problema, indicato dal 52% dei rispondenti, è invece allineare meglio gli obiettivi della cybersecurity a quelli del business. Come bilanciare quindi al meglio sicurezza e obiettivi del business? In molte realtà ci si pone questo problema e le soluzioni sono spesso diverse. Per dare una risposta a questo tema abbiamo riportato nel Report varie interviste ad esperti e a Security Officer dell'**Advisory Board** del Programma.

Al terzo posto la necessità di far fronte a una complessità crescente di gestione della cybersecurity: è un problema per oltre la metà dei rispondenti, ed è evidente che non farà altro che peggiorare in futuro, via via che le aziende si esporranno in nuovi ambiti dell'innovazione digitale. È un tema legato alla mancanza di competenze e risorse nell'ambito della security, che può essere affrontato soltanto se si lavora in un'ottica di PROGRESSIVA AUTOMAZIONE (pur mantenendo il controllo) di un numero sempre maggiore di task

Come sta cambiando la percezione con riferimento a questi rischi

Per ottenere molte delle soluzioni che i Security Manager e i CISO oggi ricercano (dal miglior collegamento con il top management e con la strategia aziendale, all'evoluzione della sicurezza verso una funzione perfettamente allineata con i reali bisogni dell'azienda) serve innanzi tutto un cambio di passo su un aspetto fondamentale: la cultura della sicurezza nella propria organizzazione e fuori da essa. Fintantoché la sicurezza informatica sarà percepita più come un costo (68% delle risposte) che non come un elemento che abilita l'innovazione e la trasformazione del business in chiave digitale (32% delle risposte), sarà molto difficile trovare una soluzione a tutti i problemi che oggi ancora limitano il potenziale valore della sicurezza.

Quali sono le iniziative chiave per la Cybersecurity?

Ad oggi il piano delle aziende italiane per la Cybersecurity si pone numerosi obiettivi, non solo salvaguardare l'operatività dell'azienda, ma anche garantirne la reputazione e la conformità alle norme. Proprio il tema della compliance è oggi il driver principale di molte delle nuove iniziative intraprese. Dal confronto con l'analoga indagine svolta un anno fa, appare evidente la crescita di importanza assegnata a "*Garantire i requisiti di Compliance / Sicurezza Nazionale*", risposta che figura al primo posto tra le nuove iniziative lanciate nel 2017. È questa conseguenza di un'attenzione oggi molto più elevata sulla rispondenza

alle norme, in tutti i settori, con l'entrata in vigore sia del nuovo Regolamento GDPR, sia anche della Direttiva Europea NIS (Direttiva on Security of Network and Information Systems, 1148/2016[1]), rivolta a mettere in sicurezza i servizi essenziali nazionali in tutti gli stati membri dell'UE.

Confrontando le risposte con quelle ottenute nell'indagine dell'anno precedente si osserva anche che:

- Alcuni aspetti mantengono un'elevata attenzione nelle politiche per la cybersecurity delle aziende: questi sono da un lato i vulnerability assessment, tipicamente svolti con l'ausilio di terze parti specializzate e condotti una o due volte all'anno. Servono a mettere in luce le debolezze a livello di configurazioni e ambienti ICT, aiutando l'azienda a intraprendere nel tempo più breve possibile le necessarie attività correttive. Si confermano inoltre ai primi posti le attività di Backup&Recovery, che risultano essere in effetti tra le misure più efficaci per la Data Protection, quindi assolutamente presenti in un qualsiasi piano di sicurezza.
- In crescita rispetto all'anno precedente figurano da un lato le iniziative di network security, passate da un quinto a un secondo posto. Una ripresa degli investimenti in queste soluzioni è dovuta da un lato a un ricorrente upgrade a livello di rete, dall'altro anche a una maggiore domanda, come conseguenza di attacchi cryptoworm che sfruttavano problematiche a livello di network. Dall'altro lato, incrementi significativi sia sul fronte delle iniziative di security governance, sia sulle soluzioni anti-malware, spinte soprattutto dal problema del ransomware. Una leggera crescita anche per le iniziative di Incident Management: anche se tuttora svolte da una minoranza di aziende (35% delle risposte) si osserva comunque un'attenzione superiore sui temi della risposta rispetto agli anni precedenti.

Per il prossimo anno, oltre l'80% dei rispondenti assegna priorità al tema del GDPR, seguita dal problema di creare maggiore awareness nell'organizzazione, e quindi al controllo degli accessi. Punteggi simili sono ottenuti da temi come la Cyber Threat Intelligence, la Cloud e Mobile security, che si configurano come Hot Topic per un 40% degli intervistati.

Gestione dei rischi associati alla supply chain

Abbiamo chiesto ai rispondenti alla survey quali controlli hanno implementato in azienda per la gestione della cybersecurity dei vendor della catena di fornitura. La situazione risulta nel complesso abbastanza buona nel campione considerato, in quanto i 3 quarti delle aziende (il 74% per la precisione) ha già in essere qualche forma di controllo, e anche più di una. L'attività più frequente (65% delle risposte) è la richiesta ai fornitori di essere compliant a norme/standard di cybersecurity. È questa anche la situazione per quanto riguarda la norma GDPR sulla data protection: sempre di più, le aziende affideranno la gestione dei dati personali a terze parti solo se queste garantiranno di essere GDPR compliant. La seconda misura, che però vede l'adozione da parte di un numero inferiore di aziende (42%) è l'inclusione di requisiti di sicurezza in ogni richiesta di proposta/ contratto con fornitori terzi. Nei contratti con i fornitori possono anche rientrare clausole di cyber insurance (26% delle risposte).

[1] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

… e i trend di adozione della cyber insurance

Dove le aziende si impegnano nel disegno di un ampio e articolato programma di cyber risk management, la cyber insurance può avere un suo ruolo ben preciso, di trasferimento del rischio che non si può mitigare o accettare. Analizzando la situazione presso il campione di aziende contattate, che presenta una maggiore maturità su questi temi rispetto alla media delle aziende italiane, la Cyber Insurance è in crescita. I risultati riportati sono il tasso di adozione della Cyber Insurance rispettivamente per i 3 anni in cui abbiamo effettuato questa indagine, e mostrano chiaramente un interesse sempre più ampio, con la percentuale di aziende che si è dotata di strumenti assicurativi specifici per l'assicurazione cyber passata dal 2% nel 2015, al 7% nel 2016 e al 15% nel 2017.

ESPERIENZA DI ATTACCHI CYBER NELLE AZIENDE ITALIANE

Le aziende subiscono oggi numerose forme di attacco: secondo la Cyber Risk Management 2018 survey, svolta da The Innovation Group tra dicembre 2017 e gennaio 2018 su 88 aziende medio grandi italiane, al primo posto figurano gli **attacchi di Phishing e social engineering** (l'invio di una mail mascherata da messaggio credibile, che giunge da una parte fidata, ma contiene invece un link/un allegato malevolo), che colpiscono oramai oltre la metà delle aziende del campione. È un risultato in linea con le più recenti indagini a livello globale, ad esempio l'ENISA Threat Landscape 2017[2], che vedono gli attacchi di Phishing in forte crescita. È questo il risultato di un trend secondo il quale il cyber crime è sempre più rivolto a sfruttare le debolezze delle persone. Negli ultimi anni infatti la maggior parte degli investimenti di sicurezza sono stati rivolti a proteggere le infrastrutture ICT: poco è stato fatto invece per elevare la cultura di sicurezza tra le persone, che sono quindi facilmente aggirabili con tecniche di social engineering.

Mentre malware e ransomware figurano in posizioni elevate (rispettivamente 52% e 49% delle risposte), come da aspettarsi dati i volumi oramai sempre più elevati di queste forme di attacchi, è invece allarmante il fatto che al quarto posto figurino gli attacchi **Business Email Compromise** (con il 38% dei rispondenti che ne ha fatto esperienza). Con questa frode, denominata anche "truffa del CEO", lo scopo delle organizzazioni criminali è quello di intromettersi, tramite furto d'identità, nei rapporti commerciali tra le aziende, soprattutto per dirottare i pagamenti verso conti correnti esteri dei criminali. Il tutto impersonificando un partner commerciale, un fornitore, un cliente, e chiedendo gli importi dovuti su IBAN diverso. Secondo la Polizia Postale italiana la CEO fraud ha acquisito grande rilevanza e impatto economico: tenendo sotto controllo queste attività, nel 2017 la Polizia Postale è riuscita a bloccare alla fonte oltre 20 milioni di euro e a recuperare 862mila euro da bonifici già disposti.

Al tema delle minacce Ransomware e della Business Email Compromise, data la grande rilevanza che hanno acquisito come minacce cyber in Italia lo scorso anno, The Innovation Group ha dedicato in settembre 2017 un webinar, "Ransomware e BEC i più gravi attacchi cyber per le aziende italiane".

Sempre dall'indagine, si ha evidenza di altre forme di attacco, che anche se in misura minore, sono comunque preoccupanti in quanto dimostrano attività molto mirate, volte ad **acquisire privilegi, a compromettere sistemi, ad accedere a dati critici** delle organizzazioni. In particolare, osserviamo la presenza di **attacchi zero-day** (minaccia informatica che sfrutta vulnerabilità di applicazioni software non ancora divulgate o per le quali non è ancora stata distribuita una patch), escalation di privilegi, **Advanced Persistent Threats**. Bassa invece la percentuale registrata con questa survey degli attacchi dovuti a interni: ne ha avuto esperienza solo il 7% delle aziende del campione (quando analoghe indagini internazionali riportano percentuali anche 4 volte superiori).

[2] ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends

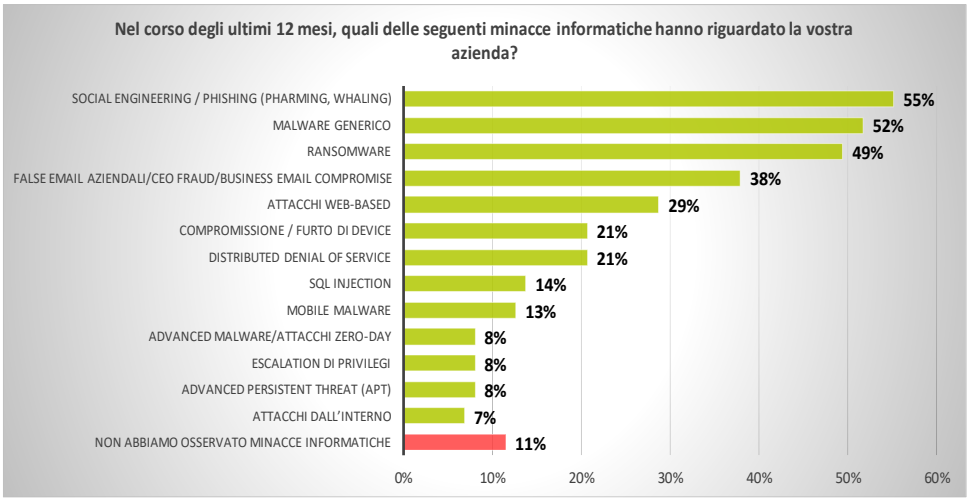

FIGURA 1 – QUALI MINACCE INFORMATICHE HANNO RIGUARDATO LA SUA AZIENDA?

Un dato importante, che merita di essere sottolineato, è che soltanto per l'11% dei rispondenti la propria azienda non ha osservato alcuna minaccia informatica: un numero che fa presupporre che forse le minacce ci sono state e semplicemente non sono state viste, o ancora, che il rispondente non ha informazioni in merito. Si tratta in definitiva di una conferma del fatto che oggi nessuna realtà può dirsi completamente al riparo da un attacco di tipo informatico.

Quali debolezze sfruttano gli attaccanti

Un risultato importante è che nel 93% dei casi gli incidenti sono stati causati originariamente da una mail contenente un allegato o un link malevolo: è una percentuale molto alta, da collegare a più tipologie di attacco (dal phishing, al malware generico, al ransomware, agli stessi APT) e conferma la preoccupazione sullo sfruttamento delle persone come primo veicolo per condurre un attacco che avrà successo. In percentuali minori ma comunque importanti appaiono le vulnerabilità che hanno permesso l'ingresso degli attaccanti (lato web server al primo posto, ma anche applicative su device endpoint, lato server o su altri device). Ulteriori debolezze sfruttate dagli attaccanti sono gli errori di configurazione e il mancato controllo sulla sicurezza delle chiavette USB, oltre alla possibilità che l'attacco sia favorito da una terza parte o un contractor (13% delle risposte).

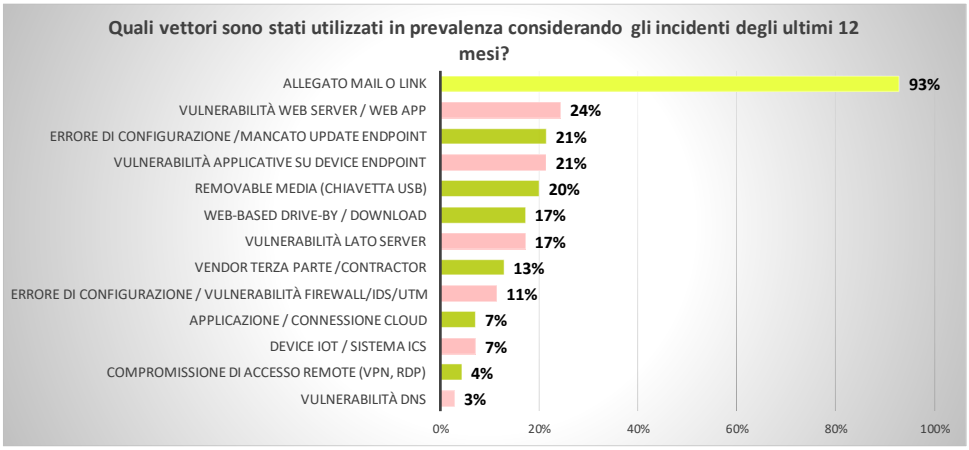

FIGURA 2 – QUALI VETTORI SONO STATI UTILIZZATI DAGLI ATTACCANTI?

A chi attribuire l'attacco

Parlando di attribuzione dell'attacco cyber – una materia sicuramente non semplice – la risposta che viene fornita privilegia (61% delle risposte) genericamente la presenza di questi malware in rete (aspetto sicuramente vero per gran parte del phishing e del malware o ransomware che si propagano tramite botnet in modo massivo su molteplici target).

Un 46% dei rispondenti afferma inoltre di ritenere di aver subito almeno un attacco sferrato in modo mirato alla propria organizzazione (sicuramente vero per tutte le minacce più evolute, dalla CEO Fraud agli APT).

Non mancano però anche altre situazioni che possono essere state all'origine di incidenti, perdite di dati e altri disservizi: sia le possibili negligenze da parte del personale (37% delle risposte), e in percentuali minori, procedure errate ed errori nei sistemi (18%), hacktivism (17%). Gli errori dovuti alle terze parti sono indicati dall'11% dei rispondenti (in linea con la risposta alla domanda precedente, che assegnava un ruolo alla vulnerabilità delle terze parti della supply chain nel 13% dei casi). Si tratta oggi di un rischio, quello delle terze parti, ancora sottovalutato, ma che di fatto è molto importante in un'economia digitale sempre più interconnessa. Ne parleremo più avanti in una sezione della ricerca dedicata.

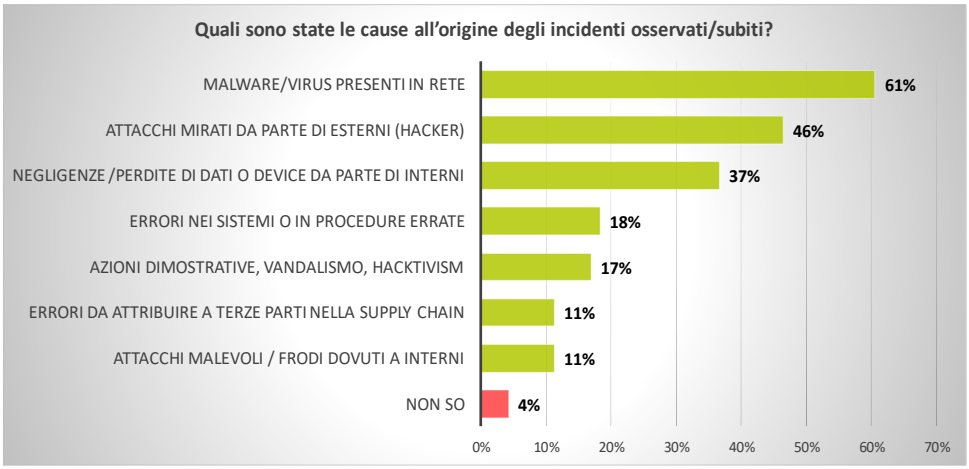

FIGURA 3 – QUALI LE CAUSE ALL'ORIGINE DEGLI INCIDENTI OSSERVATI?

Quali sono state le conseguenze degli attacchi

Parlando di incidenti informatici, spesso si tende ad esagerarne le conseguenze: un data breach di grande dimensione ha degli impatti, sia di tipo economico sia sulla reputazione dell'azienda, di grande rilievo. Ma la stessa cosa non vale genericamente per QUALSIASI incidente informatico dovuto ad attacco cyber: nella maggior parte dei casi infatti le conseguenze sono di piccolo importo, e spesso non vale neanche la pena di segnalarle.

Addirittura, un buon 28% degli intervistati non ha registrato ALCUNA conseguenza dagli attacchi in corso (ma ricordiamoci che di questi, un 11% non aveva osservato neanche gli attacchi, quindi se dovessimo dire quanti tra chi ha osservato gli attacchi è riuscito anche a non avere danni di alcun tipo, arriviamo a una quota del 17%).

Come mostrano le risposte, guardando alle conseguenze degli attacchi infromatici, nella maggior parte dei casi (35% delle risposte) sono stati: mal funzionamento dei sistemi,

disagi e perdità di produttività. Molto elevate però anche le percentuali di chi ha avuto conseguenze serie come:

- Danno all'integrità dei dati: 20%
- Furto d'identità/di credenziali: 17%
- Data breaches con perdita di know how: 14%
- Disclosure di informazioni: 13%
- Frodi finanziarie: 9%.

In tutte queste situazioni, l'impatto relativo all'incidente subito è stato sicuramente rilevante.

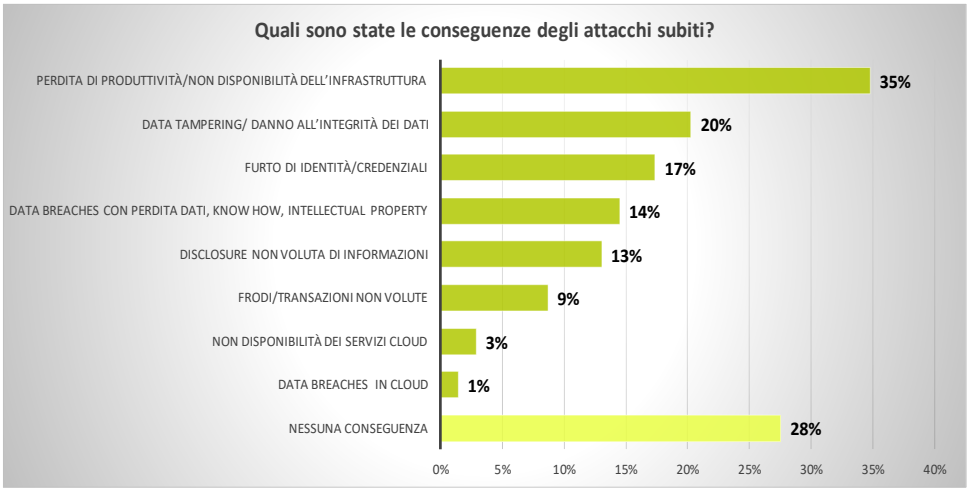

FIGURA 4 – QUALI LE CONSEGUENZE DEGLI ATTACCHI OSSERVATI/SUBITI?

Guardando quindi alla situazione attuale, con riferimento agli attacchi cyber in corso, abbiamo quasi un 90% di organizzazioni che registrano di essere state oggetto di numerose minacce. Gli attacchi sfruttano diversi vettori per colpire l'azienda – sia vulnerabilità nei suoi sistemi e applicativi, sia comportamenti errati o mancati aggiornamenti/configurazioni – ma di fatto trovano SOPRATTUTTO NELLE MAIL il veicolo principale per aprirsi un varco verso i sistemi informativi interni all'azienda.

Le cause degli attacchi sono numerose: quello che però preoccupa di più è che ben un 46% delle aziende ritenga di aver subito almeno un attacco sferrato prendendole direttamente di mira - un elemento molto allarmante che ci fa temere per il futuro impatti ancora più gravi.

Solo un 17% di aziende ritiene di essere riuscito a bloccare gli attacchi in tempo e di non averne subito le conseguenze: è una percentuale un po' bassa, considerando che abbiamo parlato con un campione di aziende caratterizzato dalla presenza di numerose misure e processi per la sicurezza informatica, già presenti nelle aziende del campione, come vedremo dalle risposte successive.

Se circa 1 azienda su 6 riesce a fermare gli attacchi senza subirne le conseguenze, vuol dire che siamo molto lontani da una situazione ottimale con riferimento alla sicurezza informatica. C'è di buono che gli incidenti nella maggior parte dei casi hanno ancora

conseguenze limitate a disservizi e perdita di disponibilità dei sistemi, o perdite di tempo per le persone coinvolte. Gli incidenti gravi come danni ai dati, data breach e frodi, riguardano oggi una minoranza di imprese: il timore è che questa percentuale cresca in futuro o che questi impatti diventino più gravi, anche semplicemente con l'entrata in vigore di norme più stringenti - che sanzioneranno maggiormente questo tipo di eventi. Pensiamo soltato al fatto che a partire dal 25 maggio 2018 sarà operativo il Regolamento Europeo sulla Data Protection (GDPR) e che quindi un'azienda che abbia subito un furto, o un danneggiamento, ai dati dei propri clienti, dovrà da un lato notificarlo (alle autorità e agli stessi clienti in casi gravi) con un problema di reputazione: dall'altro lato potrà subire una sanzione elevata, fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo.

Intervista a Davide Gabrini, collaboratore del Laboratorio di Informatica Forense dell'Università degli Studi di Pavia, afferente al Laboratorio Nazionale di Cyber Security..

TIG. L'Italia è a livello internazionale uno tra i Paesi che ha subito, negli ultimi anni, il maggior numero di attacchi cyber: ad esempio, siamo i terzi nella classifica globale delle vittime di ransomware, dopo Stati Uniti e Giappone. Come lo spieghi?

Davide Gabrini. Sono almeno vent'anni che ripetiamo le stesse cose: in Italia si osserva una preoccupante assenza di sensibilità alla sicurezza informatica, riscontrabile negli investimenti tristemente irrisori che vengono destinati alla cybersecurity, il che ci rende molto più esposti di quanto dovremmo. Abbiamo assistito alla diffusione di alcuni ransomware a velocità impressionante, nonostante fossero disponibili da mesi le patch di sicurezza che avrebbero impedito o quantomeno fortemente mitigato i danni: un segnale di un preoccupante e generale lassismo nel settore. Questo avviene nonostante si osservino ormai da anni perdite economiche consistenti e in crescita accelerata. I ransomware stanno colpendo trasversalmente e indiscriminatamente tutte le categorie, dalla grande organizzazione, all'industria manifatturiera, al piccolo studio professionale, ai singoli individui: eppure nonostante questo il pericolo non viene preso sufficientemente sul serio.

TIG. Come reagisce chi viene infettato?

Davide Gabrini. Se non altro, non può ignorare il problema: se un tempo prevalevano gli attacchi informatici più occulti, che venivano rilevati con mesi di ritardo o addirittura mai, oggi il ransomware si palesa immediatamente per chiedere il riscatto. Si tratterebbe di una minaccia relativamente semplice da debellare: basterebbe rimuovere il malware, o alla peggio reinstallare i sistemi colpiti, e ripristinare i backup. Una procedura non esente da costi, ma che comunque consentirebbe di risolvere il problema con danni contenuti. Ma avere una politica efficiente di backup e ripristino rientra in quegli investimenti preventivi che vengono spesso ignorati, al punto che la vittima preferisce pagare il riscatto, illudendosi con questo di aver risolto un problema che invece permane tal quale a prima. Soprattutto, non ci si rende conto che così facendo si finanzia la criminalità organizzata e la si incentiva ad investire maggiormente nel mercato dei ransomware. Un mercato talmente proficuo che i criminali mettono addirittura a disposizione delle vittime un supporto tecnico, con tanto di assistenza personalizzata, per aiutare "il cliente" a pagare il riscatto e a recuperare i suoi dati, dando a tutto il fenomeno un assurdo aspetto di normalità: è paradossale vedere delle vittime insensatamente rassicurate dalla presenza di questi help desk in grado di "risolvere" il problema che hanno essi stessi causato!

TIG. Qual è l'importo tipico del riscatto?

Davide Gabrini. Il valore dell'importo richiesto per riottenere i dati è variabile: si aggira sovente intorno ai 300 euro, ma si vedono anche richieste da 5-6.000 euro (il valore espresso in euro è variabile anche perché il riscatto è quasi sempre richiesto in Bitcoin ed è quindi soggetto alle fluttuazione della criptovaluta). In alcuni casi riportati dalla stampa si sono raggiunte cifre record: in Corea del Sud il web hosting Nayana, secondo quanto dichiarato dall'AD dell'azienda, avrebbe versato addirittura l'equivalente di un milione di dollari: l'attacco aveva coinvolto 150 server consentendo ai criminali di accedere ad un'ingente quantità di dati dei clienti. Alcuni attacchi

ransomware più sofisticati infatti variano l'importo da pagare anche in ragione della vittima colpita: in questo modo, i profitti dei criminali sono ottimizzati perché il riscatto è proporzionato al valore degli asset compromessi e alle effettive possibilità di spesa della vittima.

TIG. Cosa insegnano queste esperienze a chi le ha subite?

Davide Gabrini. Il più delle volte, purtroppo, niente! Molti, anche se la cosa dà fastidio, finiscono con il pagare come se avessero preso una multa all'autovelox per eccesso di velocità! Poi la vulnerabilità rimane e i backup non si fanno. Il messaggio che sta passando con il ransomware purtroppo è quello che vogliono i criminali: basta pagare e i dati tornano. La cultura che si sta creando intorno al tema è molto sbagliata: proporre il pagamento del riscatto come metodo di risoluzione del problema è eticamente inaccettabile, e i tecnici che lo suggeriscono e si incaricano addirittura della mediazione non si rendono conto che stanno commettendo il reato di favoreggiamento, adoperandosi nell'interesse dei criminali affinché possano riscuotere i loro profitti illeciti.

TIG. Business Email Compromise: come avviene questo tipo di attacco?

Davide Gabrini. Ci sono diversi metodi e differenti strategie di attacco per compromettere la sicurezza di un account e-mail aziendale, o anche solo di account aziendali sui social network. In generale lo scopo degli attaccanti è ottenere accesso alla corrispondenza dell'azienda, meglio se di un impiegato che tratta direttamente i pagamenti o addirittura di un dirigente, per prendere cognizione delle comunicazioni e ricostruire così una mappatura precisa di clienti, partner e fornitori dell'azienda. A un certo punto, l'attaccante può decidere di falsificare in modo molto credibile una comunicazione, o alterarne una effettivamente in corso, per richiedere un pagamento indebito o dirottare un transazione in corso sostituendosi ad uno o addirittura ad entrambi gli interlocutori.

TIG. Ci sono dei segnali che permettono di scoprire, intercettare una truffa di questo tipo?

Davide Gabrini. Ci si dovrebbe insospettire di stranezze improvvise, come errori di italiano incongrui da parte di chi scrive la mail o richieste inattese di variazione dei consueti dati di pagamento: un nuovo codice IBAN, un diverso istituto di credito d'appoggio, una diversa ragione sociale ecc. Simili richieste potrebbero far parte di un attacco di social engineering, ovvero essere parte di una truffa sofisticata attuabile appunto dopo aver preso cognizione delle normali procedure di gestione dei pagamenti al fine di inserirsi illecitamente nel processo nella maniera meno evidente e più rassicurante possibile. In presenza di sospetto sarebbe opportuno svolgere, prima di dare disposizioni, una o più verifiche, utilizzando preferibilmente un canale alternativo rispetto alla mail, ad esempio chiamando il destinatario sul telefono. Non è difficile immaginare una contromisura in caso di sospetto: il difficile è istruire i dipendenti affinché quel sospetto possa nascere quando serve.

TIG. In generale, nel caso in cui un'azienda si rivolga alle Forze dell'ordine per un furto di dati o un incidente informatico, come dovrebbe regolarsi per facilitare le successive indagini?

Davide Gabrini. Tanto le aziende quanto i singoli privati possono essere di grande aiuto per l'avvio delle indagini, perché in qualità di titolari dei sistemi o dei dati hanno un potere investigativo che, nelle prime fasi, supera di gran lunga quello delle Forze dell'Ordine: possono avere ad esempio disponibilità immediata di informazioni a cui gli investigatori potrebbero accedere soltanto esibendo ai provider un ordine della magistratura o addirittura, se prevista, una rogatoria internazionale – con i tempi, i costi e le difficoltà che la cosa comporterebbe. Quando invece le vittime di reato sono in grado di fornire, già in sede di querela e opportunamente preservate, tutte le informazioni a loro accessibili e utili a circostanziare i fatti, la tempestività dell'indagine è di gran lunga agevolata. Sarebbe quindi raccomandabile dotarsi di una procedura interna di incident response che includa anche precise istruzioni sui dati disponibili, sulle modalità di raccolta e conservazione e sulle figure di riferimento per la trattazione, valutazione e trasmissione delle informazioni all'Autorità Giudiziaria.

DA: EVOLUZIONE DEL CYBER CRIME IN DANNO ALLE AZIENDE ITALIANE, 9 LUGLIO 2017 (http://channels.theinnovationgroup.it/cybersecurity/evoluzione-del-cyber-crime-aziende-italiane/)

EVOLUZIONE DEL PROGRAMMA PER IL CYBER RISK MANAGEMENT

Gestire la Cybersecurity è diventato un problema sempre più ampio e complesso per tutte le organizzazioni in ogni parte del mondo. Lo stesso World Economic Forum ha posizionato il Cyber Risk tra i primi 10, al terzo posto come probabilità di attacco e al sesto come potenziale gravità dell'impatto.

TOP 10 Rischi in termini di PROBABILITA' di accadimento	TOP 10 Rischi in termini di IMPATTO
Eventi atmosferici estremi	Armi di distruzione di massa
Disastri naturali	Eventi atmosferici estremi
Attacchi Cyber	Disastri naturali
Frodi e furti di dati	Cambiamento climatico
Cambiamento climatico	Crisi di approvigionamento idrico
Migrazioni su larga scala	Attacchi Cyber
Disastri ambientali arrecati dall'uomo	Crisi alimentari
Attacchi terroristici	Perdita di biodiversità, collasso dell'ecosistema
Commercio illegale	Migrazioni su larga scala
Bolle finanziarie in mercati primari	Diffusione di malattie infettive

TABELLA 1: CLASSIFICA DEI TOP 10 GLOBAL RISKS, THE WORLD ECONOMIC FORUM GLOBAL RISK REPORT (2018)

Oggi numerose motivazioni spingono le aziende ad intraprendere un percorso per mettere in sicurezza i propri sistemi infornativi e i propri dati: secondo i risultati dell'indagine Cyber Risk Management 2018, al primo posto, come anche gli scorsi anni, il rischio di danno reputazionale legato a un incidente grave (Figura 5). La mancata compliance torna in auge quest'anno ed è una conseguenza dell'imminente entrata a regime del nuovo regolamento europeo sulla Data Protection (GDPR), che come vedremo anche nel proseguimento dell'analisi, sta impegnando le aziende per moteplici attività.

Al terzo posto figurano invece le controversie legali: un tema in crescita, che dimostra una maggiore maturità su questi aspetti rispetto al passato. Chi infatti ha la sfortuna di "vivere" un'emergenza legata ad un attacco cyber, sa quale può essere l'impatto economico legato alle eventuali controversie legali, con clienti o partner che risultano parte lesa nel caso della perdita di loro dati, o per disservizi nella produzione e nell'operatività dell'azienda che hanno danneggiato terzi. La perdita di produttività non è considerata ai primi posti, ma in realtà una stima corretta del tempo perso e dei costi esterni per risolvere un incidente, sommato al mancato business generato nello stesso tempo, mostrerebbe che è questa probabilmente la voce di costo maggiore per l'azienda.

Secondo la nota indagine Ponemon Institute sul costo dei Data breach negli USA e negli altri paesi nel mondo[3], la voce di costo maggiore sta appunto nella perdita di business, legata sia alla mancata operatività, sia anche alla perdita dei clienti nei periodi successivi all'incidente (customer churn).

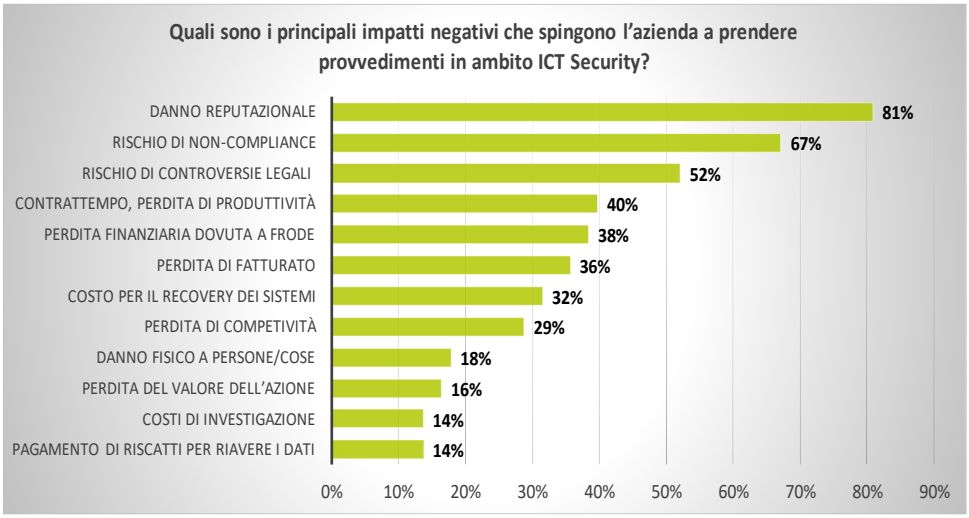

FIGURA 5 – QUALI IMPATTI NEGATIVI SPINGONO LE AZIENDE A INVESTIRE IN CYBERSECURITY?

Le principali iniziative per la Cybersecurity intraprese nel 2017

I programmi delle aziende italiane per la Cybersecurity hanno numerosi obiettivi, non solo salvaguardare l'operatività dell'azienda, ma anche garatirne la reputazione e la conformità alle norme. Proprio il tema della compliance è oggi il driver principale di molte delle nuove iniziative intraprese, come mostrano le risposte alla domanda successiva ("*Quali sono le iniziative in ambito ICT Security intraprese nel 2017*?"). Dal confronto con l'analoga indagine svolta un anno fa, appare evidente la crescita di importanza assegnata al tema "*Garantire i requisiti di Compliance / Sicurezza Nazionale*", che figura al primo posto tra le nuove iniziative lanciate nel 2017, conseguenza di un attenzione oggi molto più elevata sulla rispondenza alle norme, in tutti i settori, con l'entrata in vigore sia del nuovo Regolamento GDPR, sia anche della Direttiva Europea NIS (Direttiva on Security of Network and Information Systems, 1148/2016[4]), rivolta a mettere in sicurezza i servizi essenziali nazionali in tutti gli stati membri dell'UE.

Confrontando le risposte con quelle ottenute nell'indagine dell'anno precedente (riportate in Tabella 2) si osserva che:

- Alcune attività mantengono un'elevata importanza nelle politiche per la cybersecurity: queste sono da un lato i vulnerability assessment, tipicamente svolti con l'ausilio di terze parti specializzate e condotti una o due volte all'anno. Servono a mettere in luce le debolezze a livello di configurazioni e ambienti ICT e aiutano l'azienda ad intraprendere nel tempo più breve possibile le necessarie attività correttive. Si confermano inoltre ai primi posti le attività di

[3] Ponemon Institute 2017 Cost of Data Breach Study
[4] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

Backup&Recovery, che risultano essere in effetti tra le misure più efficaci per la Data Protection, quindi assolutamente presenti in un qualsiasi piano di sicurezza.

- In crescita rispetto all'anno precedente figurano le iniziative di network security, passate da un quinto a un secondo posto: la ripresa degli investimenti in queste soluzioni è dovuta da un lato a un ricorrente upgrade a livello di rete, dall'altro anche a una maggiore domanda, come conseguenza di attacchi cryptoworm che sfruttavano problematiche a livello di network.
- Si registrano incrementi significativi sia sul fronte delle iniziative di security governance, sia sulle soluzioni anti-malware, spinte soprattutto dal problema del ransomware. Una leggera crescita anche per le iniziative di Incident Management: anche se tuttora svolte da una minoranza di aziende (35% delle risposte) si osserva comunque un'attenzione superiore sui temi della risposta rispetto agli anni precedenti.

Principali Iniziative di Cybersecurity 2016	Principali Iniziative di Cybersecurity 2017
Vulnerability assessment/ penetration tests / audit di sicurezza	Garantire i requisiti di Compliance / Sicurezza Nazionale
Information security training and awareness	Network Security (Web Filtering, VPN, IDS, IPS, Firewall, UTM)
Network Security, Web Filtering, VPN, IDS, IPS, Firewall	Vulnerability assessment/ penetration tests / audit di sicurezza
ICT Security governance (ad esempio ruoli, strutture di reporting, direttive)	ICT Security governance (ruoli, strutture di reporting, policy)
Backup&Recovery/ Business continuity	Backup&Recovery/ Business continuity
Aggiornamento delle patch di sicurezza automatizzato/centralizzato	Aggiornamento delle patch di sicurezza automatizzato/centralizzato
Information Security Policies	Soluzioni Anti-malware
Web & Application Security (Secure Coding, Code Review, Patching)	ICT Security reporting ed integrazione con il Risk management aziendale
Garantire i requisiti di Compliance / Sicurezza Nazionale	Information security training / awareness
Mobile security/MDM/MAM	Web & Application Security (Secure Coding, Code Review, Patching)
Conformità alle normative in ambito ICT Security (PCI DSS, privacy)	Endpoint management
Incident management /response/forensic	Incident management /response/forensic
Data Protection (DLP, Database security)	Sviluppo / Miglioramento del Security Operation Center (SOC)
Risk Management / Audit	ICT Security measurement / reporting
IAM, Directory Services, User Provisioning, Privilege Management	Data Protection/ Data Loss prevention

TABELLA 2 – LE PRINCIPALI INIZIATIVE DEL PROGRAMMA PER LA CYBERSECURITY 2017 RISPETTO AL 2016

Nota negativa, il posizionamento delle iniziative di Information Security Awareness, che rispetto alla precedente indagine, perdono posizioni, segnale che sono passate in secondo piano rispetto ad altre attività ritenute più urgenti.

Una conferma della criticità oggi data dalla funzione ICT Security al tema della compliance al GDPR viene anche dalle risposte alla domanda "*Quali dei seguenti Hot Topic sono oggi più rilevanti secondo lei per un CISO/Security Manager?*". Come si osserva nella figura successiva, oltre l'80% dei rispondenti assegna il primo posto al tema del GDPR, seguito dal problema di creare maggiore awareness nell'organizzazione. Compliance al GDPR e problema delle persone sono oggi quindi le principali EMERGENZE vissute dalle aziende: la prima, imposta dalle nuove norme, la seconda invece conseguenza dell'elevata vulnerabilità ad attacchi Phishing/SE che sfruttano la debolezza delle persone.

Segue quindi il tema del controllo degli accessi, visto come un ambito che richiederà un ripensamento delle attuali soluzioni se si vuole effettivamente impostare un nuovo passo alle attuali architetture per la sicurezza ICT. Punteggi simili sono ottenuti da temi come la Cyber Threat Intelligence, la Cloud e Mobile security, che si configurano come Hot Topic per un 40% degli intervistati. Molto minore invece l'interesse per IoT e Cyber Insurance, che riguardano evidentemente una minoranza di aziende (26% e 27% delle risposte rispettivamente). Basso il punteggio assegnato al ransomware: probabilmente si spiega con il fatto che nella maggior parte dei casi, le aziende del campione, che sono più mature rispetto alla media italiana in tema di cyber risk management, non hanno subito forti conseguenze dagli attacchi ransomware, pur avendoli osservati (da Figura 1, abbiamo un 49% di aziende che dice essere stata oggetto di attacco ransomware nel 2017).

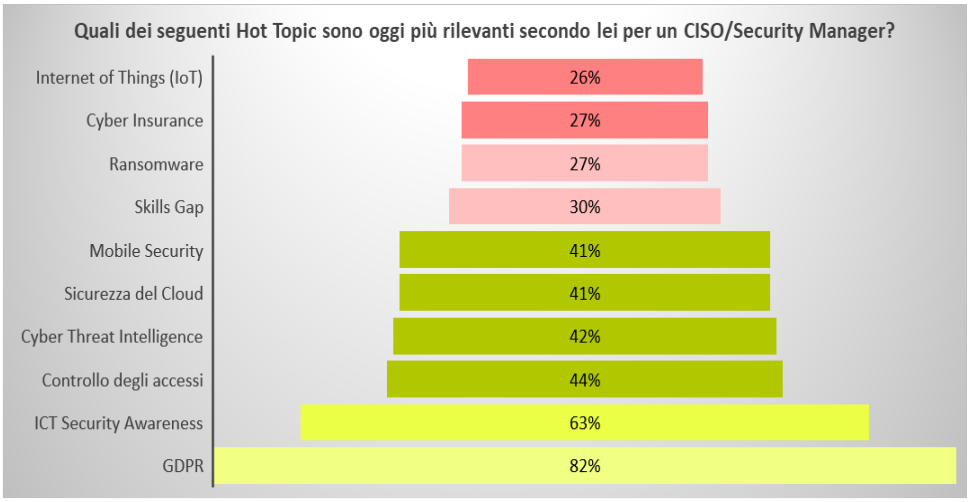

FIGURA 6 – QUALI SONO OGGI I TEMI PIU' IMPORTANTI PER UN SECURITY MANAGER?

I processi di ICT Security gestiti in outsourcing

Con riferimento alle attività per il Cyber risk management affidate a terze parti al primo posto figurano le iniziative di Vulnerability Assessment e Penetration Test, che sono svolte da esterni con queste specifiche competenze. Considerando che in prospettiva, anche per rispondere alla compliance, le analisi delle vulnerabilità dovrebbero entrare a far parte di un piano continuativo di assessment della propria *Posture* di sicurezza, sarebbe da consigliare a queste aziende una valutazione della possibilità di internalizzare queste

competenze e integrare maggiormente la gestione delle vulnerabilità con il proprio risk management.

Con riferimento alle altre voi, il ricorso a terze parti è meno evidente (le percentuali sono più basse) ma si osserva comunque che tutte le diverse tipologie di servizi sono richieste indifferentemente da aziende dei diversi settori e di varia dimensione: segnale che per molti aspetti della security il ricorso a fornitori esterni è oggi indispensabile mancando spesso le competenze interne per svolgere questi compiti.

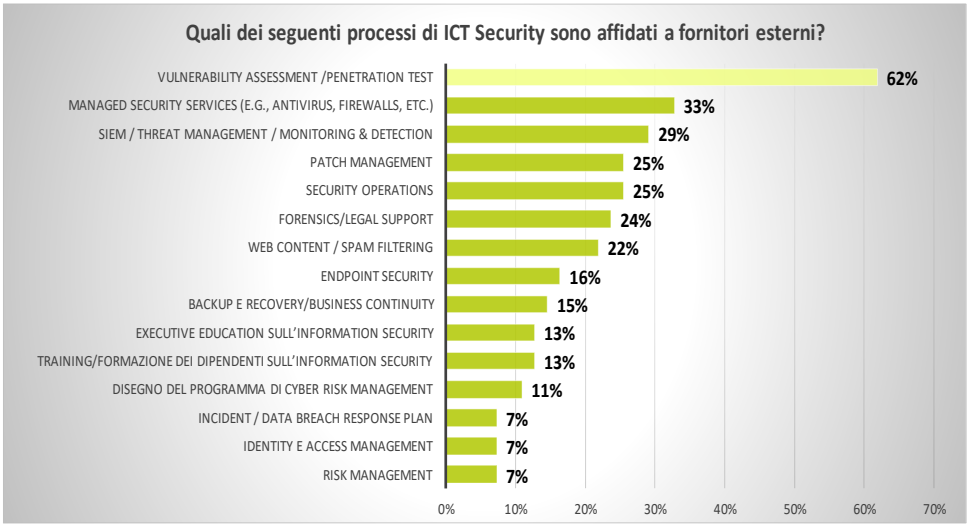

FIGURA 7 – I PROCESSI DI ICT SECURITY GESTITI IN OUTSOURCING

QUALE SARÀ IN FUTURO IL RUOLO DEL CISO

Solo una minoranza di aziende dispone oggi di una figura con responsabilità e competenze manageriali specifiche per il Cyber risk management, ma in prospettiva queste figure saranno sempre più richieste.

Quale sarà quindi in futuro il ruolo del Chief Information Security Officer (CISO)?

Guardando alle best practices internazionali, gli viene riconosciuto sempre più spesso un ruolo da Executive di livello elevato, che guida team cross funzionali e che risponde costantemente su quale è in ogni circostanza l'esposizione dell'azienda ai rischi cyber. In molte grandi organizzazioni, il CISO è oggi una figura che collabora strettamente con la corporate governance e che assicura una crescita costante del business garantendo che il rischio da lui presidiato sia gestito entro limiti di "risk appetite" accettabile. In molte organizzazioni in cui l'approccio ai temi della cybersecurity è ancora di tipo tradizionale, il CISO deve farsi carico di promuovere una cultura più allineata alle nuove sfide e ai nuovi rischi; deve interagire spesso con il top management/il Board e sedere al tavolo dove sono decisi i nuovi prodotti, la nuova strategia dell'organizzazione. Deve inoltre gestire un team di persone che operativamente garantiranno la disponibilità dei sistemi e l'integrità e la riservatezza delle informazioni: poichè disporre di uno staff di professional è sempre più complicato (dalla scarsa disponibilità di queste competenze sul mercato), il CISO dovrà farsi carico della crescita delle sue risorse, tramite programmi di training, volti anche ad aumentare la retention dello staff.

Intervista a Corradino Corradi, Head of ICT Security, Privacy & Fraud Management di Vodafone Italia.

TIG. Quali sono oggi le principali problematiche per il CISO? Quali le priorità da mettere in Agenda per il 2018?

Corradino Corradi. *Tante aziende stanno oggi affrontando una fase importante di trasformazione digitale: in molti settori, nelle Telco sicuramente, il top management è più che mai consapevole della necessità di cambiare il modello di business per mantenere il proprio vantaggio competitivo. Il CISO deve quindi impegnarsi nel far capire che va fatta grande attenzione al tema della sicurezza e della protezione dei dati. L'altra grande sfida è portare a bordo per tempo l'intera organizzazione e le persone, che non hanno ancora oggi una consapevolezza reale dei rischi, come ci si accorge ad esempio con i test di phishing a sorpresa.*

TIG. Quale dovrebbe essere un approccio efficace alla Security Awareness?

Corradino Corradi. *I metodi tradizionali stanno un po' segnando il passo: può essere utile scegliere approcci nuovi come gamification o altri strumenti aziendali, webcast e sessioni interattive con momenti di formazione e test. L'importante è far capire che non è un problema teorico ma avviene nella pratica, 'spear phishing' e mail sono oggi il veicolo principale per far entrare il malware in azienda.*

TIG. Le aziende sono sempre più interessate alle opportunità offerte da una serie di innovazioni Disruptive, dal Cloud, all'Internet of Things, all'intelligenza artificiale. Quale impatto avranno queste sulla Cybersecurity aziendale?

Corradino Corradi. *Vodafone è oggi un leader mondiale in ambito IoT, un mercato che cresce ogni anno a due cifre. La sfida per la sicurezza è garantire una security end-to-end su tutta la filiera, quindi non considerare soltanto il singolo sensore, la sua connessione con il cloud o il cloud stesso, ma l'insieme e contemporaneamente l'anello più debole dei 3. Abbiamo già visto che sta nascendo una nuova generazione di attacchi cyber che sfrutta milioni di dispositivi connessi per arrivare a una magnitudo di potenza molto superiore all'attuale. Inoltre i nuovi rischi cyber per l'IoT possono comportare problemi di safety per le persone, come si è visto nel caso dell'automotive. Parlando poi di intelligenza artificiale e Robochat, si tratta di innovazioni molto promettenti, che Vodafone ha già introdotto per i propri clienti. Permettono di fare tutta una serie di attività nuove, come interagire con lo smartphone senza usare le mani. Anche per queste nuove applicazioni la sicurezza è un elemento importante, soprattutto sul fronte dell'identificazione dell'utente. Andremo sicuramente verso l'adozione di modalità di identificazione più evolute rispetto agli attuali sistemi di identificazione (UserId e password), un cambiamento che potrebbe portare anche opportunità di business.*

TIG. Qual è la tua sensazione sul GDPR, il nuovo regolamento UE per la data protection?

Corradino Corradi. *È sicuramente una sfida importante: le grandi aziende sono già partite e hanno stanziato investimenti significativi, perché il regolamento è complesso e richiede un cambio di passo soprattutto per gli aspetti di risk processing e delle contromisure da mettere in piedi. Anche la 'data breach notification' è una novità rilevante. Nelle Telco c'era già, per altri settori invece richiede la revisione delle procedure di 'detection' e 'incident management' per riuscire a stare entro le 72 ore.*

TIG. Quale sarà in futuro il ruolo del CISO?

Corradino Corradi. *Il CISO deve essere sempre più vicino al business e, insieme al CSO o al Chief Digital officer, un ambasciatore della trasformazione digitale. Solo che mentre le altre due figure portano in azienda gli aspetti positivi del digitale, come l'impatto sulla esperienza del cliente e i nuovi ricavi da modelli di business più agili e vicini ai clienti, il CISO ha invece il compito di sottolineare i rischi di sicurezza e spingere per la protezione dei dati come elemento di differenziazione. Deve però dotarsi di un linguaggio non solo tecnico, in modo da poter comunicare al meglio con il Board. Il CISO sarà quindi in futuro una figura sempre più importante, e le Università dovranno attrezzarsi maggiormente perché si tratta di competenze molto ricercate e sempre più difficili da trovare.*

DA: L'AGENDA DEL CISO PER IL 2018, 14 DICEMBRE 2017
(http://channels.theinnovationgroup.it/cybersecurity/lagenda-del-ciso-2018/)

Se questo è a grandi linee "quello che il CISO dovrebbe essere e fare", vediamo in base alle risposte ottenute con la Cyber Risk Management 2018 survey qual è oggi la situazione dei Security Manager/CISO italiani, in un campione di aziende medio grandi con piani già molto estesi per la cybersecurity. Come mostra la figura successiva, le problematiche più urgenti che un responsabile della Cybersecurity si trova ad affrontare sono numerose.

Analizzando le prime due risposte ("*Comunicare meglio al Board*" e "*Allineare meglio cybersecurity al business*") vediamo che le criticità oggi maggiori risiedono non tanto nell'area della Security, quanto piuttosto nella sua relazione con il resto dell'organizzazione che le sta intorno.

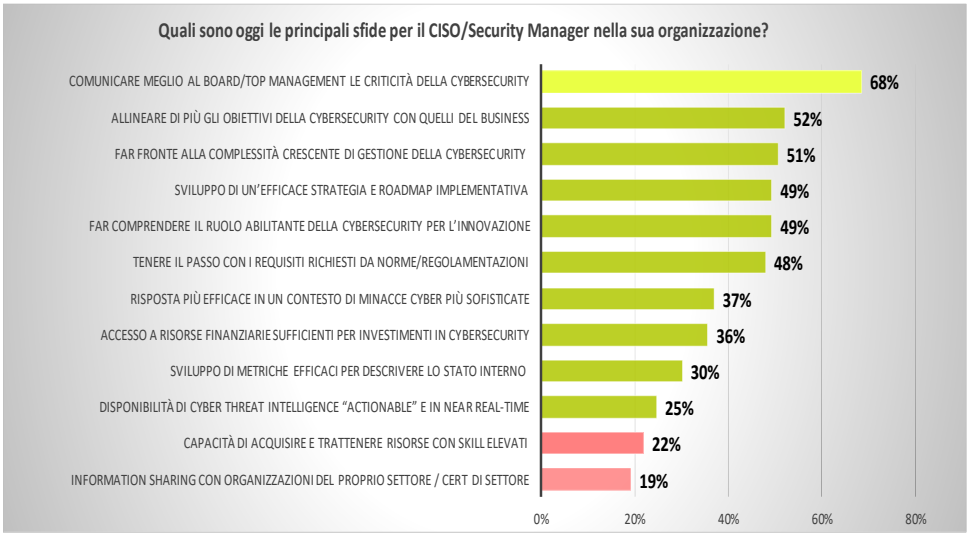

FIGURA 8 – QUALI SONO OGGI LE PRINCIPALI SFIDE PER IL CISO

Il primo problema di un CISO (68% delle risposte) è quindi come rendere partecipe e ingaggiare il top management/il Board dell'azienda comunicandogli nel modo più efficace possibile le criticità della cybersecurity che lui vede, ma che il resto del business non conosce (data la rilevanza del tema, abbiamo dedicato una parte della survey proprio a "scandagliare" questo aspetto: come impostare misurazione e reporting al Board).

Il secondo problema, indicato dal 52% dei rispondenti, è invece allineare meglio gli obiettivi della cybersecurity a quelli del business. Molti responsabili della security oggi si pongono infatti il problema su quale sia il livello di sicurezza ideale per la propria realtà. Se sarà eccessivo, probabilmente comporterà una serie di misure pesanti, per i dipendenti, per i clienti, misure che potrebbero anche peggiorare la user experience e condizionare la competitività dei prodotti o servizi dell'azienda. Proibire la navigazione o l'utilizzo di device mobile ai dipendenti non favorisce di certo la crescita e l'innovazione in azienda. Se i sistemi sono bloccati, le informazioni critiche messe sotto custodia; se devo imporre procedure e training ogni qualvolta incremento le misure di sicurezza; è probabile che le ricadute in termini di produttività e agilità del business saranno pesanti.

Come bilanciare quindi al meglio sicurezza e obiettivi del business? In molte realtà ci si pone questo problema e le soluzioni sono spesso diverse: si tratta sostanzialmente di impostare una corretta governance, come approfondiremo nel capitolo successivo.

Ulteriori considerazioni che possono essere dedotte da questa domanda sono:

- **Far fronte alla complessità crescente di gestione della cybersecurity**. È un problema per oltre la metà dei rispondenti, ed è evidente che non farà altro che peggiorare in futuro, via via che le aziende si esporranno in nuovi ambiti dell'innovazione digitale. È un tema legato alla mancanza di competenze e risorse nell'ambito della security, che può essere affrontato soltanto se si lavora in un'ottica di PROGRESSIVA AUTOMAZIONE di un numero sempre maggiore di task dell'IT e della security, in modo da lasciare il tempo alle risorse di concentrarsi sulle attività più critiche o a maggiore valore aggiunto. Ancora oggi moltissime attività IT, pensiamo al patching, all'e-commerce, alla gestione del cliente, sono svolte in modo manuale. Oltre a comportare maggiori rischi di errore, le attività manuali sono un collo di bottiglia: ad esempio, quando viene completato un vulnerability scan, passa moltissimo tempo prima che tutti i problemi identificati ricevano il rispettivo fix – un tempo che gli attaccanti conoscono bene, perché sfruttano queste "finestre temporali" per completare con successo le proprie azioni.
- **Sviluppo di un'efficace strategia e roadmap implementativa** (49% delle risposte), **Risposta più efficace in un contesto di minacce cyber più sofisticate** (37%), **Sviluppo di metriche efficaci per descrivere lo stato interno** (30%). Queste risposte sono da ricondurre alla necessità di dotarsi di un disegno e di un programma efficace di cyber risk management. Fanno riferimento alla difficoltà soprattutto di aziende di alcuni settori (meno toccati rispetto ad altri da regolamentazioni) di individuare i processi, le metodologie e le best practice specifiche per la propria realtà. Un supporto dovrebbe venire da un maggiore coinvolgimento delle istituzioni a livello nazionale su queste tematiche.
- "**Tenere il passo con i requisiti richiesti da norme/regolamentazioni**" è avvertito come una priorità del Security Manager dal 48% delle aziende – conseguenza di un numero sempre maggiore di norme che hanno e avranno impatto sulla cybersecurity – ma un numero altrettanto elevato di aziende (49%) ritiene anche che "**Far comprendere il ruolo abilitante della cybersecurity per l'innovazione**" sia oggi un compito critico del CISO.
- L'accesso a **risorse finanziarie sufficienti per investimenti in cybersecurity** è un problema solo per circa un terzo delle aziende intervistate – segnale che dove oggi l'approccio al cyber risk management è già avanzato, l'accesso ai budget non è più il primo problema di un security manager.
- "**Disponibilità di cyber threat intelligence "actionable" e in near real-time**" e "**Information sharing con organizzazioni del proprio settore / CERT di settore**" sono invece indicati come aspetti prioritari solo da una minoranza di organizzazioni. Segnale che su questi aspetti solo poche aziende sono oggi sufficientemente pronte: li considerano ancora una sfida per il medio lungo termine, non di immediata rilevanza.

Il problema è che per ottenere molte delle soluzioni che i Security Manager e i CISO oggi ricercano (dal miglior collegamento con il top management e con la strategia aziendale, all'evoluzione della sicurezza verso una funzione perfettamente allineata con i reali bisogni dell'azienda) serve innanzi tutto un cambio di passo su un aspetto fondamentale: la cultura della sicurezza nella propria organizzazione e fuori da essa. Fintantoché – come mostra anche la seguente figura – la sicurezza informatica sarà percepita più come un costo che non come un elemento che abilita l'innovazione e la trasformazione del business in chiave digitale, sarà molto difficile trovare una soluzione a tutti i problemi che oggi ancora limitano il potenziale valore della sicurezza.

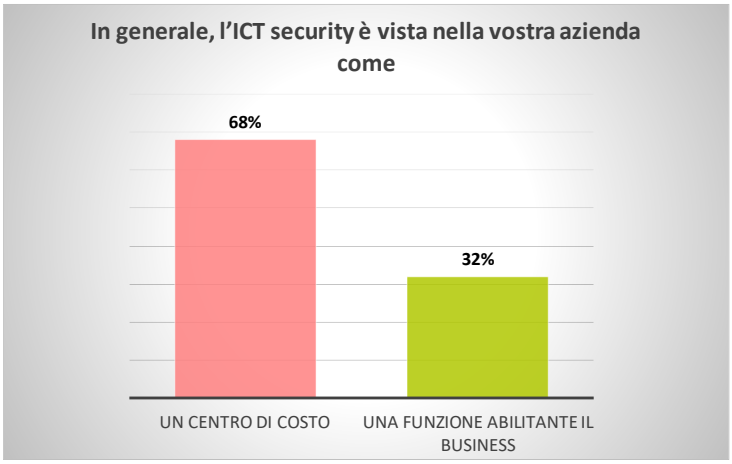

FIGURA 9 – LA SICUREZZA È ANCORA PERCEPITA PIÙ COME UN COSTO CHE COME UN BENEFICIO

Information Security Governance

È in generale compito della Governance quello di fornire una direzione e un monitoraggio sui progressi fatti verso una determinata meta prefissata. In situazioni complesse, come sono appunto quelle nelle grandi organizzazioni, la Governance è un'attività fondamentale e molto diversificata. Comprende: fissare degli obiettivi; assegnare delle responsabilità e dei ruoli; stabilire delle strutture e dei processi; implementare tutto il disegno, misurarne gli outcome e quindi verificare continuativamente se sono necessari degli aggiustamenti.

Tutto questo discorso si applica perfettamente alll'ICT security governance e/o cybersecurity governance. Il successo di una specifica struttura di governance dipenderà da molti fattori: dalle competenze dei suoi manager, dai flussi informativi che la permeano, dal tipo di relazioni instaurato. Non esiste una mappa organizzativa universale: ogni possibile scelta ha i suoi pro e i suoi contro, e come vedremo, ogni organizzazione normalmente fa una scelta diversa dalle altre.

Considerando i modelli organizzativi per l'ICT Security Governance che si sono date le aziende del campione analizzato (Figura 10), abbiamo tratto le seguenti conclusioni:

- Nella maggior parte delle aziende prevale ancora un disegno organizzativo tradizionale, in cui il manager della sicurezza informatica riporta al Chief Information Officer (42% delle risposte). È comunque una percentuale inferiore a quella che avevamo misurato nel 2015, quando la percentuale delle aziende sul campione analizzato, con questo tipo di modello, arrivava al 67%.

- Il motivo per cui sta diminuendo questo tipo di disegno organizzativo è legato al fatto che in molti più casi la security riporta oggi o direttamente al CEO/board (39% delle risposte), o invece ad altre funzioni, come ad esempio, al Chief Operating Officer (COO, 4%), al Chief Financial Officer (CFO, 6%), al Capo Risorse Umane (HRO, 3%).
- Per una percentuale ancora limitata di aziende (6%) il responsabile della sicurezza informatica è sotto al Chief Security Officer, quindi parte della Corporate Security, segnale della forte rilevanza che viene data a questi temi.

«A chi riporta il CISO, o il ruolo equivalente responsabile per la cybersecurity?»

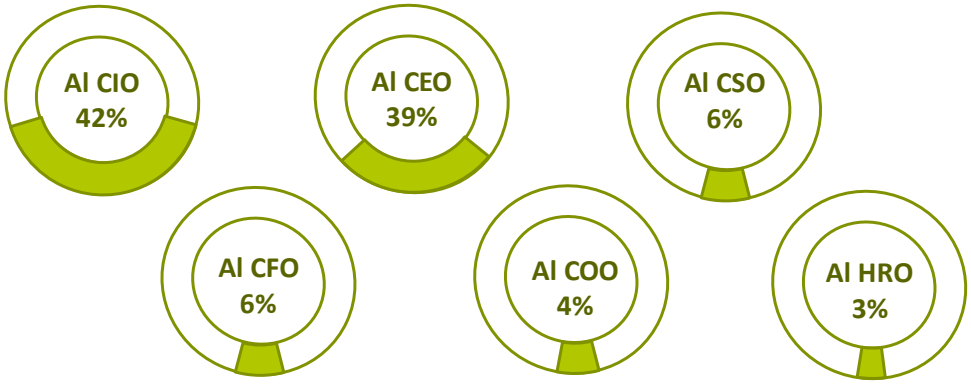

FIGURA 10 – DISEGNO ORGANIZZATIVO PER LA CYBERSECURITY: A CHI RIPORTA IL CISO/SECURITY MANAGER

Inoltre, si osservano anche molti casi (in tutto 9 aziende nella nostra analisi, come mostra la Figura 11) in cui la scelta è stata di tipo matriciale, per cui il responsabile della sicurezza riporta non a una sola funzione ma a più di una, e tipicamente vengono inclusi manager di altre funzioni come appunto COO, CFO, HRO.

Questo tipo di scelta, che porta a un disegno matriciale, è un trend in crescita legato soprattutto all'incremento della complessità organizzativa nelle aziende. Dipende dal riconoscimento di una responsabilità di altro tipo, più strategica, legata al rischio, alle risorse umane, al CFO (soprattutto dove questo ruolo è un vicedirettore che si occupa di governance), al COO quando l'interesse principale è legato all'operatività dei sistemi.

In 10 casi poi l'ICT Security non è più all'interno dell'IT, ma in una divisione dedicata o nella Corporate Security. Il vantaggio di questo tipo di organizzazione è che rende possibile svincolare le scelte e gli investimenti in sicurezza da quelli strettamente tecnologici e di processo ICT, collegandoli maggiormente ad altre esigenze (che variano da caso a caso) e in generale alla strategia complessiva dell'azienda. Inoltre garantisce una migliore segregazione delle responsabilità che è funzionale a un maggiore controllo del rischio cyber.

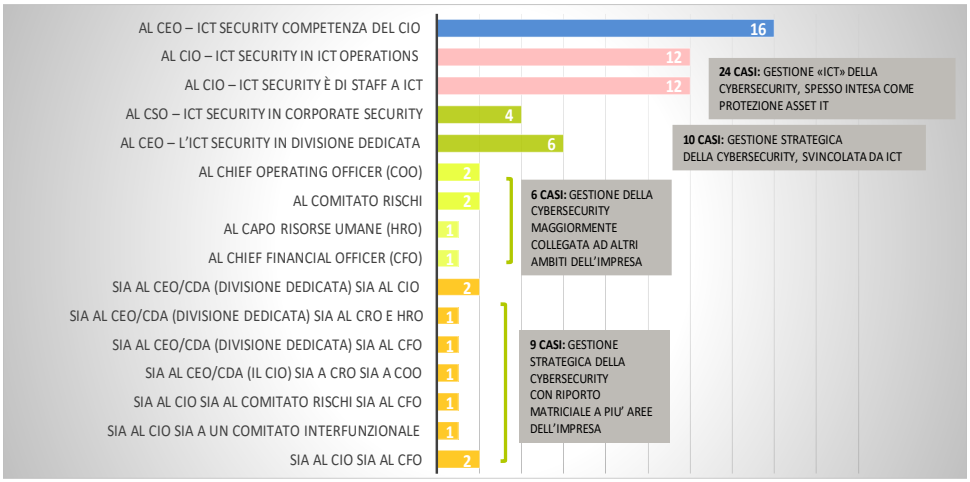

FIGURA 11 – DISEGNO ORGANIZZATIVO PER LA CYBERSECURITY: VISIONE COMPLETA

Intervista a Stefano Scoccianti, Enterprise Risk Manager di Hera.

TIG. Quale modello di cyber risk management avete adottato in Gruppo Hera, e come si sposa con il vostro Enterprise Risk Management?

Scoccianti Stefano*. Il nostro ERM e più in generale le attività di valutazione e controllo dei rischi rispondono anzitutto al principio di segregation of duties, garantendo la distinzione tra le responsabilità operative e le responsabilità di controllo/compliance: le seconde sono allocate a strutture di controllo di secondo livello, il cui compito è di fornire a tutte le funzioni e business unit aziendali un'impostazione e approccio coerenti e regole di controllo dei rischi omogenee per tipologia di rischio, adottando metodologie standard in modo da uniformare l'approccio. Rientrano in questo disegno dei controlli di secondo livello tutte le attività connesse alla compliance, sia obbligatoria (secondo le norme generali e di settore), sia per le certificazioni di qualità, così come l'approccio strutturato all'analisi e gestione dei rischio. Esiste infine un controllo di terzo livello, l'Internal Audit, per verificare che i processi implementati siano adeguati ed efficaci per consentire il raggiungimento degli obiettivi aziendali.*

Parlando di cyber risk, la metodologia di valutazione adottata è quella che segue l'approccio Magerit, riconosciuto dall'ENISA (European Union Agency for Network and Information Security), e serve a seguire obiettivi di gestione dei rischi ICT (integrità, disponibilità, riservatezza) valutando il livello di vulnerabilità di tutti gli asset ICT aziendali, tramite una visibilità puntuale su applicativi, sistemi, dati, infrastrutture, software.

Gli obiettivi di resilienza sono declinati per ciascuna delle filiere aziendali e dei principali processi aziendali, e quindi, per dare seguito alle opportune azioni di mitigazione dei rischi e implementare i più efficaci criteri di resilienza, vengono definite policy e istruzioni operative, redatte dal Presidio Sicurezza Logica e Privacy, indirizzando anche le scelte tecnologiche di alto livello sui sistemi di sicurezza.

Ulteriori indicazioni sono poi quelle rivolte a processi e risorse umane, limitando comportamenti a rischio e definendo regole stringenti ad esempio relative alle attività di gestione ed intervento sulle macchine, che sono eseguiti sotto la supervisione della Direzione Sistemi Informativi. La Direzione Servizi Informativi è incaricata di mettere in atto le contromisure di difesa dal rischio cyber, con tempistiche e piani di intervento precisi. Molteplici sono le soluzioni e gli strumenti di sicurezza adottati. Tuttavia occorre fare in modo che essi siano utilizzati in modo ottimale. Limitarsi alla loro implementazione non basta: devono anche essere efficacemente gestiti ed essere oggetto di costante attività di monitoraggio e controllo, altrimenti probabilmente rimarranno sottoutilizzati. Le iniziative che abbiamo in corso sono tante, ma l'importante è seguire questa logica: a partire dalle indicazioni dei responsabili del controllo rischi, i responsabili dell'ICT si focalizzano sulle migliori soluzioni tecnologiche e procedono alle attività di implementazione e gestione.

TIG. Quali sono i vantaggi della struttura di controllo che avete adottato?
Scoccianti Stefano. *I vantaggi di questo disegno sono molteplici. Avendo affidato il controllo a una struttura terza rispetto a chi implementa le soluzioni e le gestisce, l'attività sarà più efficace in quanto non immediatamente condizionata da comprensibili esigenze contingenti: il disegno cercherà comunque di traguardare obiettivi sfidanti pur contemperati dai vincoli operativi di natura gestionale ed economica. Inoltre, c'è un tema di specializzazione, perché il controllo è dato a figure che dispongono della corretta "strumentazione" di valutazione dei rischi, e non è detto che sia una competenza nelle disponibilità dei gestori dell'esercizio.*
Terzo vantaggio e forse il più rilevante dal punto di vista organizzativo: le problematiche di sicurezza logica sono oggi trasversali a più ambienti, riguardano anche sistemi informatici utilizzati a supporto della gestione di reti energetiche e gas, sistemi di telecontrollo del ciclo idrico o della produzione e distribuzione di energia elettrica: sono attività non sempre riconducili al mondo ICT tradizionale, spesso fanno capo ad altre aree aziendali. Figure al di sopra delle parti ed approcci di Segregation of duties permettono di garantire l'intervento anche in questi ambiti.

DA: DYNAMIC CYBER RISK MANAGEMENT NELLA PROSPETTIVA ERM NEL GRUPPO HERA,
30 NOVEMBRE 2017 (http://channels.theinnovationgroup.it/cybersecurity/dynamic-cyber-risk-erm-hera/)

Cybersecurity Governance: il modello da adottare secondo FERMA e ECIIA

Al giorno d'oggi la Cybersecurity non può più essere responsabilità solo dell'ICT. Per arrivare al coinvolgimento del top management, per avere il supporto di tutte le business unit, per farla diventare "parte integrante della cultura" dell'intera organizzazione, la Cybersecurity ha bisogno di un chiaro modello di Corporate Governance.

Sempre di più la capacità di gestire i rischi cyber con lo stesso livello di confidenza con cui sono gestiti tutti gli altri rischi dell'impresa, diventa oggi un vantaggio competitivo, un elemento differenziante per chi è in grado di comunicare ai propri stakeholder, ai clienti, al mercato, di avere adottato il miglior modello possibile di Cyber risk management, in risposta alle sfide oggi derivanti dal cambiamento tecnologico (la digitalizzazione sempre più pervasiva, il cloud); dall'evoluzione del comportamento delle persone (mobile, social); dalla facilità di accesso e trasformazione di grandi quantità di informazioni (Big Data, AI).

Qual è allora il miglior modello di governance dei rischi cyber nel nuovo contesto digitale?

Una chiara posizione è quella presa dal gruppo di lavoro misto a livello europeo, costituito da Risk Manager afferenti all'Associazione FERMA (www.ferma.eu) e da Internal Auditor della ECIIA (www.eciia.eu) di 8 diversi paesi europei e di 6 settori economici (banca, trasporti, difesa, IT, alimentare e telecomunicazioni). Il risultato del lavoro congiunto è il Report "**At the junction of corporate governance and cybersecurity**"che propone un modello ben preciso (in sintesi nella figura sotto) per organizzare internamente la gestione del rischio informatico, con l'obiettivo di aumentare la resilienza e l'efficienza delle aziende.

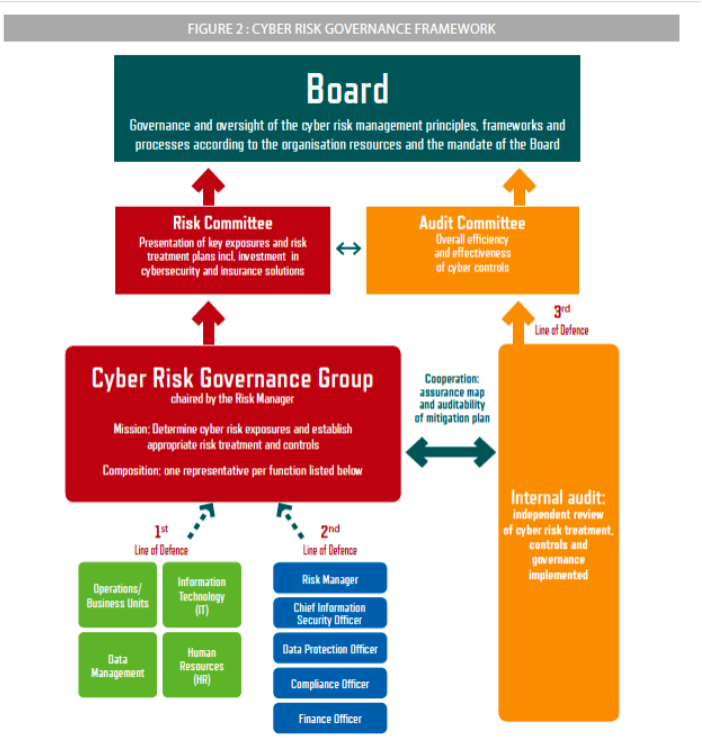

FIGURA 12 – CYBER RISK GOVERNANCE FRAMEWORK, FERMA ECIIA, LUGLIO 2017

Il modello proposto parte da 8 principi generali di cyber governance, quelli proposti dal World Economic Forum con la pubblicazione di gennaio 2017 *"Advancing Cyber Resilience: Principles and Tools for Boards"*. Questi sono:

- La creazione di una cultura sul cyber risk investendo sulla formazione del personale,
- L'identificazione dei risk owners in modo che la responsabilità sia chiaramente riconducibile a una precisa funzione,
- L'attenzione alla compliance e al rispetto delle norme;
- L'importanza della cooperazione, sia tra le aziende sia tra il settore privato e le istituzioni pubbliche;
- I risk assessment per verificare il proprio stato di esposizione;
- Le misure di sicurezza;
- L'innovazione;
- La preparazione, resilienza e capacità di preservare la continuità del business.

Quale modello per la corporate governance della cybersecurity? Come riportato nel report FERMA – ECIIA, la governance viene strutturata su tre linee di difesa.

La prima ha il compito di implementare quanto possibile per mitigare i rischi: dalle polizze assicurative alle misure tecniche, con la responsabilità sull'operatività quotidiana di prevenzione, controllo, risposta in caso di incidente: ne fanno parte il settore IT, le risorse umane, il Chief Data Officer e le Operations/Business Units. La seconda linea di difesa è responsabile dei processi che portano a monitorare e facilitare l'implementazione di

buone pratiche in prima linea: è tipicamente il ruolo del CISO (Chief Information Security Officer), che definisce le polizze e gli standard tecnici che esse devono soddisfare; monitora inoltre l'operato della prima linea, e controlla che l'esposizione al rischio informatico sia in linea con il risk appetite dell'impresa. La terza e ultima linea è formata dall'Internal Audit, che supervisiona l'operato delle prime due linee e controlla la coerenza dell'intero processo di cyber risk governance, oltre a fornire un reporting periodico al Board.

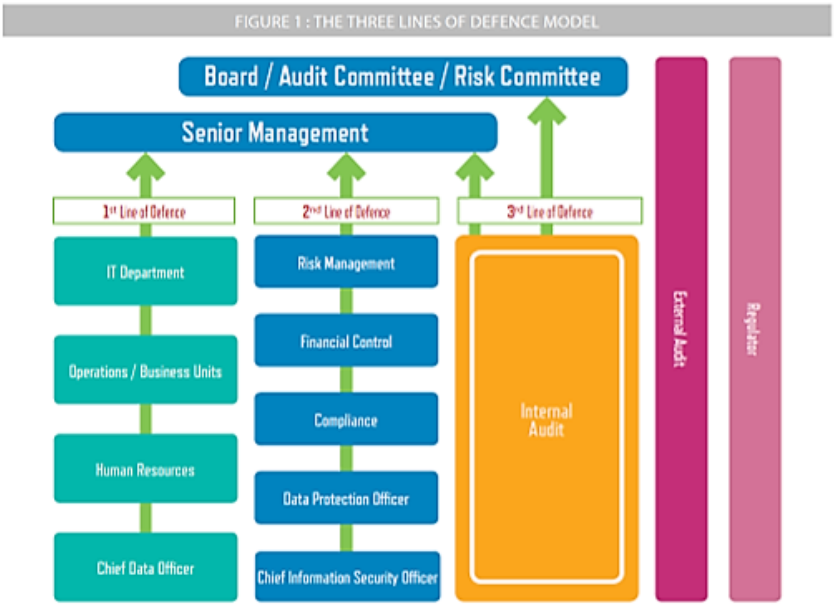

FIGURA 13 – LE 3 LINEE DI DIFESA DEL CYBER RISK GOVERNANCE FRAMEWORK, FERMA ECIIA, LUGLIO 2017

Misurazione e Reporting al CEO/Board

Misurare, misurare, misurare …. e comunicare al Board. Dovrebbero essere queste le nuove leve che il Security Manager può utilizzare il più possibile per rendere più consapevole dei rischi la sua azienda, e in particolar modo più committed il suo management.

Eppure, così non è stato finora. Oggi però siamo di fronte a una discontinuità, a fatti macroscopici come è successo nel 2017 con due eventi "black swan", imprevedibili e molto pericolosi, di cui anche il largo pubblico è stato questa volta a conoscenza: gli attacchi WannaCry e NotPetya. In entrambi i casi, il ransomware non si è limitato a crittografare dati e a chiedere somme di denaro in cambio per il riscatto dei dati, ma ha avuto conseguenze distruttive e ha comportato disservizi anche gravi, come nel caso del sistema sanitario inglese e di una multinazionale della logistica, l'operatore Maersk, che per colpa dell'attacco NotPetya ha subito perdite da mancata operatività (per un paio di settimane in tutta Europa) tra i 200 e i 300 milioni di dollari[5].

[5] NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million, AUG 16, 2017, Forbes

Con questi fatti ben noti in mente, abbiamo chiesto agli intervistati della survey se i due ransomware hanno comportato modifiche dirette nella loro organizzazione. Come si osserva dalle risposte, il risultato è che forse qualcosa sta cambiando.

- Nuovi controlli di sicurezza ICT: hanno risposto di Sì nel 42% dei casi
- Nuove modalità per comunicare gli incidenti al Board: hanno risposto di Sì nel 44% dei casi.

La percentuale non è altissima ma sta a indicare un trend di presa di coscienza molto importante (legato proprio a fatti notevoli come è stata la diffusione dei due ransomware tra maggio e luglio 2017), che comporta cambiamenti anche rilevanti, sia in processi e misure interne per la cybersecurity, sia anche nel modo di comunicare questi rischi verso l'alta direzione.

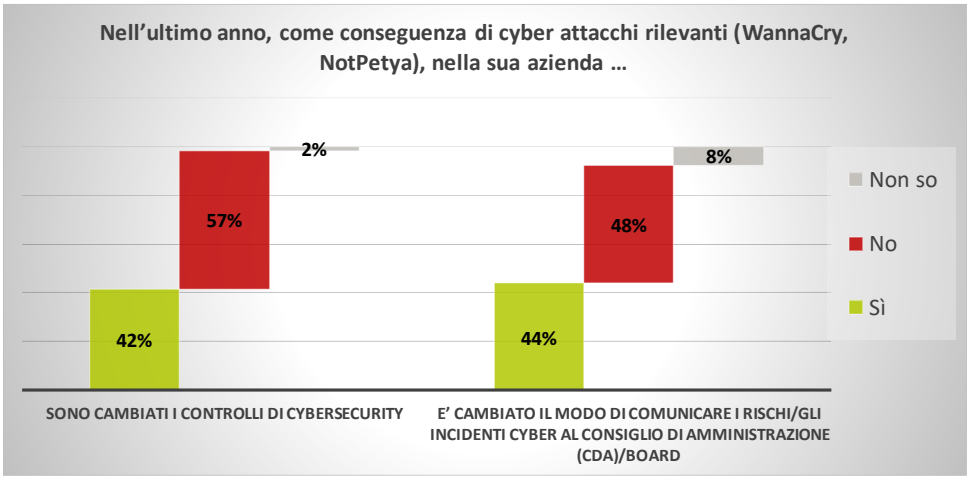

FIGURA 14 – WANNACRY E NOTPETYA: PRESA DI COSCIENZA DELLA NECESSITÀ DI INTRODURRE NUOVI CONTROLLI E COMUNICARE MEGLIO IL RISCHIO

Ma in generale si può dire che il management delle aziende è sufficientemente coinvolto in tema di cyber risk? O bisognerebbe invece incrementare i momenti di incontro e dibattito?

Secondo le risposte fornite dal campione analizzato, riportate nella Figura successiva, in questo momento nel 70% dei casi il responsabile della sicurezza partecipa ad incontri con il CEO/ Board "MAI o QUASI MAI". Questo risultato sta a indicare che probabilmente, in molte organizzazioni, il top management non è coinvolto a sufficienza, e non è quindi in grado di valutare l'impatto potenziale del cyber threat perché inconsapevole del rischio, della situazione della sua azienda, delle potenziali conseguenze negative.

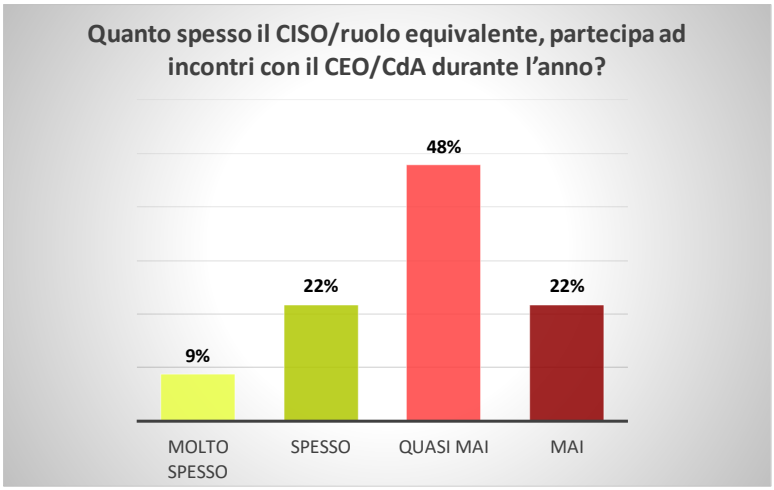

FIGURA 15 – SPESSO IL CEO/BOARD NON È CONSAPEVOLE DEL RISCHIO CYBER

Una migliore comunicazione con il top management è sicuramente un obiettivo del moderno resposabile della sicurezza, che dovrebbe basare la comprensione della reale esposizione dell'azienda ai rischi cyber su una misurazione il più possibile quantitativa del rischio. Molto lavoro andrebbe quindi fatto per rendere più efficace il reporting relativo alla security. Anche in questo senso la situazione non è ottimale: la mancanza di metriche precise, di una misurazione anche economica del rischio (come riporta la figura successiva, e come discusso anche nella successiva intervista con Marcello Fausti, VP IT Security Engineering & Application Management di TIM) non aiuta i decisori aziendali a prendere in considerazione le misure più opportune.

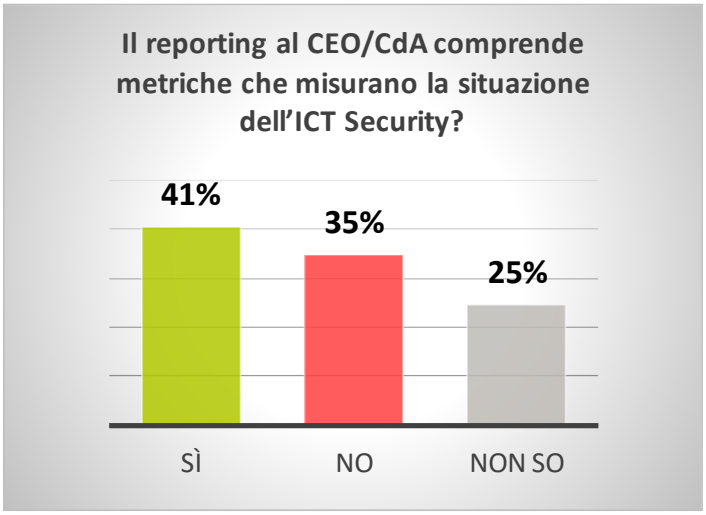

FIGURA 16 – UN SISTEMA DECISIONALE EFFICACE ANDREBBE BASATO SU UNA MISURAZIONE PIÙ QUANTITATIVA DEL FENOMENO

Il tema della misurazione e del reporting non può prescindere naturalmente dalla scelta dei corretti KPI (Figura 17): secondo i rispondenti alla survey, le metriche dovrebbero innanzi tutto riportare numeri relativi agli incidenti con perdita di dati subiti dall'azienda; a seguire, una misurazione sull'efficacia stessa dei controlli instaurati in azienda (nell'ottica del miglioramento continuo del piano di cyber risk management). Altre informazioni utili da riportare al Board/al top management sono i tempi collegati a

eventuali downtime dei sistemi; la numerosità dei tentativi di attacco subiti dall'azienda; eventi da ricollegare alle negligenze dei dipendenti e le vulnerabilità individuate e risolte. Agli ultimi posti figurano indicatori come il controllo sull'utilizzo del budget, o i risultati di test che misurino le capacità di risposta. Un suggerimento indicato invece da un rispondente è quello di includere nel reporting anche i benchmark di settore, in modo da poter misurare la Security Posture della singola azienda rispetto ai suoi concorrenti.

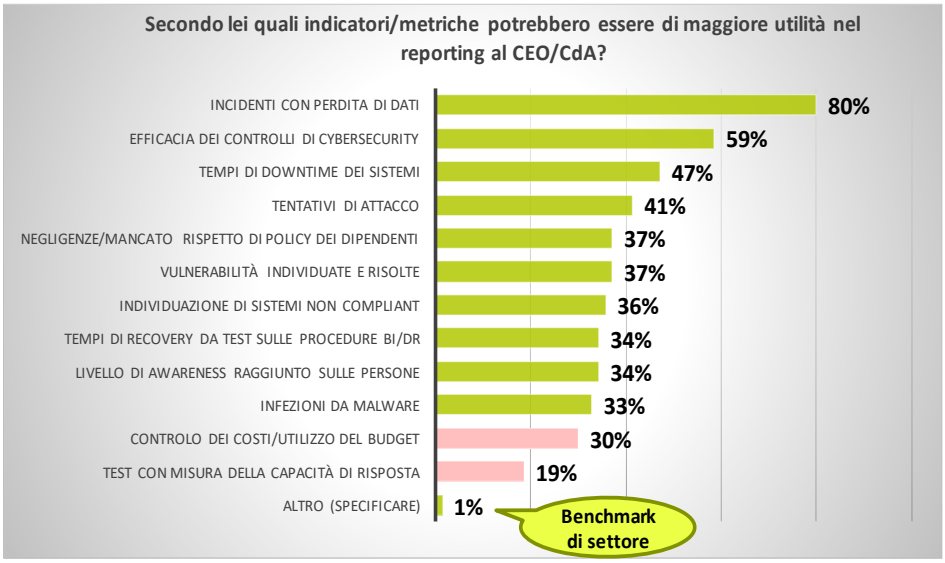

FIGURA 17 – QUALI SONO I KPI OTTIMALI PER IL CYBERSECURITY REPORTING

Intervista a Marcello Fausti, VP IT Security Engineering & Application Management presso TIM

TIG. Quali sono dal suo punto di vista le priorità di un Responsabile della Sicurezza ICT di una grande organizzazione, considerando l'evoluzione molto rapida con cui si è sviluppato negli ultimi anni il tema dei rischi cyber?
Marcello Fausti. *Credo che per poter arrivare a definire delle priorità di intervento sia necessario approfondire tre aspetti del problema cyber che richiederebbero una maggiore focalizzazione. Il primo tema è quello dei numeri e della dimensione del fenomeno cyber. Il secondo tema riguarda il concetto di rischio e la sua valorizzazione. Il terzo tema, in parte conseguenza dei primi due, riguarda la scelta del migliore approccio da seguire per mettere a punto un piano di intervento sul tema cyber. Guardiamo innanzi tutto al primo problema: tutti noi partecipiamo spesso a convegni, seminari, gruppi di studio, nei quali emerge netta e ampiamente condivisa la sensazione di gravità e urgenza del rischio cyber. Ora, pur senza voler in nessun modo sminuire o amplificare questo comune sentire, devo però registrare la perdurante mancanza di un sistema di rilevazione del fenomeno cyber che sia strutturato, condiviso e diffuso nei principali ambiti pubblici o privati che maggiormente impattano sulla vita delle persone (e.g.: PA, Sanità, Infrastrutture Critiche, etc.). Mi riferisco ad un sistema di rilevazione che "obblighi" tutti i soggetti interessati a censire gli incidenti di sicurezza secondo tassonomie e semantiche definite a priori allo scopo di "costruire" una dimensione numerica condivisa del fenomeno cyber, indispensabile a qualsiasi processo di supporto alle decisioni di qualsiasi realtà pubblica o privata. Insomma, una sorta di Istat della cybersecurity che ci aiuti ad inquadrare meglio il fenomeno che, per sua natura, ha una dimensione di sistema che, dunque, non ci consente di attuare trattamenti esclusivamente relegati a livello di singola entità o comparto. Serve, quindi, un approccio olistico basato su una rappresentazione numerica certa del fenomeno.*

TIG. Oltre alle informazioni di base, quali sono le analisi e le metriche che andrebbero sviluppate per un corretto, scientifico, cyber risk management?
Marcello Fausti. *È evidente che la dimensione numerica del problema da sola non è sufficiente a supportare il processo decisionale. Riguardo agli incidenti di sicurezza, ad esempio, i numeri contano solo se supportati adeguatamente da dei significati che aiutino ad attuare una fase di triage avente l'obiettivo di individuare il più rapidamente possibile le due cose che è necessario sapere: priorità di gestione e impatto potenziale. Questo esempio introduce un tema importante (il secondo della mia classifica) che è quello della valutazione del rischio. È un dato di fatto che oggi nelle aziende vengono adottate metodologie e best practice che propongono una valutazione del rischio basata su scale di valori ordinali (es.; Alto, Medio, Basso o punteggi da 1 a 5) se non in base alla percentuale di copertura di requisiti derivanti da normative o (appunto) da best practice. Quest'approccio è figlio dell'idea che per essere protetti è necessario e sufficiente aderire ad una serie di raccomandazioni o di regole prescrittive (nel caso di normative cogenti) che vanno bene per tutti i contesti e per tutti i business. Pur se il perseguimento di comportamenti virtuosi (come l'attuazione di best practice) è certamente positivo e ha il non trascurabile effetto di dimostrare una certa buona volontà dell'ente o azienda che le adotta anche di fronte ad eventi cyber avversi, ciò non è sufficiente. Una valutazione accurata del rischio cyber non può che passare per la valutazione il più possibile accurata dell'impatto economico dell'evento cyber avverso (i.e. perdita di fatturato, costi di ripristino del servizio, costi per retention della clientela, etc.). La valutazione dell'impatto economico potenziale di un rischio cyber è una disciplina complessa che va fatta in collaborazione con i responsabili di business nell'ambito di un processo di calibrazione delle valutazioni che ha come effetto quello di avvicinare il linguaggio della cybersecurity al linguaggio del board. Oggi, invece, si parla molto di vulnerabilità, minacce, vettori di attacco e forse poco di rischio in termini economici.*

DA: LA CYBERSECURITY NELL'ERA DELL'INNOVAZIONE DIGITALE: QUAL È LA SFIDA DA VINCERE, 13 FEBBRAIO 2018 (http://channels.theinnovationgroup.it/cybersecurity/cybersecurity-era-innovazione-digitale/)

DATA PROTECTION E ADEGUAMENTO AL GDPR

Il Regolamento europeo sulla Data Protection (GDPR, General Data Protection Regulation), adottato nell'aprile 2016, sarà effettivo a partire dal prossimo 25 maggio 2018. Con il GDPR, la protezione dei dati personali diventa una priorità strategica per aziende che non vogliono incorrere in problemi legali ed alte sanzioni (nei casi più gravi, le aziende potranno subire sanzioni pecuniarie fino a 20 milioni di euro / se superiore, fino al 4% del fatturato mondiale totale annuo).

La novità più importante del GDPR è legata al fatto che i singoli individui e i loro diritti sono posti al centro della norma. Infatti, con il GDPR arrivano molti più diritti per gli interessati rispetto al passato: gli utenti avranno oltre al Diritto di Accesso ai propri dati, anche il Diritto all'Oblio (potranno richiedere di cancellare i dati); di Portabilità dei dati (per trasferirli da un titolare del trattamento ad un altro); diritto di Revocare il consenso a determinati trattamenti. Il consenso dato da minori è valido solo se hanno almeno 16 anni: dai 13 ai 16 deve essere dato da un genitore o da chi per lui.

Ogni cittadino residente in UE avrà quindi il diritto di conoscere e decidere come i suoi dati personali sono utilizzati, archiviati, protetti, trasferiti e cancellati. Dal punto di vista delle aziende, la compliance al GDPR è un percorso difficile, che richiede una visione olistica su tutte le attività di raccolta, utilizzo e sicurezza dei dati, per quantitativi enormi. Andranno infatti considerati come dati personali qualsiasi informazione che permetta di risalire ed identificare un individuo, direttamente o indirettamente. Quindi anche indirizzi IP e dati di geolocalizzazione andranno adeguatamente protetti e messi a disposizione solo di persone autorizzate al trattamento.

In conclusione, con la nuova norma europea si passa a considerare i dati personali come un asset di grande valore: questo, del resto, è quanto sta già avvenendo con i trend tecnologici in corso, dal cloud computing, ai big data all'IoT, tutti pensati nell'ottica di offrire ai singoli individui una pletora di servizi personalizzati, ma anche di strumenti volti a riconoscerli, profilarli, analizzarli sempre di più. L'arrivo del GDPR rappresenta una pietra miliare nel cambiamento in corso, e avrà un ruolo centrale nelle politiche di data protection delle aziende nei prossimi anni.

Con l'indagine ci siamo posti innanzi tutto l'obiettivo di conoscere meglio lo stato dell'arte della Data Protection nelle aziende italiane: vediamo alcuni risultati nelle prossime pagine.

Quali informazioni proteggere da eventuali data breach?

Come è stato mostrato all'inizio del report, oltre il 90% delle aziende ha esperienza di più di una minaccia cyber nel corso del 2017, e il numero di quelle che hanno effettivamente subito un danno all'integrità dei propri database è un non trascurabile 20% (Figura 4).

Le aziende sono consapevoli che alcune tipologie di informazioni richiederebbero maggiore attenzione: come riporta la Figura successiva, al primo posto vengono le credenziali con privilegi, seguite da credenziali generiche (Userid e password). La compromissione di questi dati serve infatti agli attaccanti per acquisire il diritto ad entrare nei sistemi e svolgere ulteriori azioni fraudolente.

Al terzo posto tra le informazioni più importanti da proteggere appaiono i dati personali dei clienti, segnale di una particolare attenzione ai requisiti della privacy.

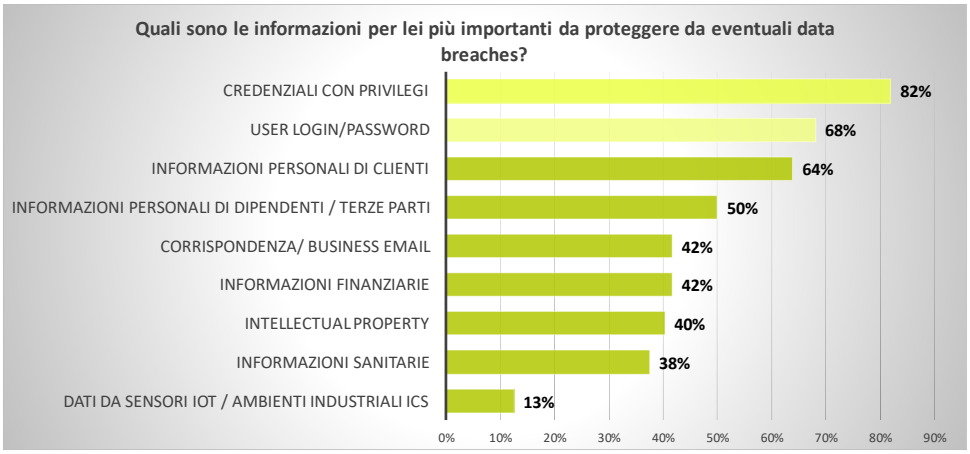

FIGURA 18. INFORMAZIONI PIÙ IMPORTANTI DA PROTEGGERE IN AZIENDA

Guardando poi alle risposte su dove risiedono attualmente i dati critici dell'azienda, a fronte di una risposta positiva con riferimento al backup, da segnale (in percentuali più basse) situazioni non proprio ideali come chiavette USB e Unmanaged endpoint.

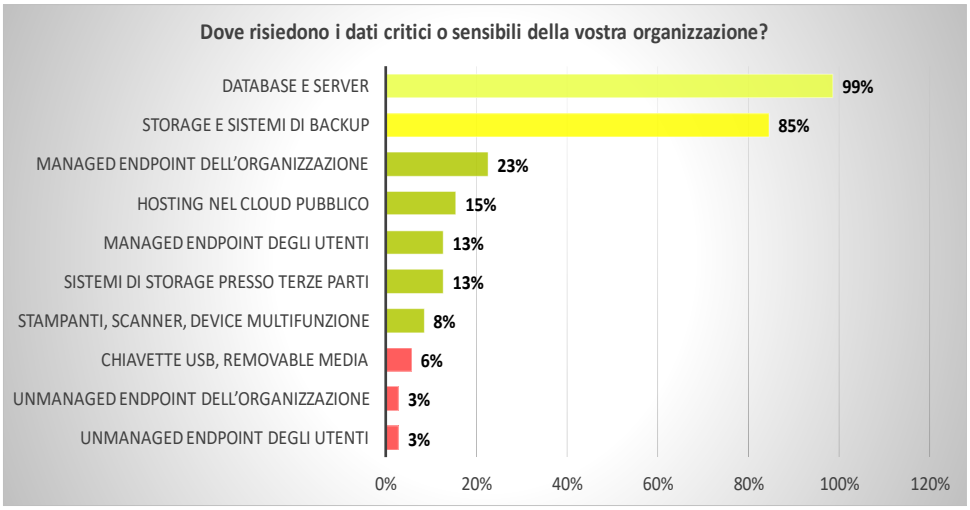

FIGURA 19. DOVE RISIEDONO I DATI CRITICI DELL'AZIENDA

Anche il fatto che i dati critici siano oggi posizionati in database e server non basta a posizionarli in perimetri protetti, in quanto molte di queste risorse possono già oggi essere migrate ad ambienti cloud, complicando così non poco le attività di compliance e le policy di data protection.

Considerando poi lo stato di adeguamento in corso al GDPR, come mostra la Figura successiva, se per alcuni ambiti (accountability framework, informativa e consensi) lo stato dei lavori è piuttosto avanzato, permangono ancora aspetti, in particolar modo

- Notifiche e gestione dei data breach
- Assegnazione del Data Protection Officer
- Trasferimenti di dati transfrontalieri

che richiedono ancora per molti di essere presi in considerazione.

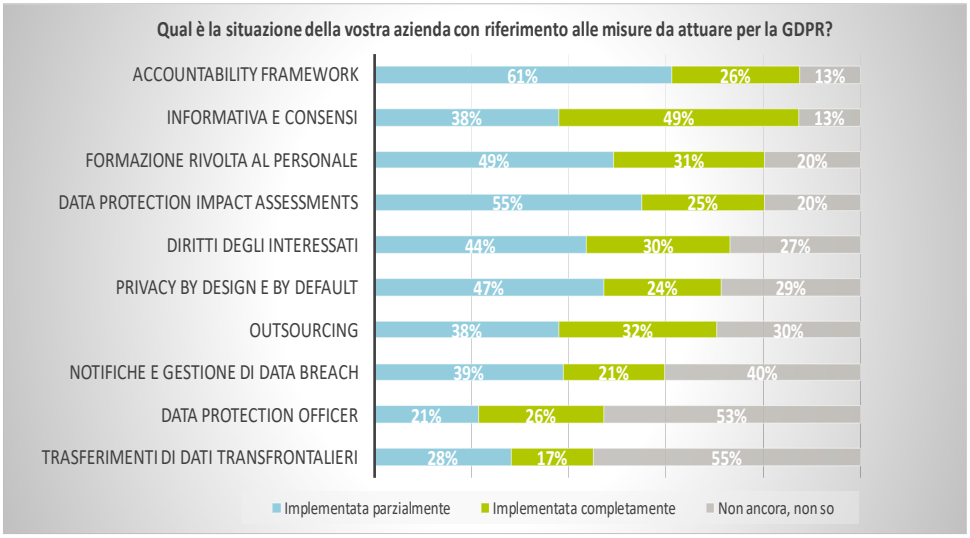

FIGURA 20. STATO DELL'ADEGUAMENTO IN CORSO AL GDPR (GENNAIO 2018)

Come affrontare il cambiamento indotto dal nuovo regolamento, tenendo presente che in futuro la mancata compliance al GDPR potrebbe essere un ulteriore grave rischio per le aziende, sia di tipo reputazionale sia anche economico a causa delle sanzioni più elevate?

Un approccio completo alla GDPR compliance deve comprendere i seguenti 4 aspetti:

CONOSCERE – GOVERNARE – PROTEGGERE – CONTROLLARE.

- CONOSCERE: il regolamento richiede espressamente alle aziende di essere consapevoli dei dati personali che trattano (quali dati sono, dove risiedono, chi vi accede, quali trattamenti sono fatti), dati che oggi rappresentano un asset di grande valore nella nuova economia digitale. Inoltre, il GDPR richiede che le aziende siano in grado di attestare questa conoscenza (accountability). Per questo motivo, considerando il fatto che non tutti dispongono di ampi piani di Data Governance e nella maggior parte dei casi i dati hanno negli ultimi anni pervaso sistemi di ogni tipo (backup, data warehouses, cluster Hadoop, NAS, cloud storage e quant'altro), sarà necessaria un'attività iniziale di investigazione e mappatura per risalire a dove risiedono tutte le informazioni. All'interno delle varie fonti dati, sarà anche importante capire in quali record sono memorizzati i dati personali, con quali rappresentazioni e campi descrittivi, o categorie. Tutta questa attività di ricognizione e classificazione andrà svolta con l'ausilio di tool dedicati.
- GOVERNARE: il nuovo Regolamento fornisce istruzioni precise su come tenere sotto controllo la situazione (pensiamo al registro dei trattamenti, alla DPIA). L'obiettivo è soprattutto quello di mantenere il sistema di governo dei dati personali constantemente allineato con quelle che sono le nuove esigenze di trattamento dei dati che arrivano dal business. La Data Governance diventa quindi un'attività obbligatoria per le aziende di qualsiasi settore e dimensione, non più un'esclusiva delle grandi organizzazioni o di alcuni ambiti (Finance, TLC).
- PROTEGGERE: la sicurezza del dato diventa prioritaria con la nuova norma EU, che ha la protezione anche nel suo nome (General Data Protection Regulation). Quali misure però utilizzare, sarà compito di ogni realtà deciderlo, in base ai suoi specifici bisogni. Tecniche che vengono indicate sono quelle crittografiche, di anonimizzazione e pseudoanonimizzazione, e tra i processi da considerare, anche quelli di cancellazione dei dati quando non sono più in uso (la policy di retention, che va anche comunicata agli interessati).
- CONTROLLARE: ultimo aspetto, ma non meno importante, il controllo o l'audit. Se non svolto internamente dall'azienda nell'ambito delle proprie procedure di controllo, potrebbe comunque essere richiesto dall'autorità Garante, che può chiedere al Titolare di dimostrare di aver predisposto tutte le opportune procedure, di avere una gestione dei dati conforme, di mantenere un registro con le attività svolte e di aver previsto e documentato in modo appropriato tutti gli aspetti, dalla richiesta di informazioni da parte degli utenti alla gestione delle notifiche in caso di data breach.

Considerando quindi questo necessario "percorso verso il GDPR", abbiamo indagato quali sono le attività che vedono oggi le aziende maggiormente coinvolte.

- Al primo posto, come era logico, gli aspetti di mappatura e inventario dei dati personali.
- La privacy-by-design e by-default è giustamente tra le attività più frequenti: infatti, deve essere incorporata in ogni progetto e/o nuovo sviluppo dell'azienda

che possa far uso di dati delle persone (pensiamo a un CRM, a una App consumer, al sito Web, ecc.).

- Segue la ricerca di soluzioni che possono aiutare l'azienda nel progetto di compliance, ad esempio relative agli aspetti di Data Governance & Protection.
- Quasi un'azienda su 2 sta poi analizzando il parco applicativo dell'organizzazione per individuare le soluzioni che utilizzano i dati personali.

Nel complesso però la figura ottenuta (per quanto riferita al periodo dicembre 2017 – gennaio 2018) conferma che molti dei lavori in corso riguardano ancora una minoranza di aziende, un segnale non molto positivo sullo stato di avanzamento della GDPR compliance nelle aziende italiane.

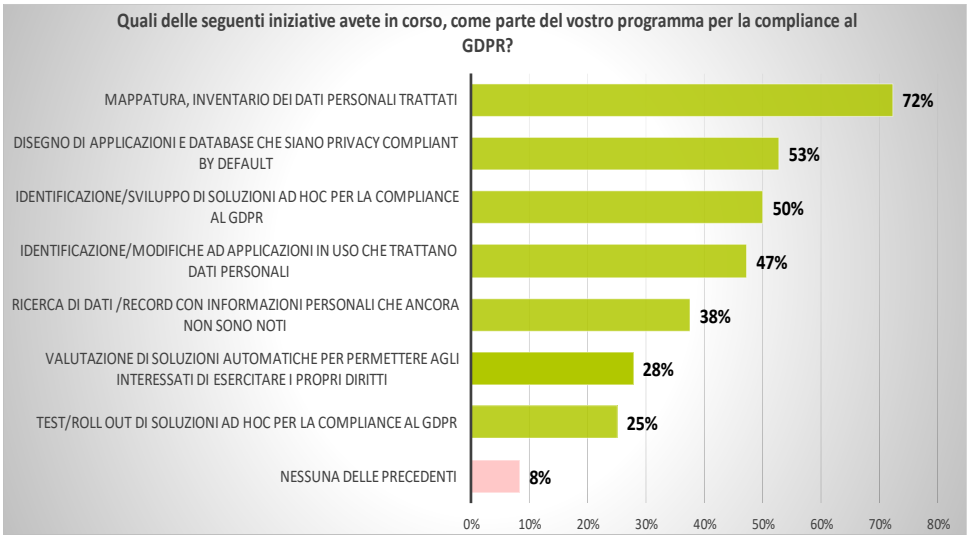

FIGURA 21. PRINCIPALI INIZIATIVE IN CORSO PER L'ADEGUAMENTO AL GDPR (GENNAIO 2018)

MISURE E PROCESSI PER LA SUPPLY CHAIN SECURITY

In un mondo sempre più globale e interconnesso, molti processi del business sono condivisi dalle aziende con la propria supply chain, fatta di terze parti come fornitori di prodotti, provider di servizi, distributori, contractor. Per la propria stessa sopravvivenza, le aziende si affidano a questi attori acquistando prodotti essenziali (come materie prime e semi-lavorati) o servizi indispensabili per la stessa continuità operativa (servizi di rete, software-as-a-service, cloud storage). Oggi la dipendenza sempre più stretta dalla propria supply chain obbliga le aziende a doverne considerare il rischio associato, la possibilità che un errore o un malfunzionamento originato dalle terze parti abbia ripercussione gravi sul proprio business.

Il Cyber Risk della Supply Chain

Supply chain sempre più integrate facilitano la cooperazione tra le diverse parti, ma allo stesso tempo offrono maggiori opportunità al cyber crime di infiltrarsi per commettere i propri abusi. Le vulnerabilità originate dalla supply chain sono molteplici: in alcuni casi i

A Supply Chain security Program focuses on the potential risks associated with an organization's suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organization's customer environments, some of which may be sensitive in nature. (Combatting Cyber Risks in the Supply Chain, SANS Institute, 2015)

fornitori vengono dotati di credenziali per accedere a reti, dati e applicazioni del business, e quindi potenzialmente hanno la possibilità di diffondere malware o commettere infiltrazioni. Altre possibilità sono: un fornitore di software potrebbe aver subito un attacco cyber, il codice da lui prodotto potrebbe contenere del malware che sarebbe quindi distribuito a tutti i clienti. Oppure, le credenziali di un fornitore potrebbero essere state sottratte e riutilizzate da un hacker.

La Figura successiva riporta l'anatomia tipica di un data breach che coinvolge la supply chain.

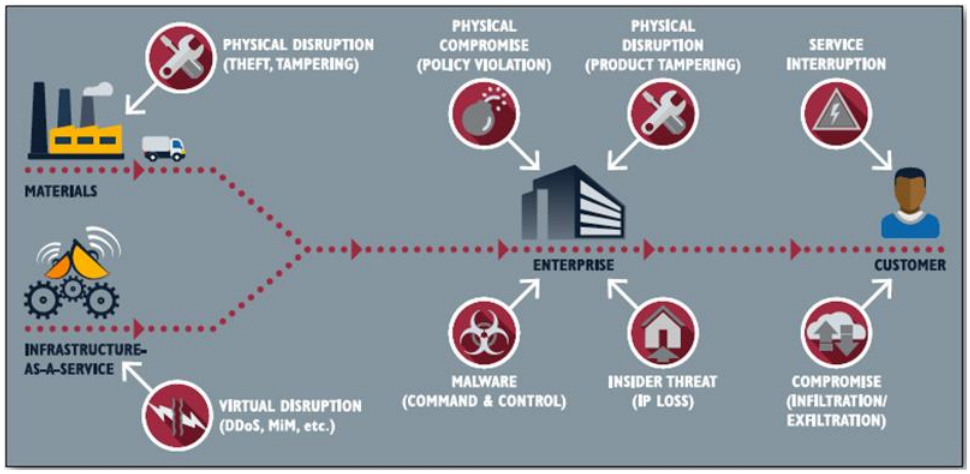

FIGURA 22. ANATOMIA DI UN BREACH ORIGINATO DALLA SUPPLY CHAIN (SANS INSTITUTE, 2015)

Negli ultimi anni molti dei data breach di più alto profilo, che hanno comportato perdite per milioni di dollari alle organizzazioni coinvolte, hanno visto un'origine proprio nella catena di fornitura. Il caso più celebre è quello della catena di vendita Target, che a fine 2013 ha scoperto un data breach di enorme dimensione, con perdita dei dati relativi a 110 milioni di clienti e 40 milioni di carte di pagamento. L'infiltrazione iniziale è stata possibile sfruttando la connessione alla rete dei negozi dei condizionatori dell'aria (HVAC) di una ditta esterna. Il furto delle credenziali per accedere alla rete ha aperto la porta agli hacker verso i database dei punti vendita, da cui per mesi sono state sottratte le informazioni sugli acquisti dei clienti.

Un caso più recente, che risale al settembre 2017, è quello di CCleaner, un software per desktop il cui compito è cancellare file temporanei e non più utili. Il programma è stato compromesso dagli hacker e quindi utilizzato per prendere di mira società di tecnologia e TLC che operano nella supply chain di aziende Fortune500.

Anche dopo il noto data breach avvenuto ad Equifax (società americana di credit reporting che ha subito il furto dei dati per 143 milioni di clienti) alcune società collegate, in particolare Visa e Mastercard, hanno dichiarato di aver subito furti di carte di credito dei propri clienti come conseguenza dell'attacco Equifax. Segnale che se viene colpito un attore di una catena del valore molto ampia e complessa, è prevedibile che a cascata ci siano conseguenze per le altre società collegate.

Secondo questo scenario, le aziende non possono più preoccuparsi di controllare i rischi cyber solo all'interno della propria organizzazione. L'integrazione e interconnessione delle supply chain comporta sia nuove opportunità, come comunicazioni in tempo reale,

maggiore efficienza e nuove sinergie, sia anche nuovi rischi. In termini di responsabilità, ad esempio per quanto riguarda il trattamento dei dati personali dei clienti, non ha importanza se questi sono compromessi presso un fornitore di hosting o cloud storage: è l'azienda che avendo ottenuto quei dati dai clienti, deve rispondere di un eventuale data breach.

Con riferimento alla Liability aziendale e alle responsabilità delle terze parti, esistono già requisiti di compliance per aspetti come la vendor due diligence, il risk management della supply chain o i requisiti dei contratti di acquisto. Il tema è come estendere queste attività tenendo conto anche del potenziale rischio cyber.

Da qui l'importanza di un programma specifico per la Supply Chain Cybersecurity, che in modo realistico permetta di comprendere quali sono i principali rischi associati alla fornitura di prodotti e servizi, e quali le possibilità che i fornitori abbiano accesso esteso a risorse, asset e dati sensibili dell'azienda.

I passaggi chiave per proteggere l'impresa da questo rischio

Proteggere un'organizzazione è un'attività già di per sé abbastanza sfidante, senza andare a pensare anche a tutti i rischi e le vulnerabilità che riguardano la supply chain. Ciò nonostante, è importante oggi valutare anche cosa succede al di fuori delle mura aziendali. Come prepararsi a gestire correttamente le terze parti?

FIGURA 23. COME COSTRUIRE UN PROGRAMMA DI VENDOR MANAGEMENT (SANS INSTITUTE, 2015)

Nel report **"Combatting Cyber Risks in the Supply Chain"** (SANS Institute, settembre 2015) Dave Shackleford propone le seguenti azioni:

1. Definire i fornitori più critici, ossia quelli che potrebbero portare alle conseguenze peggiori in caso di data breach/malfunzionamento
2. Definire il ruolo del "Vendor Owner", persona dell'organizzazione responsabile della gestione e reporting di tutti gli aspetti, comprese eventuali problematiche legali, audit, revisione di procedure e documentazione fornita dal vendor.

3. Definire linee guida e controlli.
4. Integrare gli stessi con i processi aziendali esistenti.

Intervista a Gianna Detoni, BCI Italy Forum Leader e Fondatrice di Panta Ray

TIG. Quali sono oggi le minacce alla resiliency di un'organizzazione che possono derivare da problemi originati dalla supply chain?

Gianna Detoni. *Innanzitutto, è bene specificare che la resilienza di un'organizzazione non dipende soltanto dal grado di attenzione della stessa alla questione, ma dall'impegno di tutti gli stakeholder che intervengono in una qualche maniera nei processi critici (tra questi, senza dubbio, vi sono i fornitori). Parlando nello specifico di supply chain, un recente report del Business Continuity Institute ha mostrato che – nel corso del 2016 – il 70% delle organizzazioni nel mondo ha avuto a che fare con una o più interruzioni derivate dai fornitori. Nella maggior parte dei casi, queste interruzioni hanno comportato per le organizzazioni problemi di natura economica (perdita di produttività e aumento del costo del lavoro), commerciale (perdita di ricavi e della qualità del servizio) e reputazionale (danni all'immagine del brand e reclami dalla clientela). Tra le cause di questi incidenti, le principali sono i problemi IT, la perdita di talenti e skill, e attacchi cyber o data breach.*

TIG. Guardando ai rischi cyber, è quindi possibile che debolezze in termini di cybersecurity dei fornitori abbiano impatti gravi sull'azienda? Qualche esempio?

Gianna Detoni. *Sicuramente. È emblematico il caso di Target, la seconda più grande catena di discount degli Stati Uniti. Durante le vacanze di Natale del 2013, gli hacker sono riusciti a entrare nei sistemi dell'azienda tramite una falla nei server del fornitore degli impianti di climatizzazione per i punti vendita. In questo modo hanno avuto accesso ai dati e alle carte di credito di oltre 100 milioni di persone. Questo ha ovviamente generato un gigantesco danno economico, commerciale, legale e reputazionale per Target, che evidentemente non aveva analizzato a dovere la propria supply chain e le minacce che ne potevano derivare.*

Si potrebbero citare molti altri casi con una dinamica assimilabile. Ad esempio, Home Depot, altro grosso retailer statunitense, ha subito un attacco simile dopo un furto di credenziali a danno di un fornitore. Nell'analizzare la propria supply chain, le organizzazioni devono fare particolare attenzione ai fornitori che rappresentano singoli punti di cedimento o concentrazioni inaccettabili di rischio, ovvero quelle situazioni in un cui un incidente o un'interruzione dalla parte del fornitore ha un impatto diretto e determinante sulle attività e i processi urgenti dell'organizzazione stessa. In questi casi, è necessario assicurarsi della resilienza dei fornitori e della robustezza dei loro sistemi di sicurezza con gli stessi principi e lo stesso rigore che useremmo per la nostra organizzazione.

TIG. Come affrontare i problemi di cyber risk management associati alla supply chain? Quali sono le best practices internazionali?

Gianna Detoni*. Approcciando il discorso da un punto di vista culturale, prima ancora che tecnico. Software antivirus, firewall e altre soluzioni tecniche sono indispensabili, ma sono veramente efficaci solo se diventano parte integrante di un processo di gestione del rischio e della continuità operativa che coinvolga l'intera organizzazione (non solo la funzione IT) e anche la supply chain. In termini pratici, se abbiamo bisogno di avere garanzie da parte dei fornitori, dobbiamo pretendere la possibilità di effettuare una revisione indipendente del loro livello di affidabilità. Tale revisione dovrebbe essere concordata nel momento in cui si stipula il contratto. In termini di standard e best practices internazionali, si può fare riferimento alla ISO/IEC 27005:2011 sull'information security risk management e alla ISO/TS 22318:2015 sulla supply chain continuity, oltre che alle diverse fonti normative in materia. Inoltre, il Business Continuity Institute nel 2017 ha incentrato la Business Continuity Awareness Week sul tema della cyber resilience e – per l'occasione – ha prodotto una serie di contenuti molto interessanti, che sono a disposizione di chiunque gratuitamente sul loro sito.*

DA: RESILIENZA DELLA SUPPLY CHAIN E RISCHI CYBER, 22 GIUGNO 2017
(http://channels.theinnovationgroup.it/cybersecurity/resilienza-supply-chain-rischi-cyber/)

Al giorno d'oggi, in conclusione, l'analisi della maturità di un programma di cyber risk management non può esimersi dal considerare la vulnerabilità associata alla mancanza di controlli di sicurezza sui vendor e su altri business partner lungo la catena di fornitura. Le esperienze citate sono la dimostrazione che anche in casi in cui esisteva un importante piano interno, è bastato non considerare questa minaccia per essere in definitiva attaccati e compromessi da criminali che hanno sfruttato backdoor e collegamenti insicuri con terze parti che avevano accesso ai loro sistemi.

Con in mente queste premesse, abbiamo chiesto ai rispondenti alla survey quali controlli hanno al momento implementato in azienda per la gestione della cybersecurity dei vendor della catena di fornitura. La situazione risulta nel complesso abbastanza buona nel campione considerato, in quanto i 3 quarti delle aziende (il 74% per la precisione) ha già in essere qualche forma di controllo, e anche più di una.

- L'attività più frequente (65% delle risposte) è la richiesta ai fornitori di essere compliant a norme/standard di cybersecurity. È questa anche la situazione per quanto riguarda la norma GDPR sulla data protection: sempre di più, le aziende affideranno la gestione dei dati personali a terze parti solo se queste garantiranno di essere GDPR compliant.
- La seconda misura, che però vede l'adozione da un numero inferiore di aziende (42%) è l'inclusione di requisiti di sicurezza in ogni richiesta di proposta/ contratto con fornitori terzi. Nei contratti con i fornitori possono anche rientrare clausole di cyber insurance (26% delle risposte).
- In alcuni casi il controllo del fornitore diventa molto più attento (23% dei rispondenti). In questi casi si eseguono anche ispezioni, audit, si fanno compilare questionari.
- Ulteriori misure, condotte da una minoranza di aziende sono poi le revisioni dei piani di Business Continuity o di Incident Management dei fornitori.

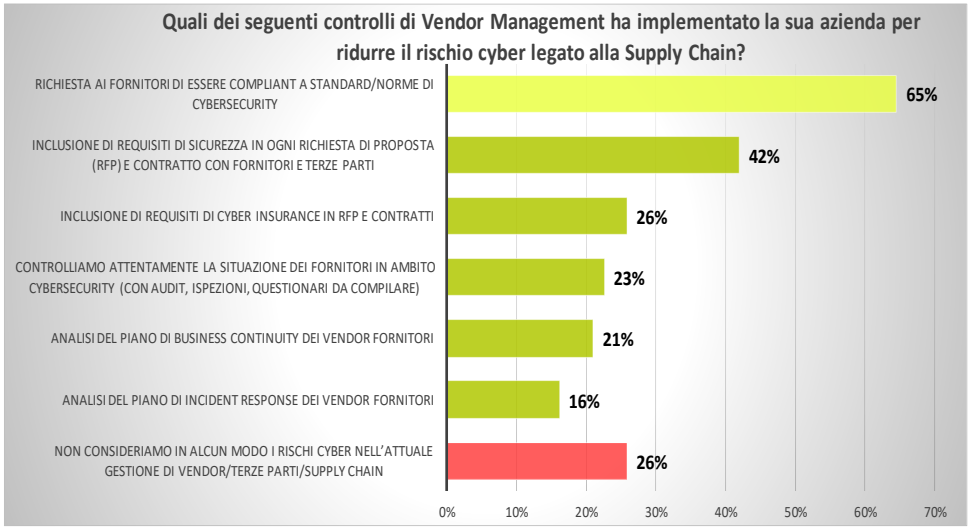

FIGURA 24. I CONTROLLI DI VENDOR MANAGEMENT IMPLEMENTATI PER RIDURRE I RISCHI CYBER

Intervista a Francesco Di Maio, Head Security Department, ENAV.

TIG. Quali sono oggi le problematiche più avvertite dai Chief Information Security Officer?

Francesco Di Maio. *Il principale tema con cui deve confrontarsi oggi un Responsabile della sicurezza informatica è l'aspetto culturale, la necessità di diffondere maggiore consapevolezza su questi rischi. Sappiamo infatti che la principale debolezza di un'architettura di sicurezza rimane l'elemento umano: è quindi necessario far crescere l'awareness e avere una maggiore cultura. I modi per farlo sono diversi, e alcuni risultano essere più efficaci della formazione tradizionale, introducendo ad esempio aspetti legati alla gamification.*

Secondo problema: riuscire a collegare l'intera supply chain sui temi della cybersecurity. Tutti i fornitori di beni e servizi esterni devono possibilmente adeguarsi al modello interno di gestione: bisogna avere un modello di sicurezza basato sul trust, sulla fiducia da parte di tutti delle capacità altrui. Essendo l'ENAV un'infrastruttura critica, ci aspettiamo da tutti i nostri fornitori un'elevata professionalità nell'erogazione dei rispettivi servizi. Anche i produttori di software dovrebbe dotarsi di metodologie di sviluppo sicuro, processi di verifica interni, modelli di patching basati su standard internazionali oggettivi e misurabili. Terza sfida: semplificare. Le organizzazioni sono sempre più complesse. Lo sforzo di tutti i CISO deve quindi essere quello di ridurre i silos, eliminare le complicazioni. Bisogna disporre di una mappatura dei sistemi più critici e di un processo di security governance nella sua interezza, comprensivo di aspetti di Security by design e anche di un approccio sicuro lungo tutto il ciclo di vita dei prodotti/servizi erogati.

TIG. In pratica come assicurare la sicurezza della Supply Chain?

Francesco Di Maio. *Si tratta di impostare un "Security through evidence"; essere cioè in grado di dimostrare secondo vari modelli che il codice rilasciato è sicuro, che sono rispettate le linee guida base (come la verifica di processi di routine, il superamento di stress test, la gestione dell'autorizzazione dell'utente). Noi prevediamo nei processi di procurement la fornitura di linee guida base: il cliente deve fornire nei contratti specifiche tecniche e requisiti base. Anche ai nostri provider chiediamo appropriati livelli di sicurezza: sia per quanto riguarda i processi e l'organizzazione, sia garanzie di continuità operativa, misurate sulla base di specifici SLA.*

TIG. In molte aziende il Responsabile della Sicurezza lamenta la difficoltà di coinvolgere il Board/Top Management e renderlo partecipe delle criticità della cybersecurity: è anche il vostro caso?

Francesco Di Maio. *Non direi: per noi la sicurezza informatica è un elemento critico del business. La nostra azienda è totalmente tecnologica: disponibilità, integrità e riservatezza dei dati sono aspetti assolutamente critici e prioritari, e l'alta direzione dà risposte consistenti. Non avvertiamo questo problema.*

TIG. Parliamo di ottimizzazione della Governance della Cybersecurity: quale struttura di governance deve essere scelta da ogni azienda?

Francesco Di Maio. *Una struttura ideale non esiste, dipende dalla singola organizzazione e dai suoi scopi. Ognuno deve effettuare una valutazione interna e quindi disegnare la governance partendo dal concetto che tutto deve essere risk based. Da questa analisi iniziale derivano output specifici per ogni singola organizzazione. Nel mondo dell'aviazione civile abbiamo anche norme specifiche in tal senso, l'EASA (l'agenzia europea per la sicurezza aerea, European Aviation Safety Agency) ha avviato un programma con regolamenti di grande impatto. Inoltre ci sono linee guida comuni per salvaguardare la fear competition tra tutti gli attori, in modo che tutti i provider di servizi di navigazione aerea abbiano misure comparabili. Oltre alle varie iniziative dell'EASA per rispondere ai rischi di cybersecurity, va ricordato poi l'avvio dell'European Strategic Coordination Platform for cybersecurity, un'iniziativa voluta invece da una serie di attori pubblici, privati e vari rappresentanti dell'aviazione (linee aeree, aeroporti, aviazione commerciale). Si tratta di un modello condiviso e coordinato di risposta, con l'obiettivo di elevare il livello di intelligence e information sharing nell'aviazione. Queste iniziative fanno anche sì che vengano adottate da tutte le parti delle prassi comuni, come la nomina di un CISO, l'analisi del rischio secondo modelli standard, una cybersecurity governance comprensiva degli aspetti di monitoraggio e reporting del rischio.*

DA: LE SFIDE DELLA TRASFORMAZIONE DIGITALE E IL NUOVO RUOLO DEL CISO, 16 GENNAIO 2018 (http://channels.theinnovationgroup.it/cybersecurity/le-sfide-della-trasformazione-digitale-ruolo-del-ciso/)

CYBER INSURANCE: ADOZIONE E MOTIVAZIONI

La copertura assicurativa per rischi IT e Cyber (CYBER INSURANCE) è uno strumento di trasferimento del rischio che in prospettiva sarà sempre più utilizzato dalle aziende. Le compagnie assicurative si stanno infatti adeguando, creando coperture specifiche per questi rischi, ma permangono una serie di elementi che ne frenano la diffusione.

- Non è facile valutare con certezza i rischi e i costi legati agli attacchi cyber. Da un lato manca una statistica condivisa sugli eventi di sicurezza associati. Le minacce cyber sono in continua evoluzione per cui anche una comparazione storica degli incidenti presenta numerose difficoltà. Inoltre, si ha oggi una visione molto parziale sulla situazione corrente in materia di sinistri cyber, che spesso non sono oggetto di notifica neanche all'interno delle singole organizzazioni (come visto in precedenza, parlando di misurazione e reporting degli incidenti cyber). Questo cambierà in parte, con il GDPR per quanto riguarda i dati personali, e con la Direttiva NIS, per quanto riguarda gli incidenti che riguardano gli operatori di servizi essenziali (energia, banche, TLC, utilities, trasporti, infrastrutture digitali, sanità).
- È anche molto difficile stimare il valore del danno economico associato a un incidente cyber: anche lo stesso tipo di evento (pensiamo ad esempio a un data breach che comporti la perdita di dati) ha effetti molto diversi in aziende diverse, oppure a seconda del database impattato dall'attacco. Serve quindi una stima del danno personalizzata per la singola azienda, che non può essere estrapolata in generale: un elemento che rende più complessa la stesura della polizza assicurativa.
- Manca infine una cultura adeguata su questi temi: in molte aziende, data la mancanza di figure come il Risk Manager o il CISO, la gestione del rischio IT e Cyber è tuttora responsabilità dell'area IT, con coinvolgimento molto limitato delle altre funzioni aziendali e in molti casi scarso interesse per questi temi da parte del top management.
- Infine, ulteriore ostacolo nella stesura di polizze cyber, il fatto che il cyber risk ha oggi un'elevatissima probabilità di accadimento, e questo, rispetto ad altre forme di rischio, rende ancora più difficile la stesura di adeguate coperture assicurative.

Nonostante questi limiti, dove le aziende si impegnano nel disegno di un ampio e articolato programma di cyber risk management, la cyber insurance può avere un suo ruolo ben preciso, di trasferimento del rischio che non si può mitigare o accettare.

Analizzando la situazione presso il campione di aziende contattate, che come abbiamo visto anche dalle precedenti risposte presenta una maggiore maturità su questi temi rispetto alla media delle aziende italiane, la Cyber Insurance è in crescita. I risultati riportati sono il tasso di adozione della Cyber Insurance rispettivamente per i 3 anni in cui abbiamo effettuato questa indagine, e mostrano chiaramente un interesse sempre più ampio, con la percentuale di aziende che si è dotata di strumenti assicurativi specifici per l'assicurazione cyber passata dal 2% nel 2015, al 7% nel 2016 e al 15% nel 2017.

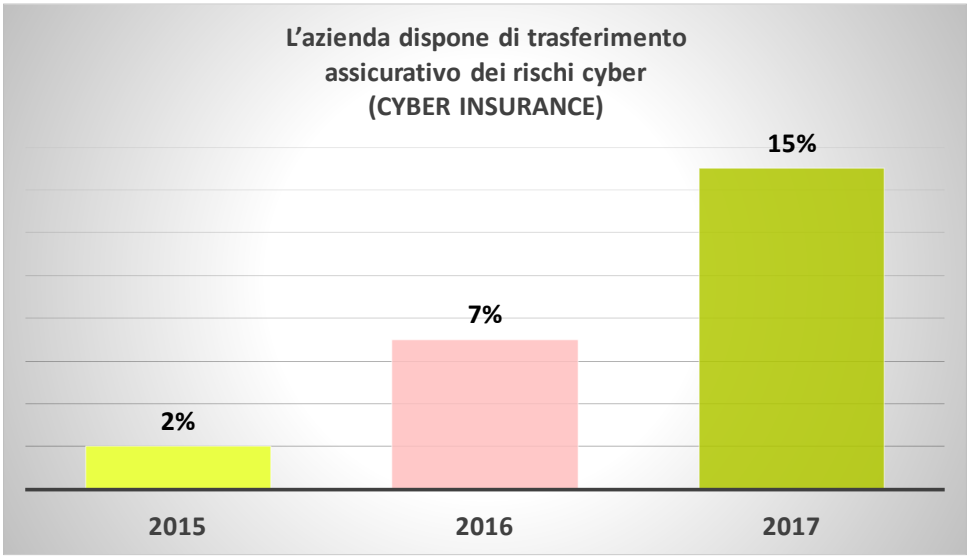

FIGURA 25. ADOZIONE DELLA CYBER INSURANCE NEL 2015, 2016 E 2017

Questo significa che in Italia, dove il mercato è ancora in una fase di sviluppo iniziale rispetto ai numeri raggiunti a livello internazionale, si ha quasi un raddoppio anno su anno dell'adozione di strumenti assicurativi per il rischio cyber. In aggiunta, le previsioni per il 2018, guardando sia ai nuovi piani di adozione sia all'interesse per il tema, sono di un'ulteriore raddoppio nell'acquisto di cyber insurance.

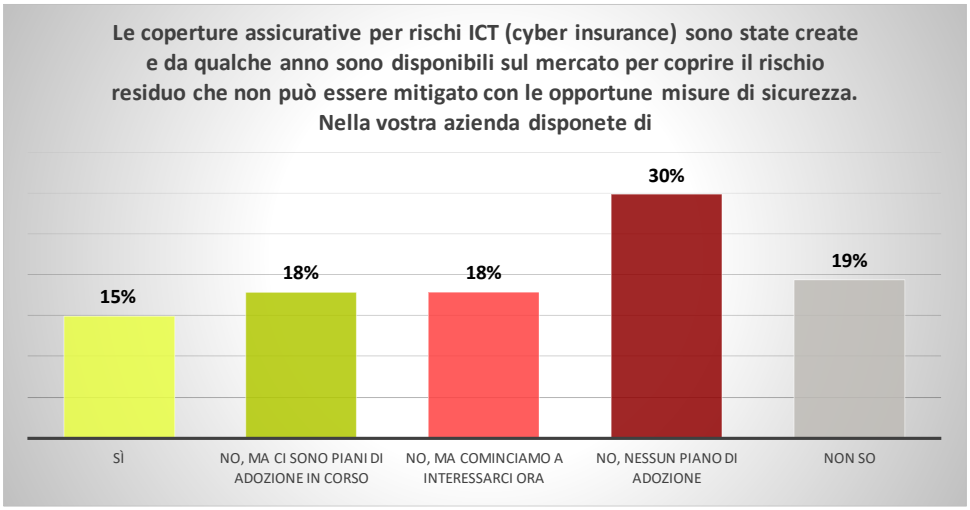

FIGURA 26. PIANI DI ADOZIONE DELLA CYBER INSURANCE NEL 2018

Le motivazioni indicate dai rispondenti per quanto riguarda il ricorso alle assicurazioni cyber stanno a indicare che questo discorso è oggi valido soprattutto per i primi due aspetti:

- La copertura dei costi associati all'interruzione di attività dovuta a un eventuale incidente informatico: un tipo di assicurazione che evidentemente rientra tra le attività consigliate per ridurre l'impatto nell'area della Business Continuity, una delle voci di costo che possono assumere valori molto critici in determinate situazioni (come in precedenza citavamo il caso dell'attacco ransomware NotPetya che ha comportato alcune settimane di riduzione dell'operatività per l'operatore europeo della logistica Maersk, con costi per centinaia di milioni di euro).
- La copertura dei costi di un eventuale data breach, l'altra situazione che spaventa molto oggi le aziende, e che in futuro, almeno per quanto riguarda alcune categorie di dati, richiederà numerose attività, dall'incident response, alle notifiche agli interessati, al ripristino della situazione.
- Al terzo posto per ordine di importanza viene giustamente il valore della reputazione / del brand, che in caso di incidente informatico può richiedere attività specifiche (dalla comunicazione, agli aspetti legali e di gestione dell'incidente) che possono almeno in parte essere coperti da un'assicurazione specifica.
- La copertura per la responsabilità è indicata invece solo a un quarto/quinto posto.

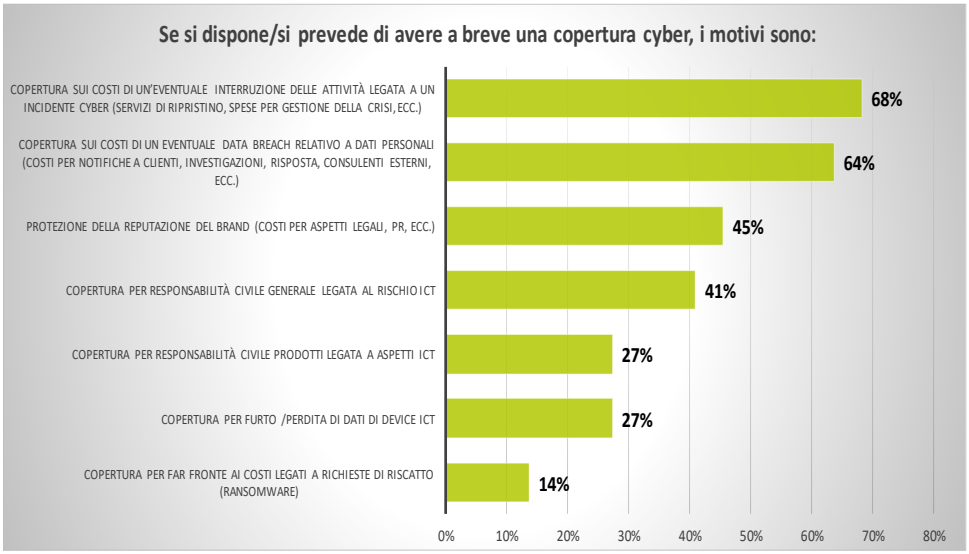

FIGURA 27. MOTIVAZIONI PER L'ADOZIONE DELLA CYBER INSURANCE

CONCLUSIONI

Gli incrementi visti durante tutto il 2017 in sofisticazione, scala e impatti degli attacchi cyber sono un dato di fatto. Il solo attacco WannaCry, che si è svolto tra il 12 e il 28 maggio 2017, ha colpito circa 200.000 computer in 150 paesi a livello globale, con impatti molto gravi, obbligando le aziende a chiudere gli uffici, fermare l'operatività e bloccare le vendite.

Per il mega data breach che ha colpito la società USA di credit reporting Equifax (ha riguardato 148 milioni di persone), si prevedono costi oltre i 430 milioni di dollari entro il 2018, legati alle spese legali (la società sta subendo numerose azioni), a servizi offerti ai clienti per la protezione dei loro conti e della loro identità, a spese per investigazioni digitali e tecnologie di security.

Questi fatti sono stati sufficienti da dimostraree una volta per tutte le gli attacchi cyber non possono più essere un ambito della sola funzione ICT ma riguardano direttamente i livelli apicali delle aziende.

I risultati dell'indagine svolta tra la fine del 2017 e l'inizio del 2018, su un campione di aziende di dimensione medio grande (caratterizzato dalla presenza di numerose attività per la cybersecurity e programmi già strutturati di Cyber risk management), parlando direttamente con i responsabili della sicurezza ICT di queste aziende, o figure comunque collegate e a conoscenza della situazione della propria azienda, hanno permesso di evidenziare alcuni elementi importanti:

- Nessuno si può dire completamente protetto dall'evenienza di un incidente cyber: nonostante le numerose iniziative in corso, le vulnerabilità e la sofisticazione e continua mutazione degli attacchi rendono questa sfida molto complessa.
- Fino ad oggi l'area della cybersecurity è stata troppo orientata a strutturarsi "a silos", in modo separato dal resto dell'organizzazione (un limite anche all'interno dello stesso dipartimento ICT, come si vede nello scarso collegamento esistente tra sicurezza e sviluppo applicativo). Servirebbe invece un approccio più coordinato con il resto dell'organizzazione e orientato a comunicare meglio le problematiche della cybersecurity al top management/al board. Le stesse attività di misurazione e reporting sono oggi poco strutturate, qualitative invece che quantitative, in molti casi inesistenti.
- Oggi tra i primi driver per la sicurezza rimane la compliance, basti pensare all'impatto che sta avendo il GDPR, come confermano anche le risposte alla survey. La stessa norma richiede però di ripensare le attività basandole innanzi tutto su una valutazione del rischio. Un approccio risk based deve anche far leva su un maggiore orientamento alla misurazione e all'analisi tramite attività di cyber threat intelligence, di continuo monitoraggio all'interno e all'esterno, verso la supply chain, subfornitori, ecc). In questo modo sarà possibile anticipare i possibili impatti negativi e anche prioritizzare gli investimenti.

Le organizzazioni sono quindi consapevoli che sugli aspetti di Cyber risk management è fondamentale rivedere la propria impostazione e le modalità di gestione del rischio cyber.

In conclusione, riteniamo che nei prossimi anni le priorità dei CISO debbano essere:

- Ripensare il disegno complessivo, le misure e i processi del Cyber risk management, adottando ad esempio framework consolidati, e puntando soprattutto a diffondere una cultura sul tema e una maggiore security awareness in azienda.
- Estendere il monitoraggio della security, sulla base di un disegno preciso di Threat Management e strumenti opportuni per il Vulnerability Management, integrato con una comunicazione dei risultati di tutto questo lavoro adottando Security Metrics e un reporting efficace verso il top management/board.
- Allineare meglio la security alle iniziative di Digital Transformation e sviluppo del business: la velocità è oggi un elemento critico per competere nel mondo Digitale, servono quindi meccanismi nuovi per garantire una maggiore sicurezza delle applicazioni e dei trattamenti dei dati dei clienti.
- Valutare tutte le possibilità di gestione del rischio cyber, ossia, come insegna il Risk Management, "evitare, accettare, mitigare e trasferire tale rischio", quest'ultima attività valutando le coperture assicurative oggi disponibili sul mercato. Come calcolare però l'impatto economico del cyber crime? la possibile perdita finanziaria per l'azienda come conseguenza di un attacco informatico? Questa nuova scienza è in via di sviluppo, dai risultati dell'indagine appare evidente che le aziende mettono al primo posto, nella valutazione dei costi, la mancata operatività e i danni legati alla possibile perdita/furto dei dati personali.

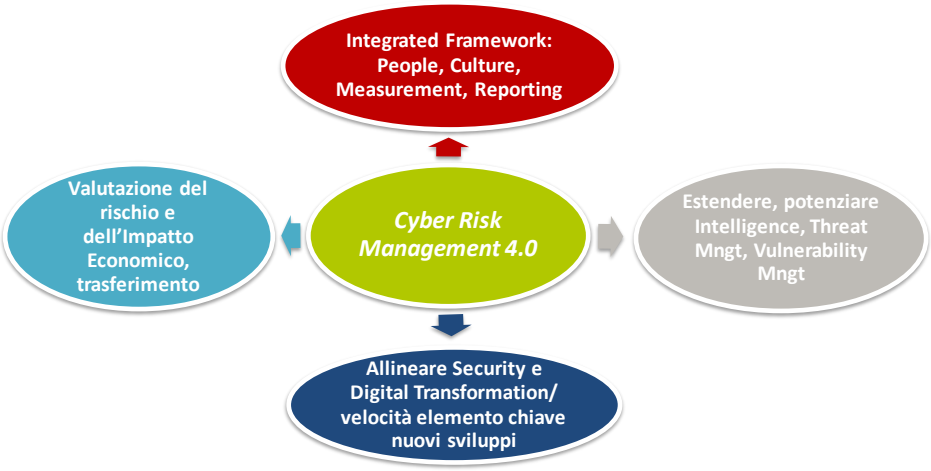

FIGURA 28. COME DEVE EVOLVERE IL CYBER RISK MANAGEMENT PER SUPPORTARE L'IMPRESA 4.0

Una gestione ottimale del Cyber risk management avrà in futuro impatti molto positivi per l'azienda, ancora in parte sconosciuti (tanto che non le viene ancora neanche attribuito il ruolo di funzione abilitante): basti pensare al fatto che questo ambito sarà sempre più spesso parte di processi di Due Diligence (pensiamo a transazione M&A), a verifiche sulla possibilità di individuare coperture assicurative; a controlli da parte di clienti e partner lungo la supply chain.

Si ringraziano per il loro supporto i Partner del Programma Cybersecurity e Risk Management 2018

Fondata nel 2009, The Innovation Group (TIG) è una società di servizi di consulenza e di ricerca di mercato indipendente, specializzata nello studio delle evoluzioni del mercato digitale e nei processi d'innovazione abilitati dalle tecnologie e dalla conoscenza.

Ci rivolgiamo ad aziende ed organizzazioni dell'Economia Digitale che desiderano sviluppare strategie di crescita attraverso programmi e iniziative di go-to-market, basati sulla produzione e gestione integrata della conoscenza all'interno e all'esterno dell'azienda. Sviluppiamo analisi, ricerche e approfondimenti progettati per il mercato italiano, per diffondere la conoscenza e la comprensione del mercato digitale e dei settori a più forte innovazione. Mettiamo a disposizione piattaforme integrate di servizi e contenuti per facilitare gli scambi e le relazioni con il mercato, gli influencer, gli stakeholder e gli ecosistemi.

Ai nostri clienti proponiamo un approccio concreto, volto ad affiancarli ed accompagnarli nella fase di realizzazione di piani strategici, per valorizzare le risorse e le capacità esistenti al proprio interno e prendere le decisioni più utili in tempi rapidi. Oltre ad idee e thought leadership, offriamo alle aziende gli strumenti per posizionarsi al meglio sul mercato e comprendere i bisogni dei propri clienti.

The Innovation Group

Innovating business and organizations through ICT