Cyber, un rischio difficile da individuare

Massimiliano Colombo
Regional Underwriting Manager

Fattori tecnici e normativi in rapida evoluzione rendono il cyber un rischio imprevedibile, ma con più esperienza e strumenti migliori, la minaccia può essere gestita meglio.

Panoramica

Il mondo digitale è una delle minacce principali che caratterizzano l'attuale panorama del rischio. I sondaggi[1] sui dirigenti mondiali hanno classificato i rischi informatici in una posizione elevata, assieme all'incertezza geopolitica e ai cambiamenti climatici, mentre un sondaggio sui gestori del rischio europei ha citato il cyber come il principale rischio di preoccupazione.

800 milioni

di posti di lavoro attuali potrebbero essere eliminati dall'automazione entro il 2030

La tecnologia è un importante motore del cambiamento politico ed economico, le due principali cause di crescente imprevedibilità per il business, come rivela l'Indice di Imprevedibilità di QBE. I social media stanno cambiando il dibattito politico, mentre si prevede che le nuove tecnologie, come i veicoli autonomi, la robotica e l'intelligenza artificiale, avranno un impatto enorme sulla vita delle persone. Secondo McKinsey, circa il 60% delle occupazioni sarà in qualche modo influenzato dall'automazione, ed entro il 2030 circa 800 milioni di posti di lavoro attuali potrebbero non esistere più.

La tecnologia è ora al centro della maggior parte delle organizzazioni, ne guida le operazioni, le catene di fornitura e la distribuzione. Tuttavia, il ritmo di adozione della tecnologia sembra superare le capacità tecniche e di sicurezza informatica della maggior parte degli utenti e delle aziende. Molti non capiscono appieno cosa significa il cyber per loro, né prevedono l'impatto sulla loro attività quando qualcosa va male.

A posteriori, molti incidenti informatici sembrano prevedibili, se non addirittura prevenibili. Tuttavia, rispetto a rischi come le catastrofi naturali o gli incendi - che sono ben compresi e possono essere modellati utilizzando dati storici di perdita, il rischio informatico è particolarmente difficile da individuare. È molto difficile prevedere quando, dove e come si svolgerà un evento informatico. Anche quando è possibile identificare scenari probabili, l'impatto probabile e la perdita finanziaria potenziale possono essere difficili da prevedere e calcolare.

(1) World Economic Forum Global Risks, 2019 PwC survey, https://www.ferma.eu/2018-european-risk-manager-report

Una miriade di incognite

La tecnologia e gli eventi informatici ci pongono di fronte a molte incognite. Gli incidenti informatici derivano da una vasta serie di cause e fattori scatenanti, come attacchi informatici, guasti tecnici, attraverso la catena di fornitura o un dipendente disonesto.

Le organizzazioni non sapranno dove saranno colpite né il grado di impatto. Inoltre, poiché ogni azienda ha una propria struttura IT, è difficile imparare dall'esperienza dei colleghi.

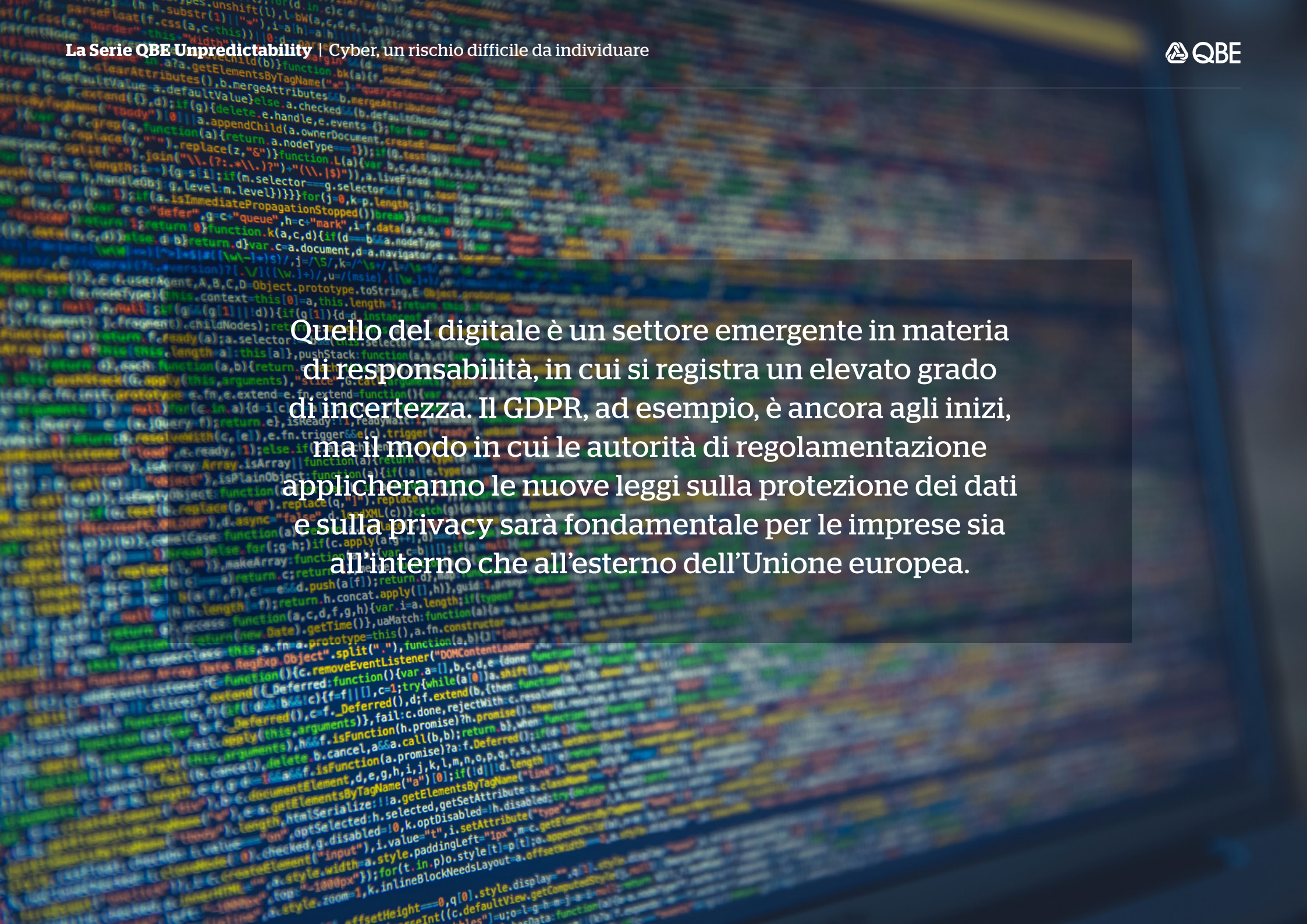
Tenere il passo con il rischio informatico è un'altra sfida. Il cyber è una corsa senza fine in cui gli hacker sono sempre un passo avanti e nuove vulnerabilità possono provenire da settori inaspettati. Le minacce emergenti includono l'utilizzo di dispositivi di internet degli oggetti e le vulnerabilità dell'hardware

> Il cyber è una corsa senza fine in cui gli hacker sono sempre un passo avanti e nuove vulnerabilità possono provenire da settori inaspettati.

(come le minacce Meltdown e Spectre 2018), mentre l'attenzione si sta ora rivolgendo agli attacchi informatici alimentati dall'intelligenza artificiale. Per quanto solide siano le difese di sicurezza informatica di un'organizzazione, è impossibile rimanere immuni dal rischio.

Prevedere l'impatto di un incidente informatico è particolarmente difficile e varierà notevolmente da azienda a azienda, anche per lo stesso incidente. Ad esempio, l'attacco del malware NotPetya del 2017 ha causato gravi disagi a diverse aziende, mentre altre aziende dello stesso settore ne sono uscite indenni.

Anche le dimensioni e l'interconnettività sono all'origine dell'imprevedibilità - la violazione dei dati degli hotel di Marriott dello scorso anno ha colpito 500 milioni di persone, mentre l'epidemia di ransomware WannaCry del 2017 ha colpito circa 300.000 computer in 150 paesi. Secondo una recente ricerca dei Lloyd's di Londra, un grande attacco globale di malware potrebbe colpire più di 600.000 aziende in tutto il mondo e costare 193 miliardi di dollari, tanto quanto un grande evento di catastrofe naturale.



Quello del digitale è un settore emergente in materia di responsabilità, in cui si registra un elevato grado di incertezza. Il GDPR, ad esempio, è ancora agli inizi, ma il modo in cui le autorità di regolamentazione applicheranno le nuove leggi sulla protezione dei dati e sulla privacy sarà fondamentale per le imprese sia all'interno che all'esterno dell'Unione europea.

Interruzione dell'attività

Eventi come WannaCry e NotPetya evidenziano il potenziale di interruzioni delle attività legate al cyber e le perdite contingenti di interruzione delle attività, che sono particolarmente difficili da prevedere e quantificare, data la complessità e le concentrazioni di rischio all'interno delle catene di fornitura fisiche e digitali.

Ad esempio, un produttore che subisce un'interruzione dei sistemi IT potrebbe essere in grado di compensare la perdita di produzione, ma si troverebbe ad affrontare il costo aggiuntivo di soluzioni alternative e la potenziale perdita di affari. L'anno scorso, il produttore di semiconduttori TSMC è stato colpito da un malware, con una perdita stimata del 3% di ricavi e costi aggiuntivi. Le perdite da interruzione delle attività e le spese aggiuntive derivanti dall'attacco NotPetya sono costate 300 milioni di dollari rispettivamente al gruppo di spedizione Maersk e alla società di logistica FedEx, mentre il produttore alimentare Mondelez ha riportato perdite dovute a questo attacco per oltre 100 milioni di dollari.

In qualità di assicuratori del rischio informatico, assistiamo a molti eventi in cui le aziende non hanno compreso appieno gli effetti a catena di un incidente informatico. Anche quando un'azienda si prepara a possibili scenari informatici, è difficile prevedere l'andamento dei piani di continuità operativa nella pratica. Il riavvio dei sistemi in un ambiente controllato, ad esempio, è molto diverso dalla realtà del riavvio a seguito di un'interruzione o di un attacco ransomware.

"In qualità di assicuratori del rischio informatico, assistiamo a molti eventi in cui le aziende non hanno compreso appieno gli effetti a catena di un incidente informatico."

Incertezza normativa

La rapida evoluzione tecnologica fa sì che il quadro normativo e giuridico sia in continua evoluzione. Ciò vale in particolare per le leggi sulla privacy e sulla protezione dei dati, ma anche per i requisiti di sicurezza informatica e i regimi di responsabilità, ad esempio, l'introduzione di veicoli autonomi, internet degli oggetti e l'intelligenza artificiale sollevano una serie di questioni normative e giuridiche.

Le nuove normative e le leggi non testate creano incertezza per le imprese, dall'entità delle penali ai risarcimenti richiesti dalle persone interessate. Ciò è già evidente con il regolamento generale dell'UE sulla protezione dei dati (GDPR), che nel maggio 2018 ha introdotto norme severe in materia di protezione dei dati e della vita privata. Il GDPR conferisce alle autorità di regolamentazione maggiori poteri e ai consumatori maggiori diritti, ma ci vorranno diversi anni prima che le implicazioni del GDPR siano pienamente comprese.

Quello del digitale è un settore emergente in materia di responsabilità, in cui si registra un elevato grado di incertezza. Il GDPR, ad esempio, è ancora agli inizi, ma il modo in cui le autorità di regolamentazione applicheranno le nuove leggi sulla protezione dei dati e sulla privacy sarà fondamentale per le imprese sia all'interno che all'esterno dell'Unione europea. Il GDPR si applica alle imprese che trattano dati UE in qualsiasi parte del mondo, mentre un numero crescente di paesi sta ora cercando di introdurre requisiti simili.

Anche quello delle controversie è un settore emergente del cyber. A tutt'oggi non abbiamo ancora assistito a un gran numero di controversie, ma è evidente che in futuro la responsabilità civile è destinata a crescere. Leggi come il GDPR rendono più facile per i singoli chiedere un risarcimento a seguito di un incidente informatico, anche per danni non finanziari, come la sofferenza emotiva. L'atteggiamento nei confronti della privacy e delle interruzioni dei servizi sta cambiando, e il numero crescente di incidenti informatici sta portando ad azioni collettive, in quanto gli investitori e i consumatori chiedono il risarcimento dei danni subiti.

Prossimamente...

Sii il primo a ricevere una copia dell'indice di imprevedibilità QBE quando viene pubblicato.

qbeitalia.com/imprevedibilita

Prevenzione

Il rischio informatico non è destinato a scomparire. Tuttavia, una stabile gestione del rischio e delle disposizioni assicurative può migliorare la situazione e aiutare le organizzazioni ad affrontare meglio gli effetti.

> È ancora presto per la digitalizzazione. Tuttavia, grazie all'esperienza, le aziende potranno comprendere meglio i rischi informatici e la prevenzione.

93%

dei gestori del rischio lavora attualmente a stretto contatto con i colleghi dell'IT e della sicurezza informatica

37%

già identifica e valuta i rischi prima dell'adozione delle nuove tecnologie da parte dell'azienda

Tecniche di gestione del rischio ben consolidate, ad esempio, possono aiutare le organizzazioni e i loro consigli di amministrazione ad adottare la tecnologia e favorire la digitalizzazione. Un'indagine condotta dalla Federazione delle associazioni di gestione del rischio (FERMA) ha rilevato che il 93% dei gestori del rischio lavora attualmente a stretto contatto con i colleghi dell'IT e della sicurezza informatica, mentre il 37% già identifica e valuta i rischi prima dell'adozione delle nuove tecnologie da parte dell'azienda.

È ancora presto per la digitalizzazione. Tuttavia, grazie all'esperienza, le aziende potranno comprendere meglio i rischi informatici e la prevenzione. Nel frattempo, le aziende possono adottare misure per ridurre il rischio. Ad esempio, oltre ai controlli di base della sicurezza informatica, come i test di penetrazione, i patch e la formazione, la capacità di prevedere un evento informatico come l'interruzione o la violazione dei dati può ridurre significativamente l'impatto.

Ad un livello elevato, le aziende dovrebbero riflettere su cosa sia una violazione o un'interruzione dei dati, identificando i dati, i servizi e i terzi che sono critici per la loro attività. È conveniente dedicare

del tempo a elaborare scenari in anticipo, preparando piani di risposta alle crisi e di continuità operativa. L'esperienza ha dimostrato che una buona preparazione può ridurre significativamente l'impatto di una violazione dei dati e, costruendo una resilienza globale, un'organizzazione dovrebbe essere in grado di rispondere a qualsiasi evento informatico, anche se inatteso.

La tecnologia potrebbe anche venire in aiuto alle aziende, fornendo strumenti per aiutare a valutare e quantificare il rischio informatico. Le piattaforme di valutazione del rischio informatico possono già valutare e confrontare il rischio informatico e la sicurezza informatica di un'organizzazione, nonché aiutare a quantificare le perdite o a mappare le catene di approvvigionamento. Tali strumenti sono nelle prime fasi di sviluppo, ma probabilmente diventeranno indispensabili nei prossimi anni.

Le imprese possono anche trasferire i rischi al settore assicurativo e accedere ai loro servizi e alle loro competenze. I prodotti assicurativi informatici sono in continuo miglioramento e possono offrire un ulteriore comfort, mano a mano che le organizzazioni investono in nuove tecnologie e modelli di business digitali.

Misure da adottare per ridurre il rischio informatico:

Misure base:

- penetration testing
- patching
- formazione

Pianificazione per un evento cyber:

- outage
- data breach

Contattaci

Se non ti sei già registrato per ricevere la serie Unpredictability, puoi farlo su:

qbeitalia.com

aprile 2019

QBE Italy
Via Melchiorre Gioia 8
20124 Milan
Italy

T: +39 02 3626 3500 | qbemilan@it.qbe.com