Kaspersky for Business

KASPERSKY lab

# Sicurezza IT: in aumento il budget per promuovere le iniziative di digital transformation

Kaspersky Lab

# Sommario

# Introduzione

È un periodo difficile per il business. Il mondo è sempre più piccolo e in questa nuova epoca in cui i consumatori vogliono tutto e subito e i clienti chiedono risultati immediati, la concorrenza è più agguerrita che mai: il **70% dei consumatori** afferma di poter trovare facilmente soluzioni alternative grazie agli strumenti tecnologici.

**47%**

**dei CEO**

riceve richieste per implementare politiche di digital transformation

In questo contesto, molteplici aziende stanno intraprendendo strategie di digital transformation. **Gartner ha infatti rilevato che quasi la metà (47%) dei CEO** riceve richieste per implementare politiche di questo genere dal proprio Consiglio di Amministrazione, al fine di migliorare le proprie prospettive di crescita e le relazioni con i clienti. Molti, per esempio, stanno migrando un numero sempre maggiore di piattaforme e dati sul cloud, per scalare o rispondere alle richieste del mercato e con la necessaria agilità per stare al passo con la concorrenza.

**Questi dati costituiscono il fondamento della digital transformation. Le iniziative data-driven sono aumentate fino a svolgere un ruolo di primo piano nelle organizzazioni di tutte le dimensioni, fornendo ai responsabili aziendali la motivazione necessaria per poter eseguire con successo le strategia sia a breve che a lungo termine.**

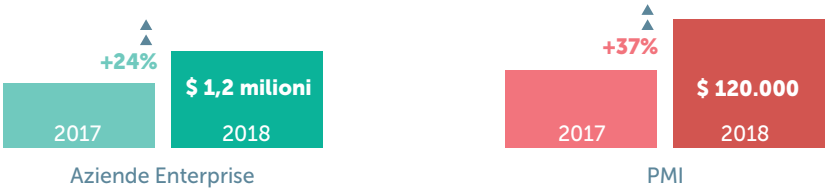
Dal momento che le aziende si stanno trasformando digitalmente, le considerazioni sulla cybersecurity sempre più spesso devono svolgere un ruolo strategico nell'azienda, che si riflettano negli attuali dibattiti all'interno delle strutture che riportano al CISO e nella spesso citata esigenza di dare alla sicurezza informatica il giusto spazio al tavolo delle decisioni.

Gli elementi chiave per prendere sul serio la cybersecurity in azienda sono chiari: man mano che le aziende si affidano sempre di più alle piattaforme digitali, non possono permettersi che queste siano inadeguate. E qui sorge un problema, perché il mondo dei rischi per la sicurezza IT è in continua evoluzione. Ogni giorno emergono nuove minacce e appena le infrastrutture aziendali si adattano, prendono vita nuove vulnerabilità.

La nostra missione è comprendere la complessità e le esigenze della sicurezza IT, per aiutare le aziende a proteggere ciò che per loro è più importante. Continuando la nostra ricerca annuale nell'economia della sicurezza IT, questo report si basa su dati provenienti da esercizi precedenti per identificare come le organizzazioni stanno rispondendo ai cambiamenti nel panorama delle minacce e per comprendere le abitudini di spesa per la sicurezza IT che potrebbero rappresentare il successo o il fallimento delle aziende nel mondo. Di seguito viene presentata una panoramica dei nostri risultati.

## Gli attacchi diventano sempre più sofisticati e complessi

La notizia preoccupante per le aziende di tutti i settori è che l'impatto finanziario dei cyberattacchi e dei conseguenti costi di ripristino è in continuo aumento. **Per le aziende Enteprise, il costo medio di un data breach è ora poco superiore a $ 1,2 milioni, con un incremento del 24% dal 2017 e un aumento del 38% dal 2016. La storia è la stessa per le piccole e medie imprese, con un impatto finanziario di un data breach in aumento del 37% negli ultimi dodici mesi, da $ 88.000 del 2017 a $ 120.000 nel 2018.**




Migliorare il software e l'infrastruttura rappresenta la conseguenza più costosa di una violazione della sicurezza sia per le aziende Enterprise sia per le PMI. Tutto ciò evidenzia i danni creati alle infrastrutture aziendali dalle varie epidemie di ransomware, dagli exploit dannosi e dagli attacchi alla supply chain negli ultimi dodici mesi, dando un quadro generale dell'effort richiesto per rinnovare i sistemi colpiti e rispondere in maniera più sostenibile a un attacco.

Per le aziende Enterprise di tutto il mondo, migliorare l'infrastruttura dopo una violazione richiede in media $ 193.000, un aumento di oltre il 46% rispetto ai **$ 132.000** del 2017. In effetti, questa cifra è più elevata per le aziende Enterprise in tutte le aree geografiche, eccetto l'America Latina, mostrando come la maggior parte delle grande aziende si trovino nella stessa situazione quando si tratta delle implicazioni finanziarie di un data breach. Il nostro studio sottolinea inoltre come gli incidenti di cybersecurity possano danneggiare direttamente il modo di fare business, con danni a rating/premi di assicurazione **($ 180.000)** e perdita di business **($ 131.000)**: entrambi presenti nella classifica delle cinque conseguenze più costose di un data breach.

Una significativa quantità di denaro viene anche impiegata per migliorare il livello delle conoscenze e delle competenze a cui hanno accesso le aziende Enterprise attraverso la formazione dei dipendenti **($ 137.000)**, l'impiego di professionisti esterni **($ 126.000)** o l'assunzione di nuovo personale **($ 106.000)**. In un momento storico caratterizzato da una generica carenza di competenze in tutto il settore, la sfida per tutte le aziende è data da una sempre maggiore difficoltà di effettuare un adeguato investimento per l'assunzione di un talento. Questa è probabilmente la ragione per cui le aziende si stanno concentrando molto di più sulla formazione della forza lavoro attuale, piuttosto che sulle nuove assunzioni.

## Le strategie di trasformazione sono a rischio

Quest'anno i risultati hanno mostrato che gli incidenti più costosi sono correlati all'infrastruttura cloud. Ciò che è evidente è che il boom del cloud e la mobilità hanno presentato molte opportunità sfruttabili dai cybercriminali. Questi fenomeni hanno anche aperto le aziende ai rischi legati agli errori umani, mentre la natura distribuita dell'infrastruttura cloud presenta una grande complessità di gestione. L'uso di piattaforme di cloud computing per un certo periodo è aumentato sia nelle aziende Enterprise che nelle PMI, offrendo diversi vantaggi per le organizzazioni ma, allo stesso tempo, mettendo a rischio i dati aziendali.

Osservando le prime tre tipologie di minacce più costose, gli incidenti di sicurezza che impattano sull'infrastruttura IT ospitata da terze parti hanno avuto il maggiore peso per le PMI **($ 118.000)** e hanno rappresentato il secondo più grande impatto finanziario per aziende Enterprise **($ 1,11 milioni)**. Anche gli incidenti che inficiano i servizi cloud di terze parti che l'azienda utilizza hanno una notevole incidenza finanziaria sulle PMI **($ 89.000)**, a indicare che le strategie di digital transformation delle imprese (l'adozione del cloud rientra tra queste) potrebbero essere causa di esposizione agli incidenti IT qualora le aziende non riescano a trovare un modo per ridurre i rischi.

## La sicurezza sta diventando sempre più strategica


**del budget IT**
viene allocato
per la cybersecurity

Per combattere tali minacce, alla sicurezza viene dato un sempre più spazio in azienda. Le organizzazioni stanno iniziando ad avvertire il reale impatto della cybersecurity sulle attività aziendali; i risultati dello studio mostrano che i timori per i costi di un incidente **stanno costringendo i responsabili aziendali ad assegnare alla cybersecurity una parte maggiore del budget IT (23%) e stanno attirando maggiormente l'attenzione del top management rispetto agli anni precedenti**.

Le aziende Enterprise si aspettano che i loro budget per la sicurezza IT crescano del 15% nel corso dei prossimi tre anni. Lo stesso è vero per le microimprese, con un investimento significativo per le aziende con meno di 50 dipendenti, dove le risorse sono spesso scarse, mentre le PMI si aspettano di vedere una crescita del 14% nella propria spesa per la cybersecurity entro il 2021. Le aziende in Medio Oriente, Turchia e Africa, intanto, si aspettano un aumento di quasi un quinto (19%) dei propri budget per la sicurezza IT nei prossimi tre anni, in contrasto significativo con le aziende Enterprise in Giappone (12%) e Nord America (11%).

Una possibile spiegazione è che l'aumento dei controlli normativi, per esempio l'introduzione del GDPR nell'Unione Europea, potrebbe avere un impatto sull'importanza assegnata alla sicurezza IT: la legislazione riterrà le imprese responsabili per la protezione dei dati personali dei clienti, prevedendo severe sanzioni per chi non risulta essere compliant. Ciò rende alquanto sorprendente che le aziende in Europa prevedano un aumento dei budget per la sicurezza IT di appena il 13% nel corso dei prossimi tre anni: una stima inferiore rispetto ad alcune altre aree geografiche.

Questi risultati non solo evidenziano i costi crescenti associati con la difesa contro i cyberattacchi, ma illustrano anche il valore e l'importanza che i dirigenti assegnano alla capacità di proteggere le proprie aziende dalle minacce più recenti.

Infatti, il coinvolgimento del top management nel dibattito sulla cybersecurity è un evidente segno che la sicurezza viene sempre più inserita nella strategia aziendale. Un aspetto emerge chiaramente dal nostro studio: la risposta e il ripristino dagli incidenti di sicurezza e data breach non sono mai stati tanto importanti. Continuate a leggere per scoprire ulteriori dettagli.

# Metodologia

Il Kaspersky Lab Corporate IT Security Risks Survey è un'indagine globale sui responsabili IT aziendali condotta a partire dall'anno 2011. **Un totale di 6.614 intervistati provenienti da 29 Paesi ha risposto a domande sulla spesa per la sicurezza IT della propria organizzazione, sui tipi di minaccia che devono affrontare e sui costi di ripristino dagli attacchi.** Le aree geografiche interessate comprendono LATAM (America Latina), Europa, Nord America, APAC (Asia Pacifica con la Cina), Giappone, Russia e META (Medio Oriente, Turchia e Africa).

In tutto il report, le imprese sono indicate come microimprese (aziende molto piccole con meno di 50 dipendenti), PMI (piccole e medie imprese con 50 - 999 dipendenti) e delle aziende Enterprise (imprese con oltre 1.000 dipendenti). In questo report non sono inclusi tutti i risultati del sondaggio.

# Risultati principali

**Il costo dei data breach è aumentato di oltre un quinto sia per le aziende Enterprise sia per le PMI.** L'impatto finanziario medio di un data breach è pari a **$ 1,23 milioni** per una grande azienda, con un aumento del 24% rispetto ai **$ 992.000** del 2017. Lo stesso vale per le PMI, con un aumento dei costi da **$ 88.000** dello scorso anno a **$ 120.000** nel 2018: una crescita del 37%.

**Le aziende in Asia Pacifica, Giappone e Nord America registrano i costi di ripristino più alti.** Subire un data breach è più costoso per le aziende Enterprise in Giappone **($ 1,7 milioni**), seguito da Nord America **($ 1,6 milioni)** e Asia Pacifica con la Cina **($ 1,5 milioni)**. Il Nord America è al primo posto per le PMI **($ 149.000)**. Sia per le aziende Enterprise sia per le PMI, l'impatto finanziario medio di un data breach è più basso se hanno sede in Russia, pari rispettivamente a **$ 246.000** e **$ 74.000**.

**La media dei budget destinati alla sicurezza è aumentata tra le aziende di tutte le dimensioni.** Le aziende Enterprise spendono una media di **$ 8,9 milioni** per la cybersecurity, mentre i budget per la sicurezza delle PMI sono cresciuti da **$ 201.000** nel 2017 a **$ 246.000** nel 2018. L'aumento maggiore ha interessato le microimprese, la cui spesa media per la sicurezza è passata da **$ 2.400** a **$ 3.900** negli ultimi dodici mesi, dimostrando che anche le imprese più piccole iniziano a prendere sul serio la sicurezza IT.

**La minaccia più costosa è legata alla perdita di dati aziendali.** Gli incidenti con impatto sull'infrastruttura IT ospitata da una terza parte sono tra le minacce più costose, sia per le aziende Enterprise **($ 1,09 milioni)** sia per le PMI **($ 118.000)**, seguiti dall'inappropriata condivisione dei dati da dispositivi mobili e dagli incidenti riguardanti servizi cloud di terze parti.

**La complessità delle infrastrutture e la mancanza di conoscenze sono fattori determinanti per gli investimenti nell'ambito della sicurezza IT.** Più di un terzo delle aziende cita la maggiore complessità della propria infrastruttura IT (34%) e la necessità di migliorare le competenze specialistiche in materia di sicurezza (34%) come motivazioni per investire nella cybersecurity.

# Costo medio dei data breach

Le aziende di piccole e grandi dimensioni hanno una serie di fattori di costo da considerare a seguito di un data breach, dai costi per il personale al pagamento di sanzioni e di compensazioni. Ma che cosa comporta esattamente un "tipico" data breach da un punto di vista finanziario? Per le aziende, il costo medio attualmente supera $ 1,23 milioni, contro i $ 992.000 del 2017. I costi maggiori invece provengono dal miglioramento di software e infrastrutture ($ 193.000), ma anche fattori quali danni al rating/premi assicurativi ($ 180.000) e formazione ($ 137.000) hanno un grande impatto.

La situazione è la stessa per le piccole e medie imprese, con un costo medio per data breach cresciuto da $ 87.800 del 2017 a $ 120.000 nel 2018. Le PMI si trovano di fronte a molti degli stessi costi che sostengono le grandi aziende: l'impiego di professionisti esterni, danni al rating e perdita di business (il tutto per $ 15.000) con il più grande impatto complessivo che rappresenta una grande parte delle entrate di una PMI.

**In seguito ai notevoli e costosi incidenti dello scorso anno, sembra che le aziende stiano investendo in maniera consistente per migliorare la protezione e rafforzare la copertura assicurativa**

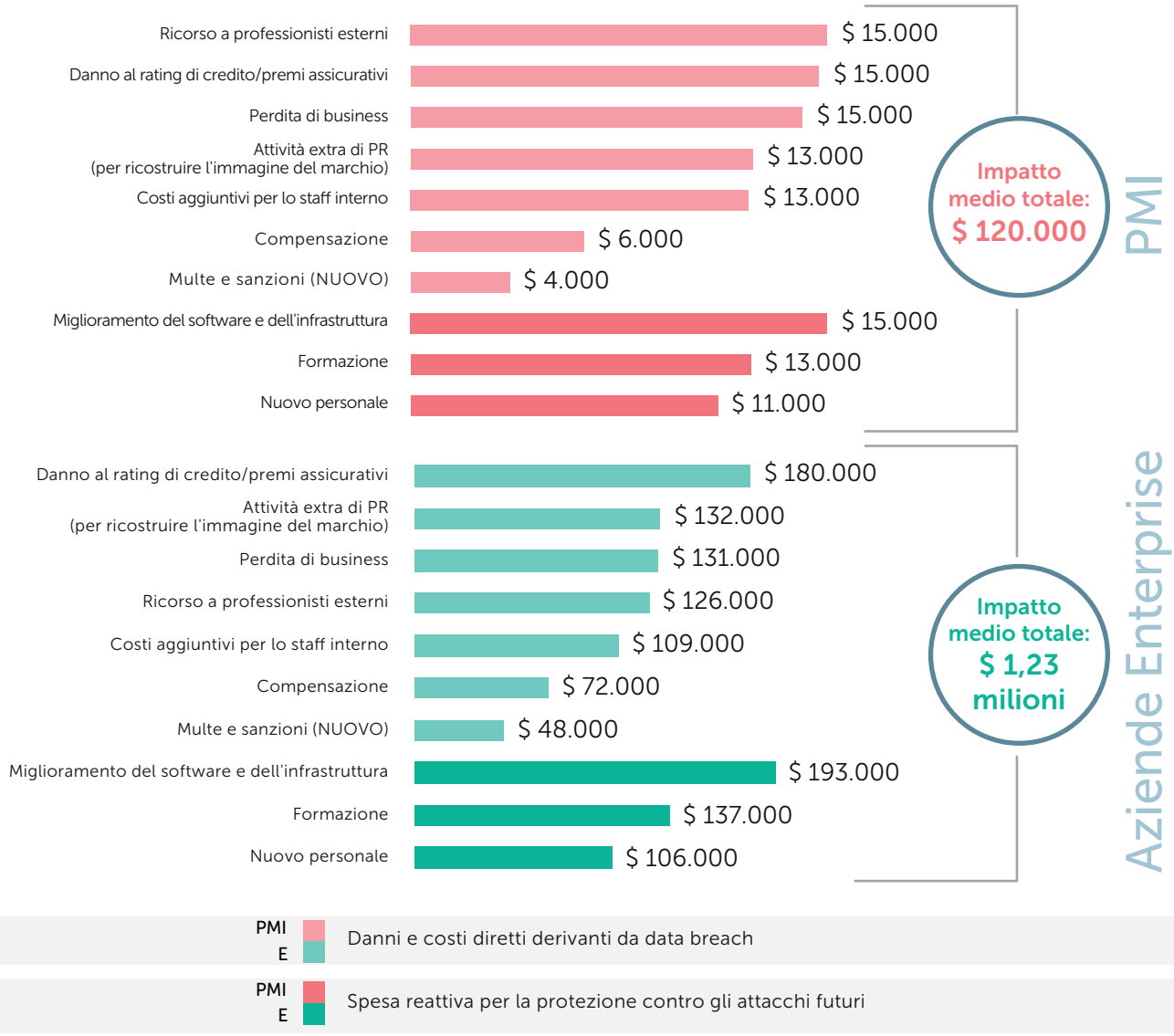



***Figura 1:*** *Impatto finanziario medio di un data breach a livello globale*

È interessante notare che i costi connessi al ripristino da un data breach variano notevolmente tra le aree geografiche. Per le PMI i costi medi sono aumentati in tutte le sette aree geografiche incluse nello studio, con il Nord America ($ 149.000) e l'Asia Pacifica con la Cina ($ 135.000) classificati come i più costosi e la Russia ($ 74.000) come la meno costosa.

E lo stesso vale per le aziende Enterprise Il costo medio di un data breach è pari a $ 1,7 milioni per le aziende Enteprise in Giappone, $ 1,6 milioni in Nord America e $ 1,5 milioni in Asia Pacifica con la Cina. Per quanto riguarda le PMI, i data breach hanno il più basso impatto finanziario per le aziende in Russia ($ 246.000), con un aumento di soli $ 6.000 dal 2017.

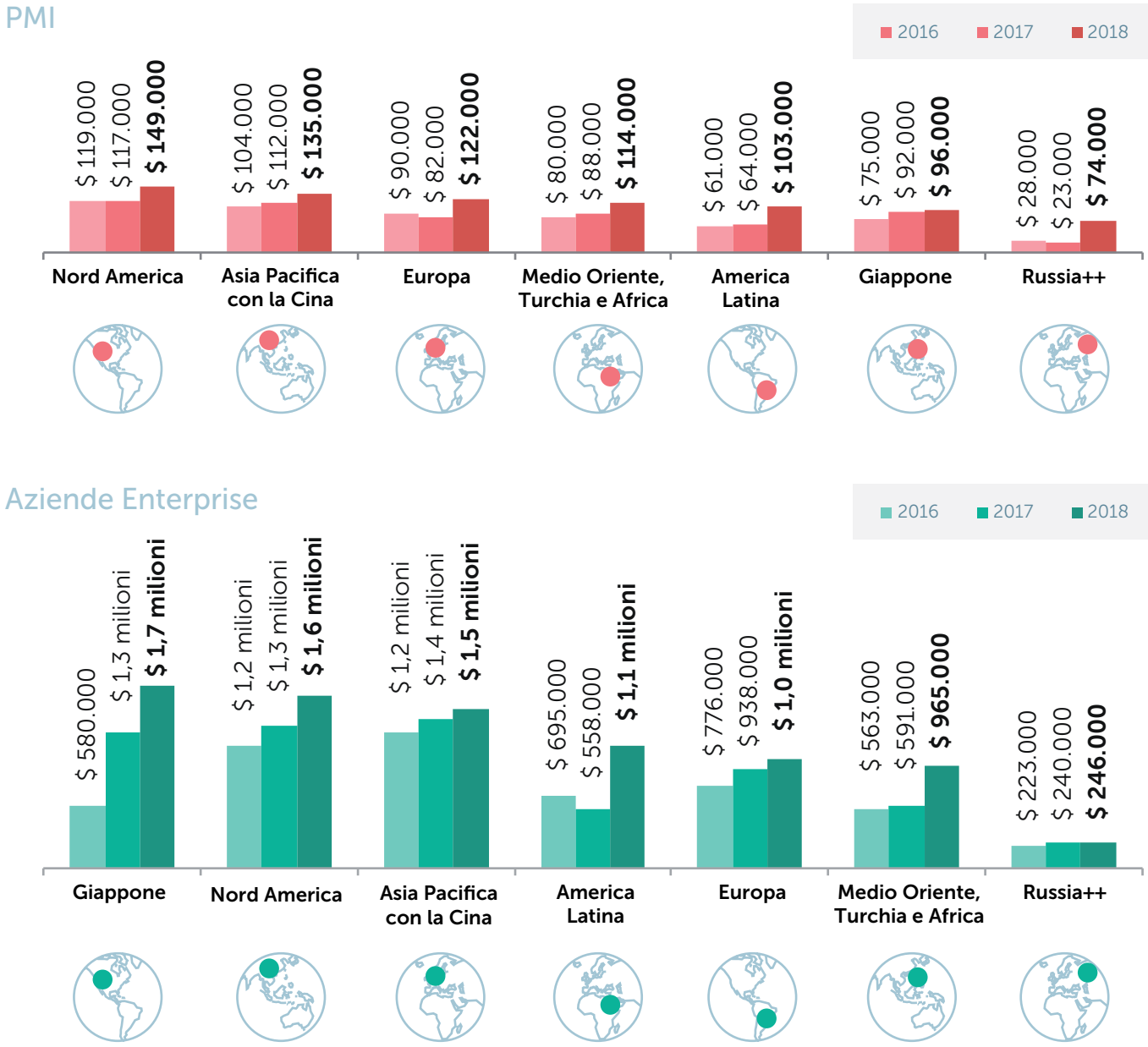



***Figura 2:*** *Impatto finanziario medio di un data breach per area geografica*

Qualunque sia il motivo, i costi sono in evidente crescita generalizzata e pongono gravi pressioni finanziarie sulle aziende grandi e piccole, identificando il motivo per cui la sicurezza sta diventando una problematica di rilievo ed essendo le imprese in continua trasformazione. Ma che fine fa esattamente tutto questo denaro extra speso?

# Perché i costi sono in aumento?

Con le spese sostenute in seguito a un data breach può essere difficile per le imprese identificare esattamente dove viene investito il loro denaro. Il nostro report ha rilevato che la realizzazione di miglioramenti tecnici a seguito di un incidente porta soprattutto un pesante onere finanziario per le aziende Enteprise e per le piccole e medie imprese, oltre a danni ai premi assicurativi e ad azioni per migliorare le competenze interne.

Per le aziende Enterprise, il miglioramento di software e infrastruttura rappresenta il costo maggiore a seguito di un data breach, pari a $ 193.000, seguito da danni al rating/premi assicurativi ($ 180.000) e investimenti nella formazione ($ 137.000). Il modello è simile per le piccole e medie imprese, dove quattro diversi costi condividono la prima posizione: miglioramenti infrastrutturali, impiego di professionisti esterni, danni al rating e perdita di business. Il tutto costa alle PMI $ 15.000 in media.

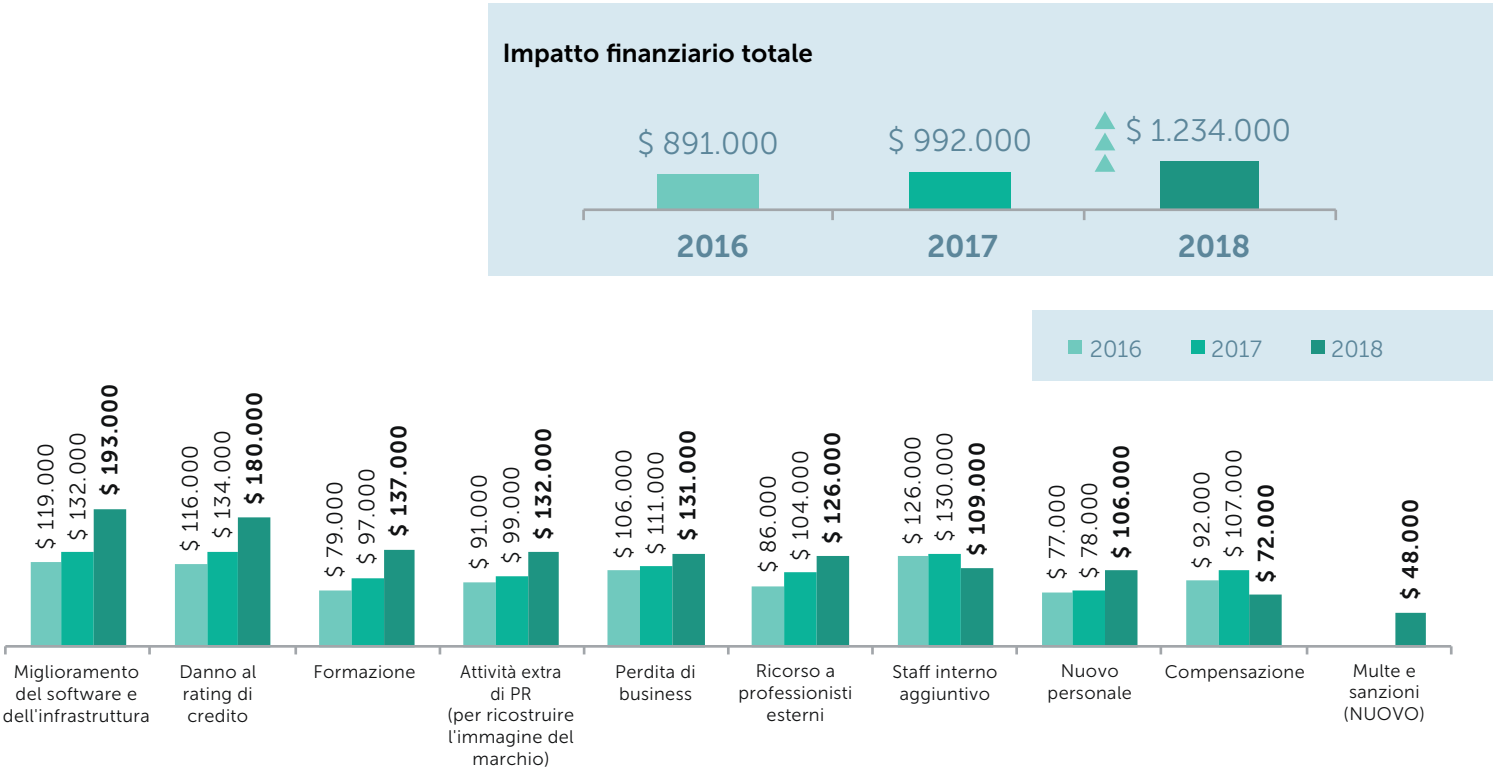



***Figura 1:*** *Rilevamento dell'impatto finanziario di un data breach per le aziende*

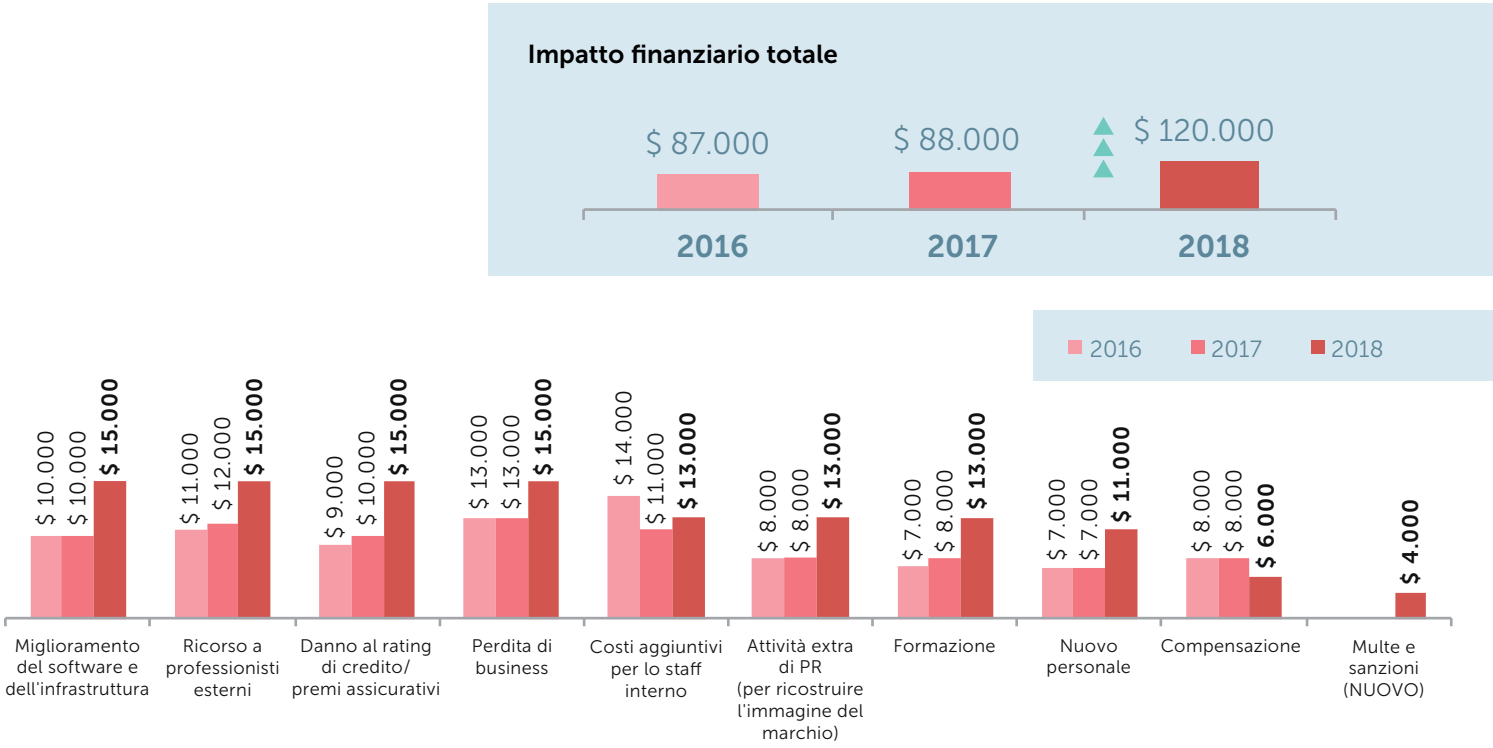



***Figura 2:*** *Rilevamento dell'impatto finanziario di un data breach per le PMI*

Ci sono anche alcune interessanti variazioni geografiche che sono degne di menzione. Per esempio, l'impiego di professionisti esterni è una delle conseguenze più costose di una violazione della sicurezza per le PMI in Nord America, America Latina ed Europa, suggerendo che le imprese in queste aree geografiche hanno maggiore bisogno di competenze aggiuntive.

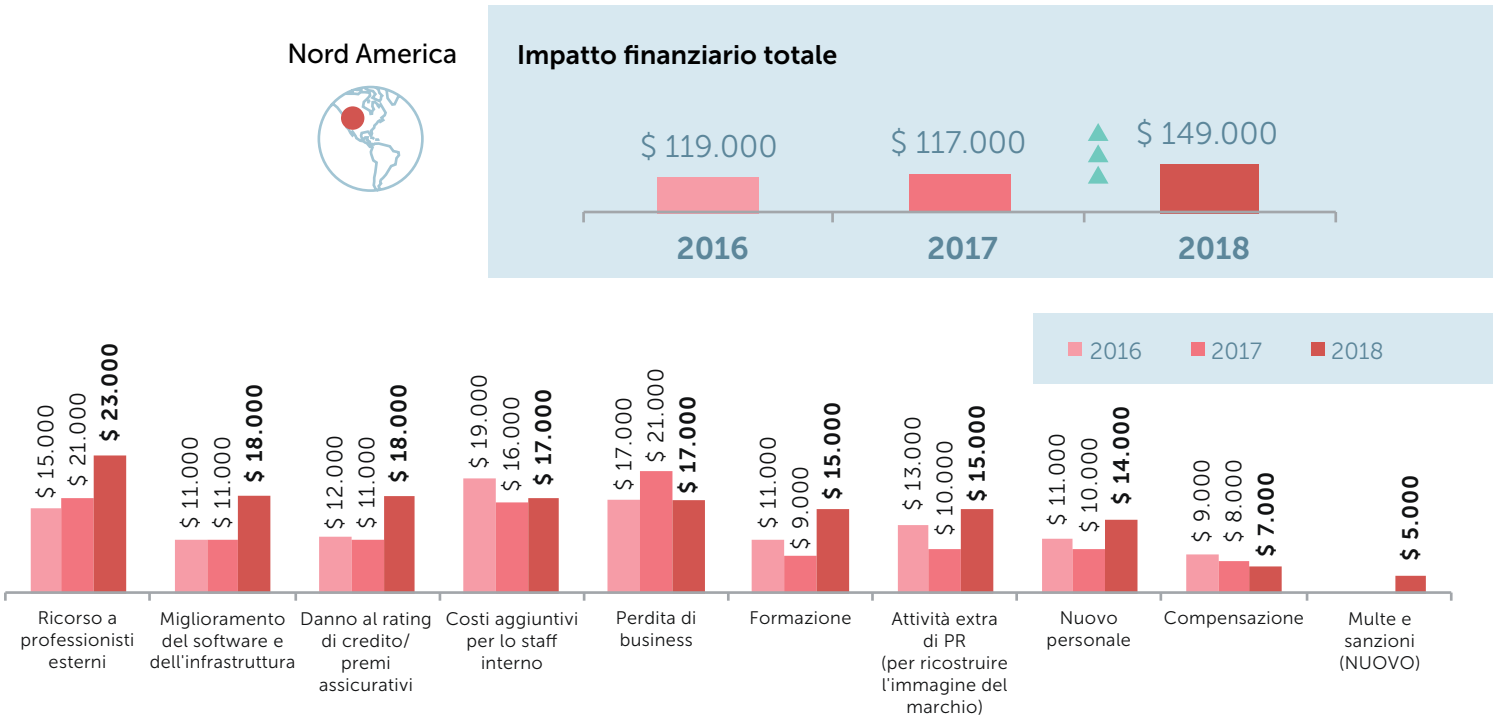



***Figura 3:*** *Impatto finanziario di un data breach per le PMI in Nord America*

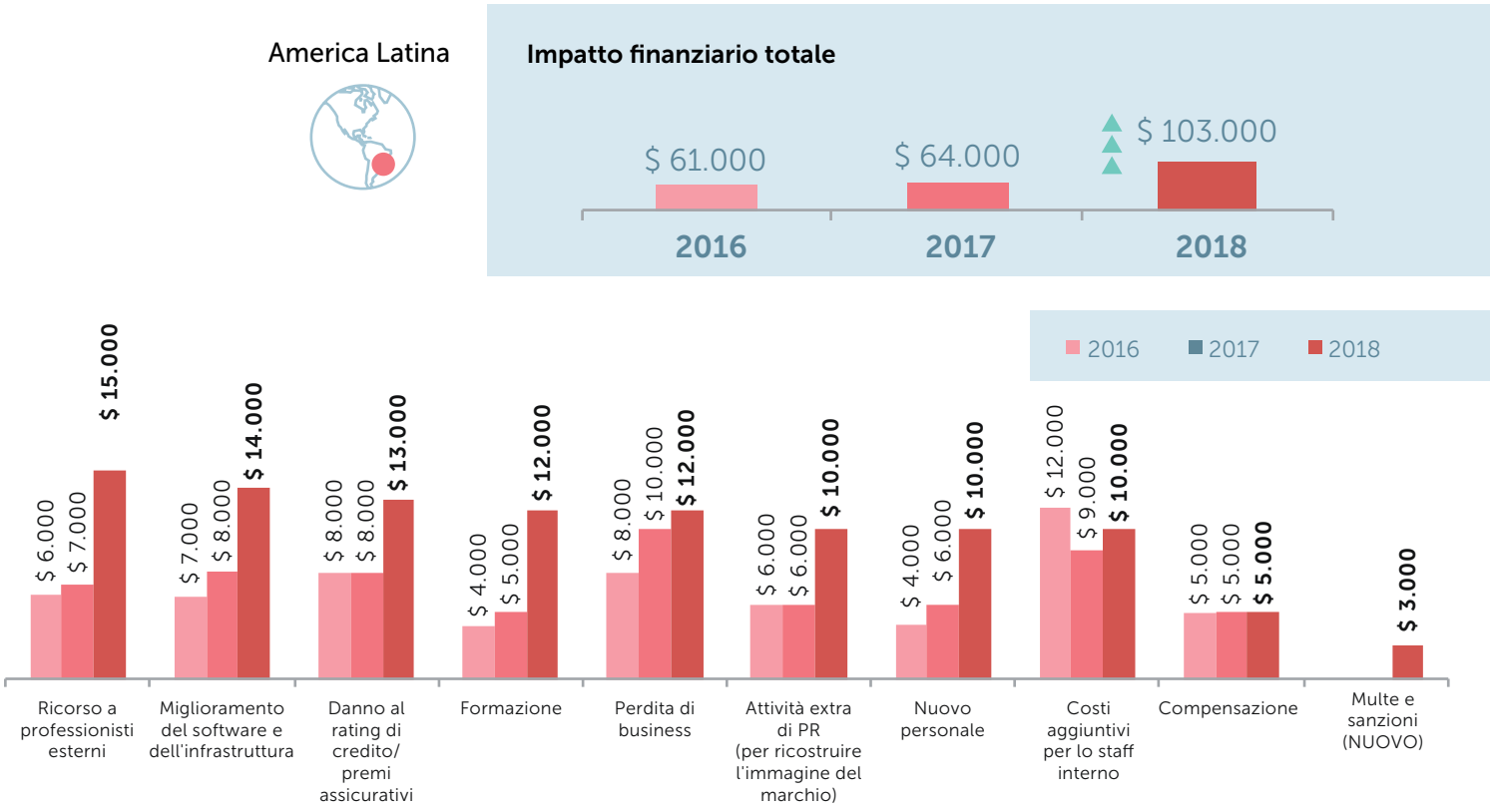



***Figura 4:*** *Impatto finanziario di un data breach per le PMI in America Latina*

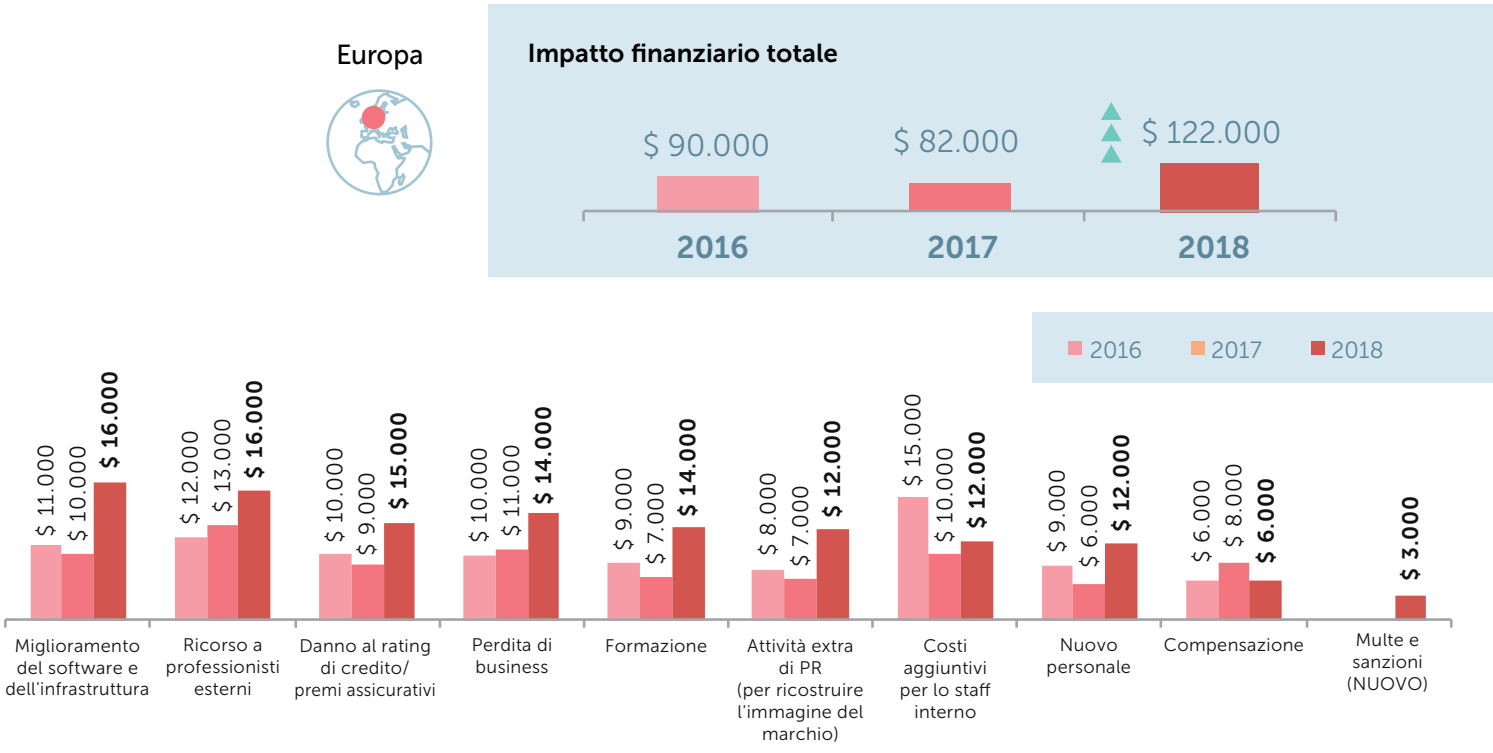



***Figura 5:*** *Impatto finanziario di un data breach per le PMI in Europa*

Inoltre, ci sono alcune aree geografiche dove la minimizzazione o il ripristino della reputazione è molto più che una priorità. L'attività extra di PR per la ricostruzione dell'immagine del marchio è classificata come il secondo fattore più costoso per le piccole e medie imprese in Giappone ($ 13.000) e il terzo più costoso per le aziende Enteprise in Medio Oriente, Turchia e Africa ($ 113.000) e le PMI in Russia ($ 8.000).

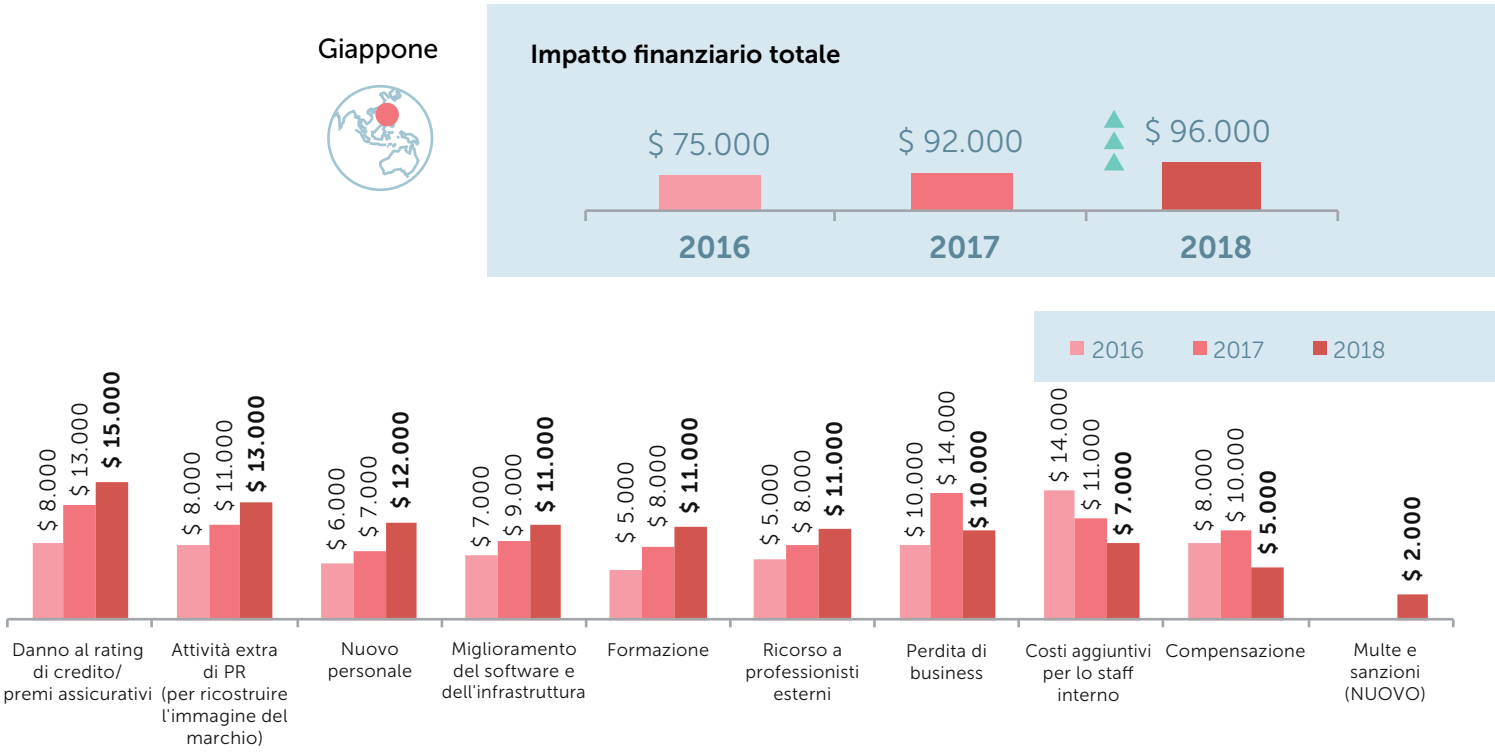



***Figura 6:*** *Impatto finanziario di un data breach per le PMI in Giappone*

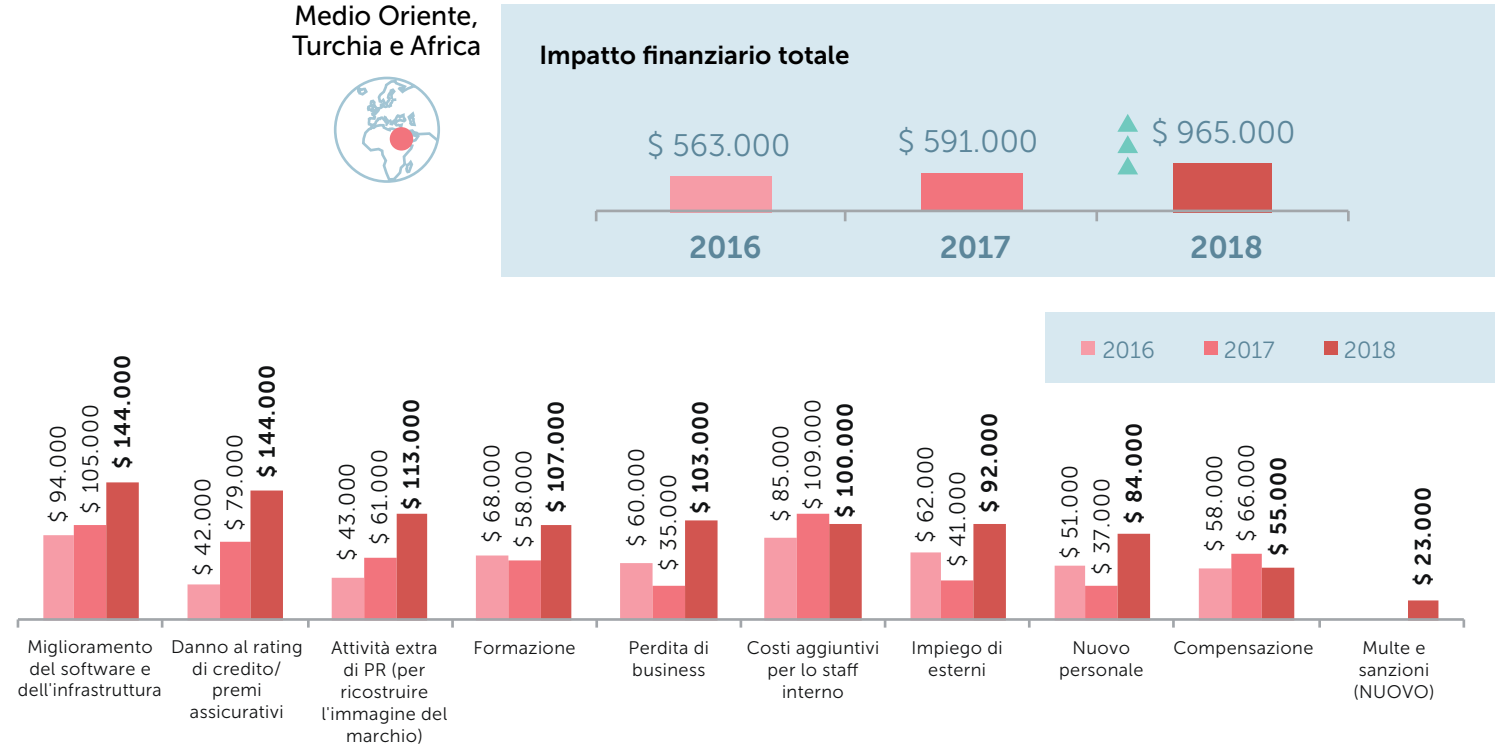



***Figura 7:*** *Impatto finanziario di un data breach per le aziende in Medio Oriente, Turchia e Africa*

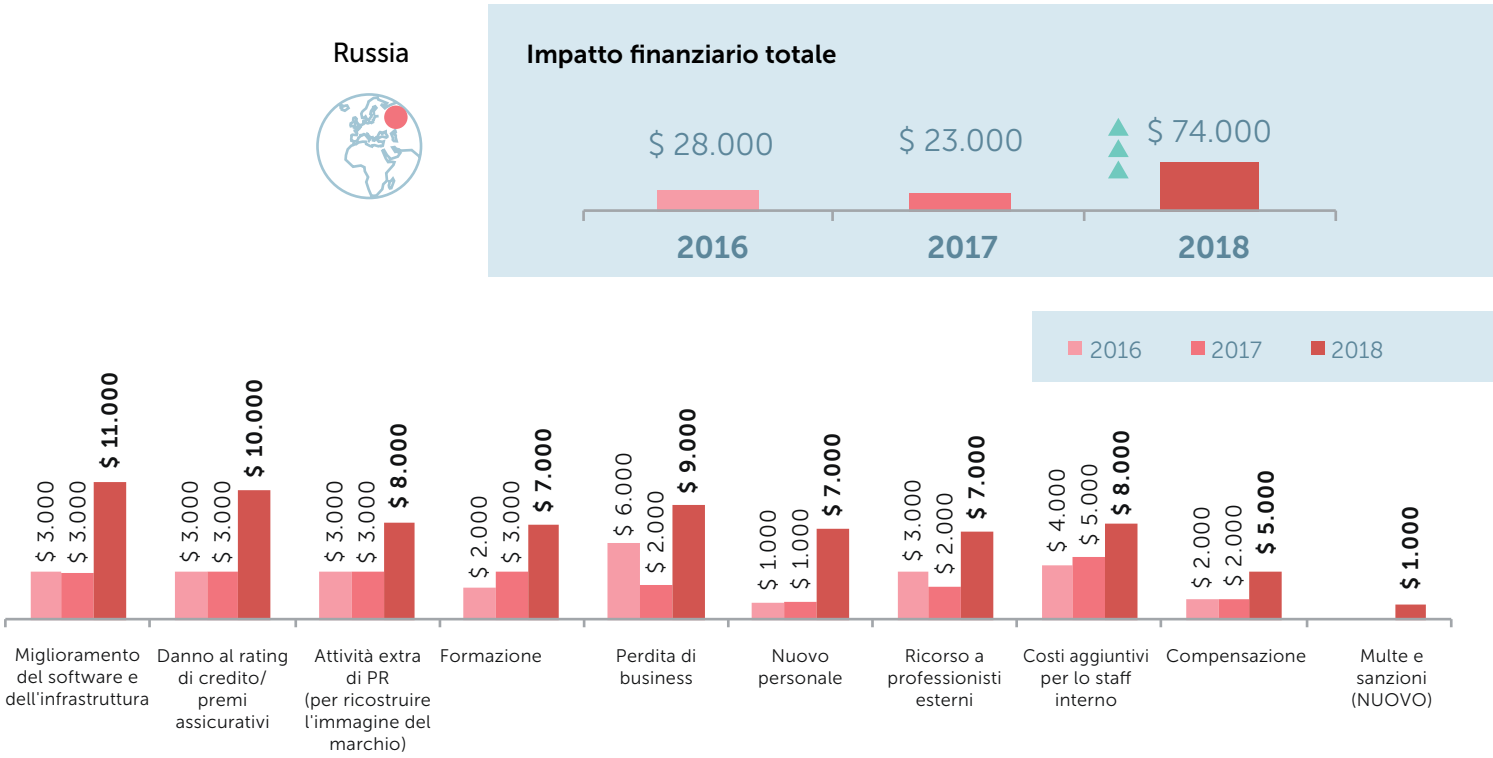



***Figura 8:*** *Impatto finanziario di un data breach per le PMI in Russia*

Infine, le PMI nell'area geografica Asia Pacifica con la Cina devono misurarsi con la perdita di business a seguito di un data breach, con un costo medio di $ 17.000, che suggerisce che i clienti locali sono particolarmente diffidenti verso quelle aziende che hanno subito una violazione.

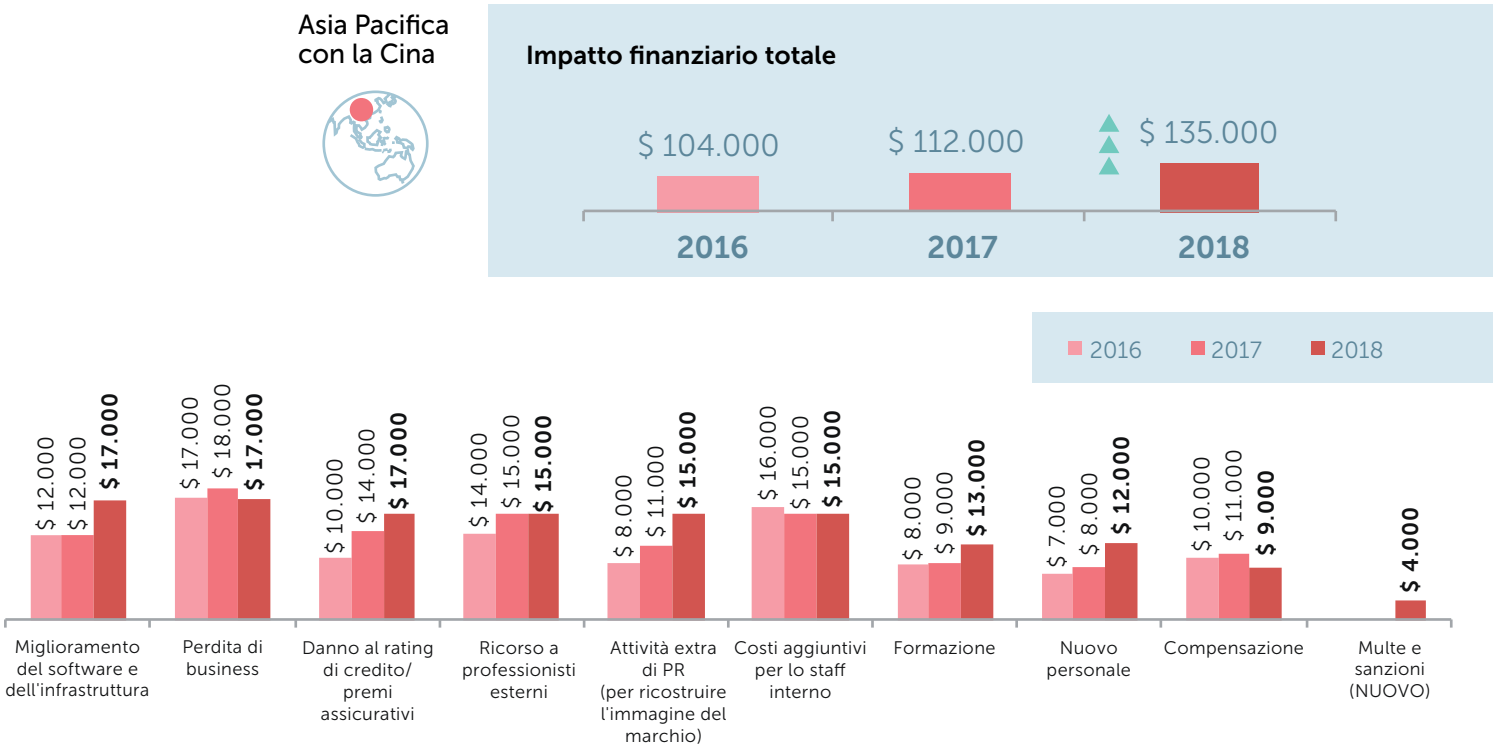



***Figura 9:*** *Impatto finanziario di un data breach per le PMI in Asia Pacifica con la Cina*

# Gli attacchi più costosi: tutti i dati a portata di mano

Non è sufficiente sapere quanto costa un data breach. Ulteriori informazioni a riguardo possono provenire dalla scoperta dei diversi tipi di minaccia che le aziende devono affrontare e da cui, in caso di successo, il ripristino è più costoso. **I primi cinque tipi di data breach con il più grande impatto finanziario per le aziende Enterprise sono stati:**

- Attacchi mirati - **$ 1,64 milioni**
- Incidenti che interessano l'infrastruttura IT in hosting - **$ 1,47 milioni**
- Perdita fisica di supporti o dispositivi di proprietà dell'azienda - **$ 1,42 milioni**
- Incidenti che coinvolgono dispositivi IoT - **$ 1,41 milioni**
- Incidenti che interessano servizi in cloud - **$ 1,38 milioni**

**I primi cinque per le PMI sono stati:**

- Incidenti che interessano l'infrastruttura IT in hosting - **$ 179.000**
- Incidenti che coinvolgono dispositivi IoT - **$ 148.000**
- Incidenti che interessano gli ambienti virtualizzati - **$ 146.000**
- Incidenti che interessano servizi in cloud - **$ 130.000**
- Incidenti che interessano terze parti con cui condividiamo i dati - **$ 130.000**

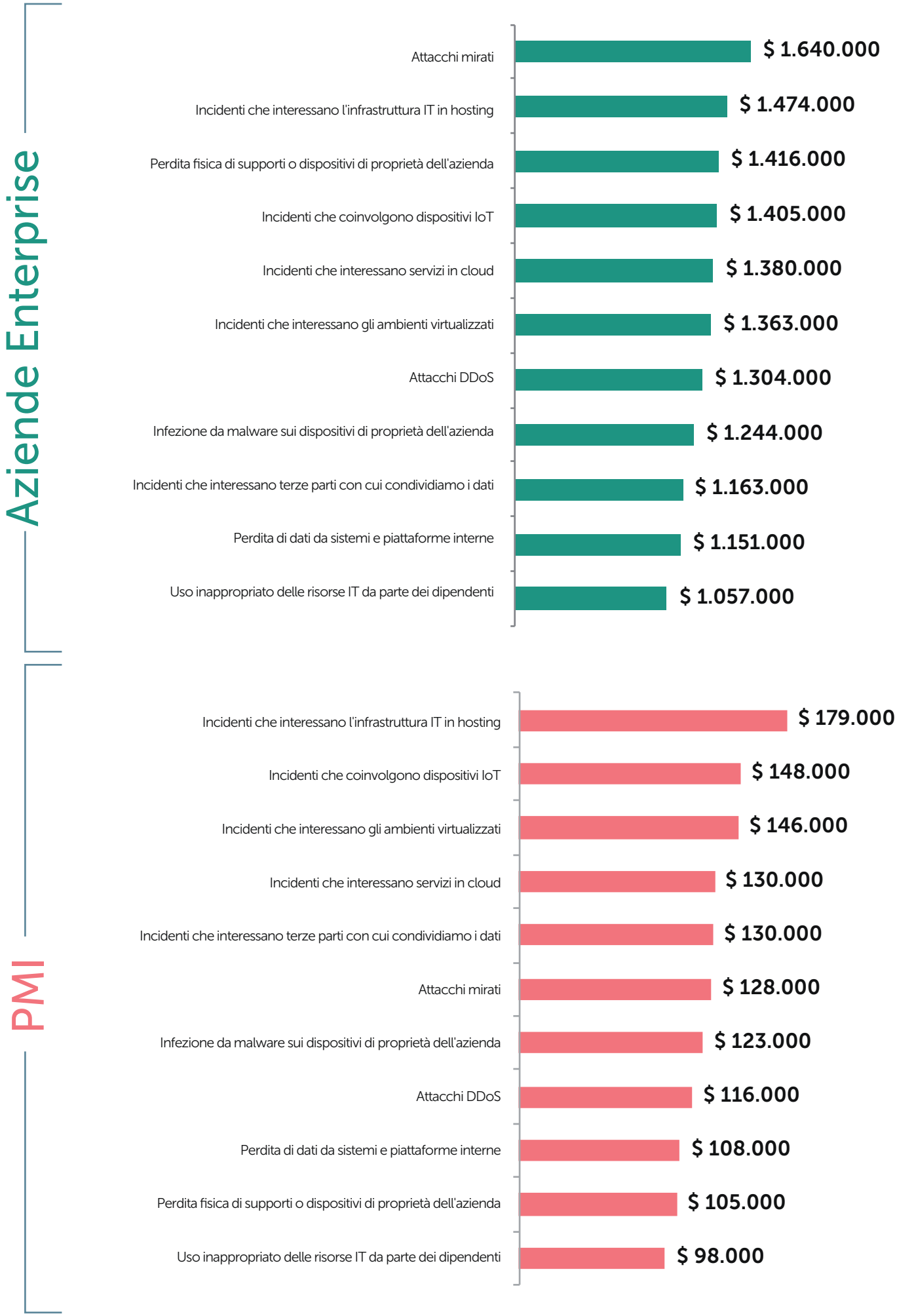



**Figura 9:** Tipi di data breach e relativo impatto finanziario

Nel processo di adozione delle strategie di digital transformation, spesso le aziende collaborano con terze parti per eseguire la migrazione dei dati o modificare l'accesso alla propria infrastruttura. Le aziende fanno affidamento a fornitori esterni per l'adozione delle misure necessarie per la sicurezza.

**Tuttavia**, i costi dei data breach causati da terze parti mostrano che questa fiducia è spesso mal riposta, poiché eventuali errori da parte del fornitore possono avere un impatto diretto sul cliente.

Quando si tratta di incidenti di cybersecurity, il quadro è molto simile, con le terzi parti che diventano causa degli incidenti più costosi. **I cinque principali riguardanti le aziende Enterprise sono stati:**

- Attacchi mirati - **$1,11 milioni**
- Incidenti che interessano l'infrastruttura IT in hosting - **$ 1,09 milioni**
- Incidenti che coinvolgono dispositivi IoT - **$ 993.000**
- Incidenti che interessano servizi in cloud - **$ 942.000**
- Perdita di dati da sistemi e piattaforme interne - **$ 909.000**

**Per le PMI, i primi cinque sono stati:**

- Incidenti che interessano l'infrastruttura IT in hosting - **$ 118.000**
- Incidenti che coinvolgono dispositivi IoT - **$ 98.000**
- Incidenti che interessano servizi in cloud - **$ 89.000**
- Attacchi mirati - **$ 87.000**
- Incidenti che interessano terze parti con cui condividiamo i dati - **$ 83.000**

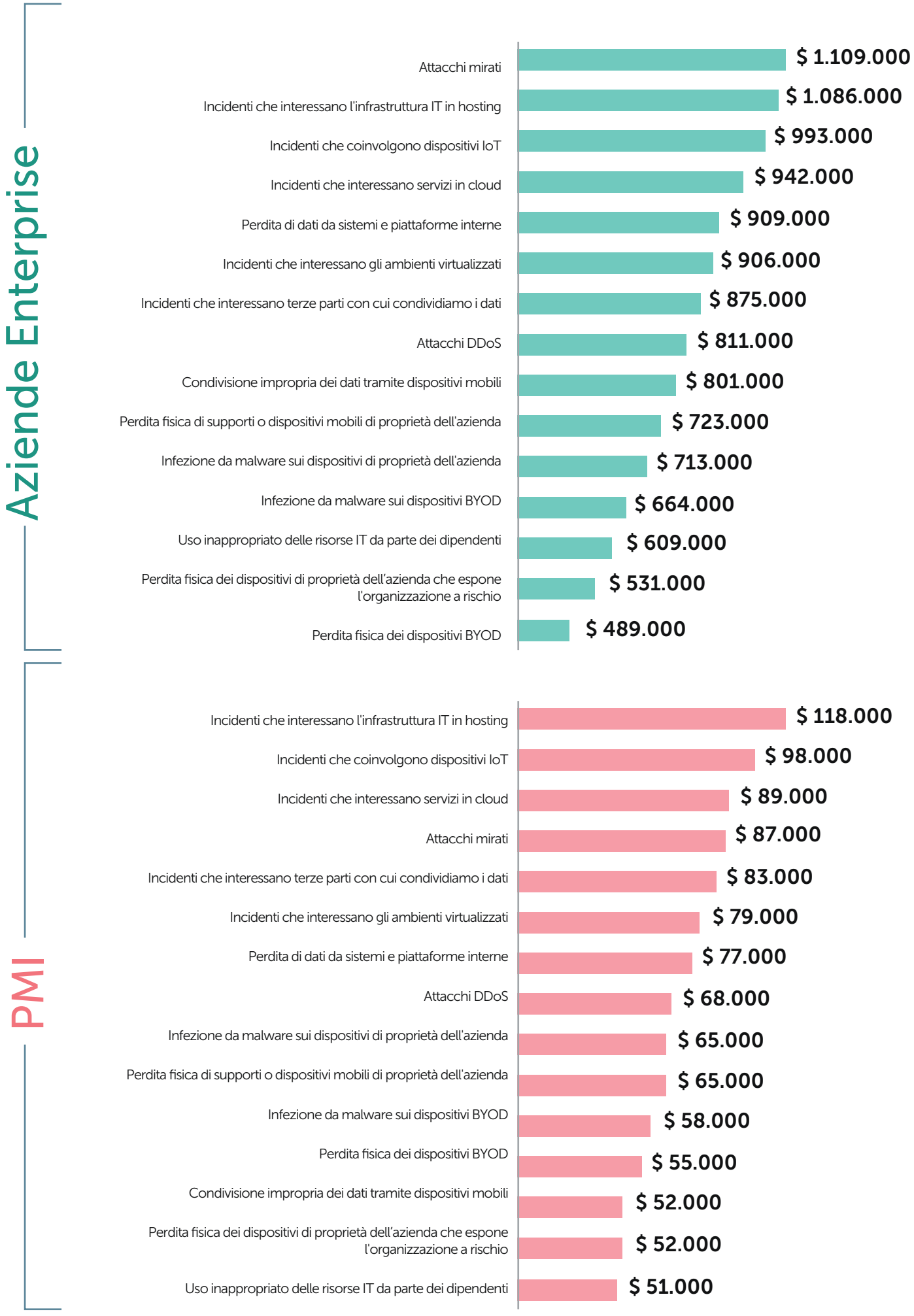



**Figura 10:** Tipi di incidenti di cybersecurity e relativo impatto finanziario

# La sicurezza IT è all'ordine del giorno del top management

I costi che le aziende devono sostenere a causa dei data breach e degli incidenti di sicurezza aumentano ogni anno. Pertanto, la necessità di creare strumenti e processi per la difesa contro le attività dei cybercriminali diventa sempre più importante. Questa tendenza si riflette sulla quantità di denaro che le aziende Enterprise e le PMI spendono per la sicurezza IT.

I budget per la sicurezza IT sono infatti aumentati nelle aziende di tutte le dimensioni nel corso degli ultimi dodici mesi. Nelle aziende, la percentuale del budget IT che viene speso per la sicurezza è aumentata dal 23% nel 2017 a oltre un quarto (26%) nel 2018, per una spesa pari a una media di $ 8,9 milioni.

Un modello simile può essere visto sia nelle PMI che nelle microimprese. Oggi le PMI spendono una media di $ 246.000 all'anno per la sicurezza IT, pari al 23% del budget IT complessivo rispetto al 20% nel 2017. Le microimprese mostrano il massimo aumento percentuale, con i budget per la sicurezza aumentati dal 16% ($2.000) al 20% ($4.000) della spesa IT totale.

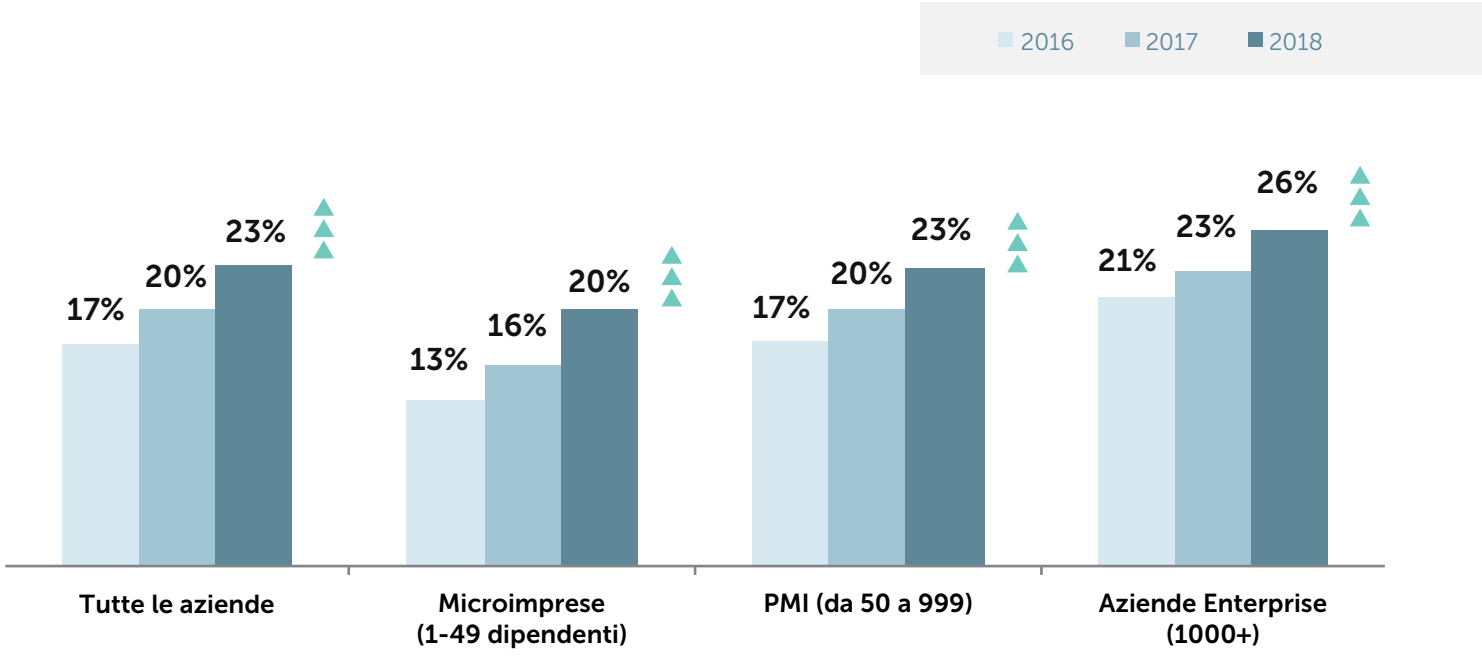



***Figura 11:*** *Rilevamento della percentuale del budget IT speso per la sicurezza*

Questi risultati sono coerenti in praticamente tutte le aree geografiche, ma è interessante notare la presenza di alcune anomalie, in particolare tra le aziende in Nord America e in Medio Oriente, Turchia e Africa, dove le proporzioni di spesa dei budget IT hanno mostrato l'aumento più grande dal 2017. I budget aziendali in Nord America sono cresciuti di 9 punti percentuali, raggiungendo il 28% del budget IT totale, mentre in Medio Oriente, Turchia e Africa è stato registrato un aumento di 8 punti percentuali, arrivando al 27%.

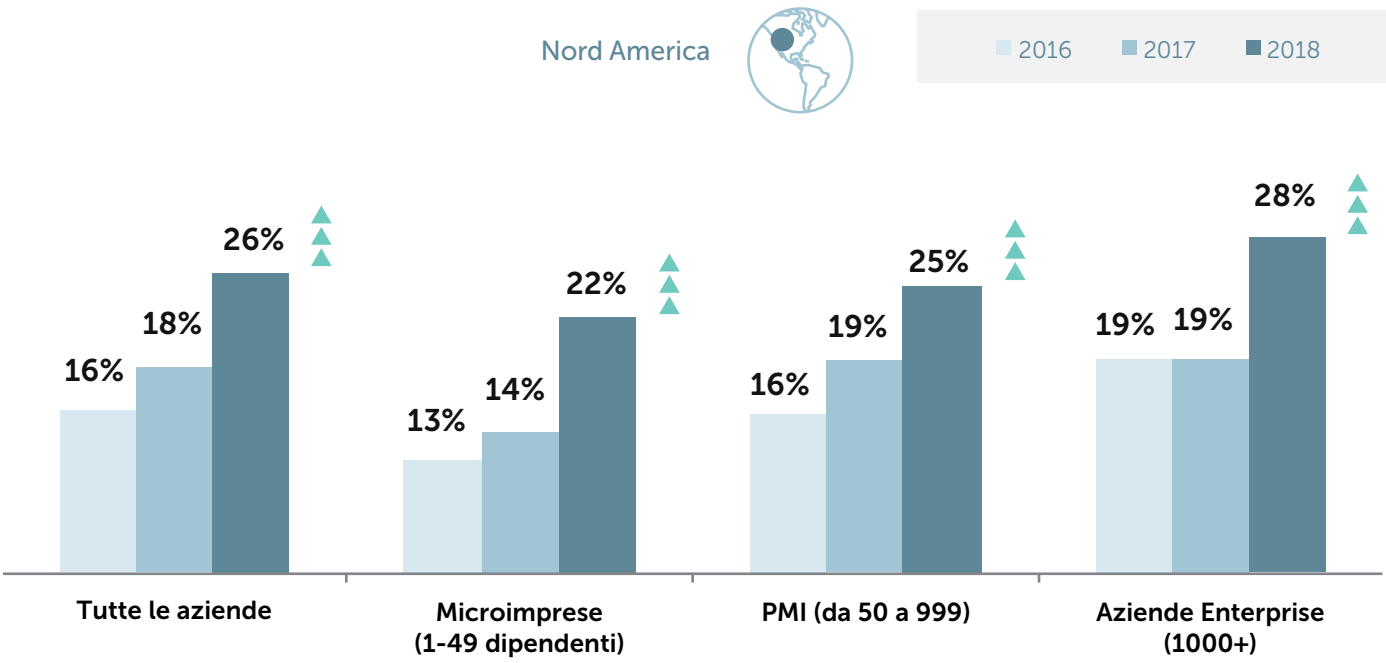



***Figura 12:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Nord America*

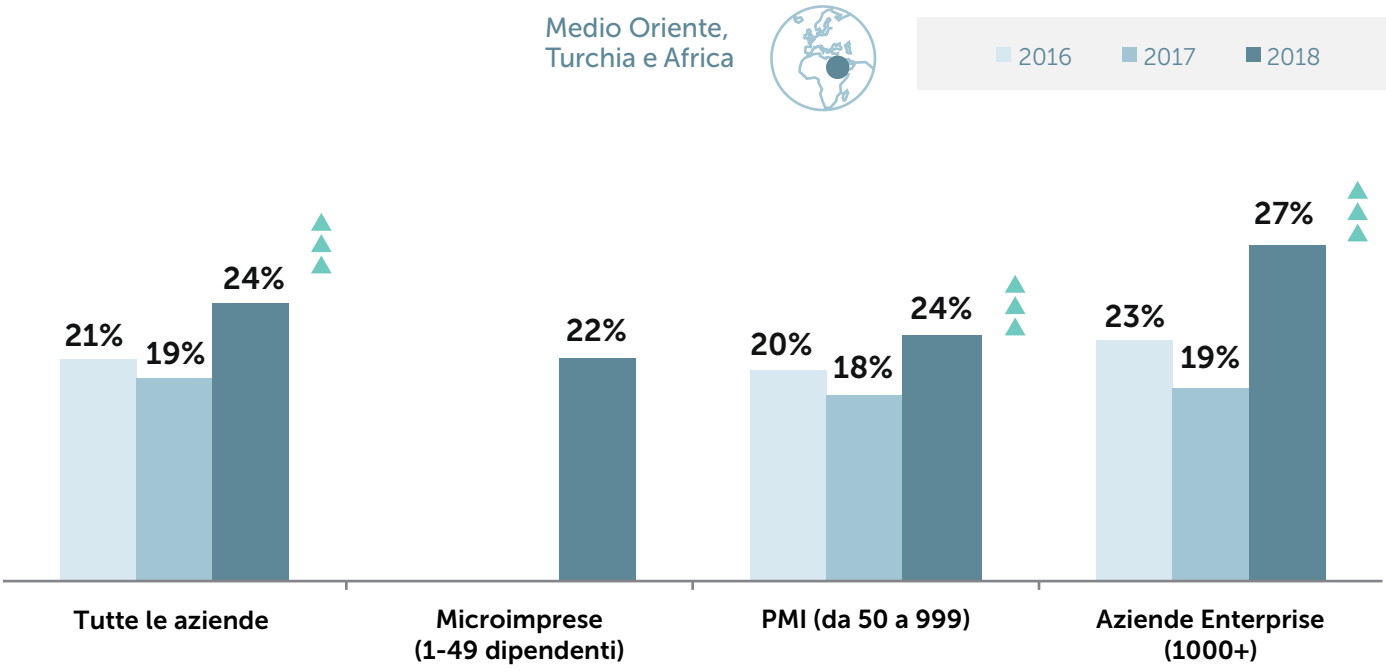



***Figura 13:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Medio Oriente, Turchia e Africa*

In confronto la percentuale dei budget destinata alla sicurezza IT è rimasta invariata per le PMI e per le aziende Enteprise in Asia Pacifica con la Cina (rispettivamente 23% e 26%) e per le Aziende Enterprise in Giappone (26%). Questa mancanza di movimento potrebbe essere spiegata dal fatto che le aziende giapponesi spendono per la sicurezza una media di $ 31,1 milioni: una cifra significativamente maggiore rispetto a qualsiasi altra area geografica.

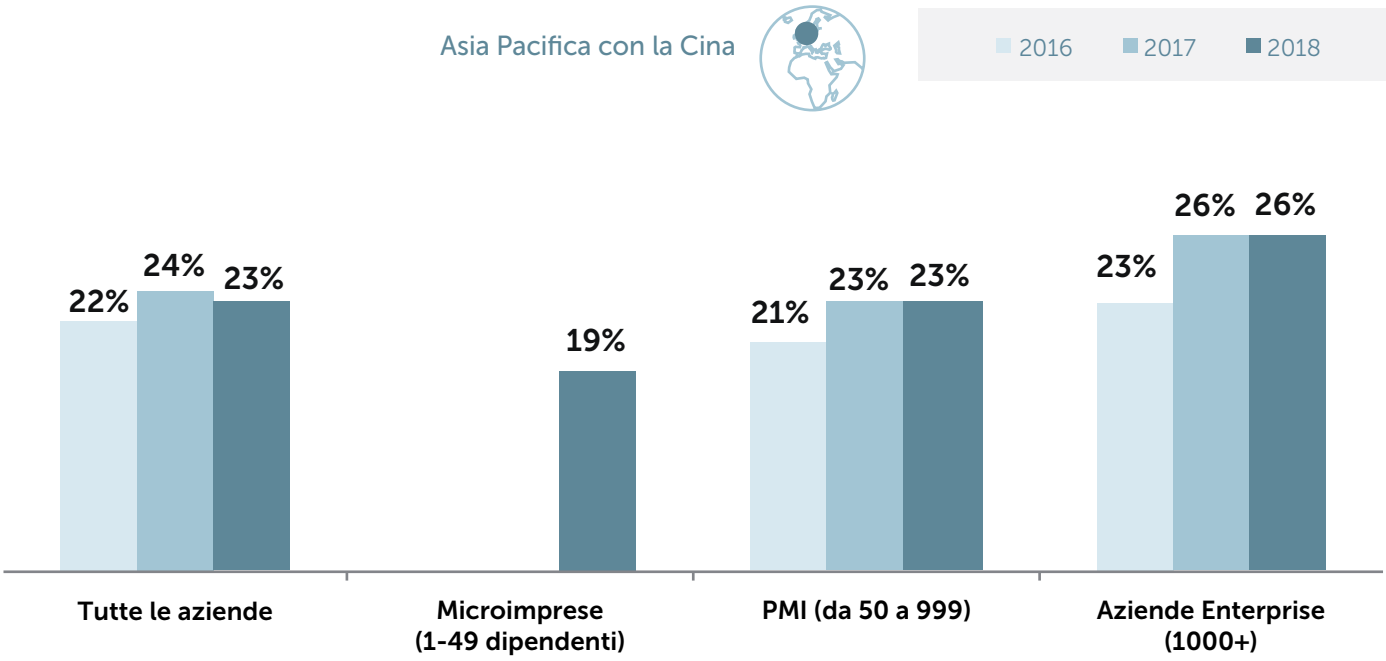



***Figura 14:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Asia Pacifica con la Cina*

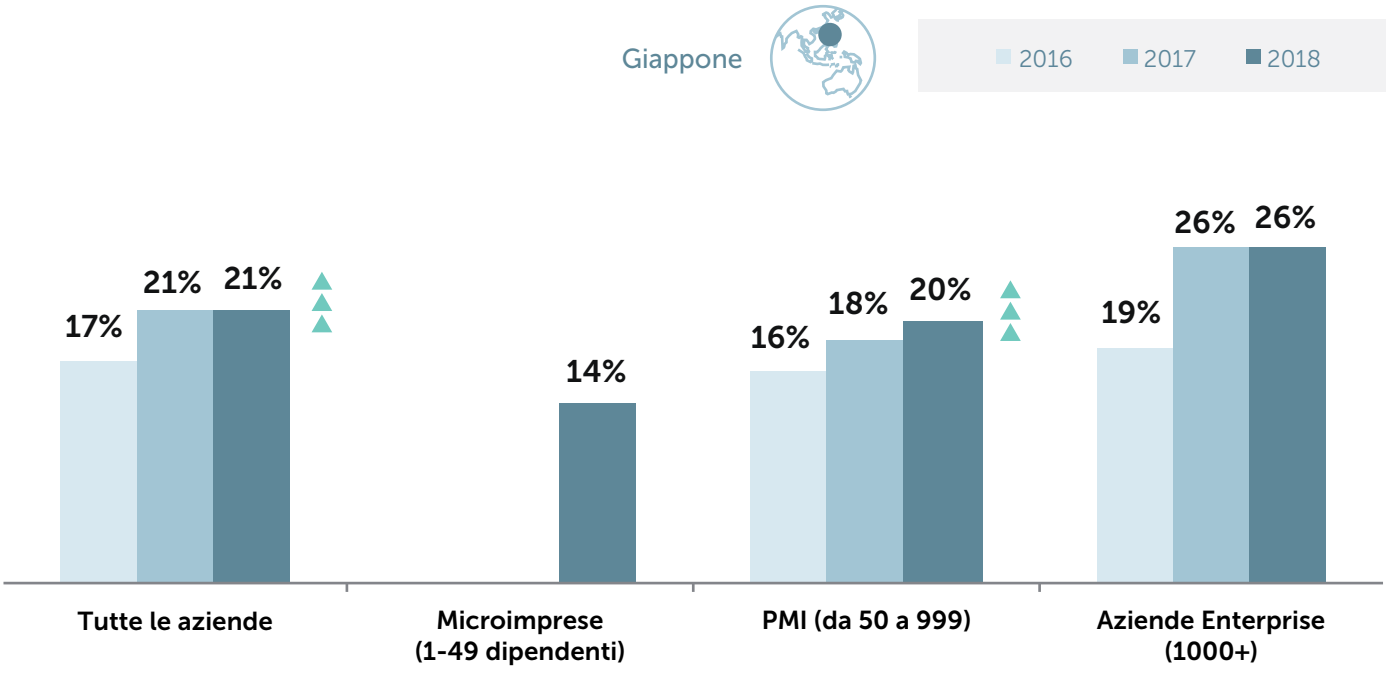



***Figura 15:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Giappone*

Inoltre, le imprese si aspettano che i propri budget per sicurezza IT crescano ancora in futuro. A livello globale, sia le microimprese che le aziende Enteprise prevedono che la quantità di denaro che spenderanno per la cybersecurity aumenterà del 15% nel corso dei prossimi tre anni, mentre le piccole e medie imprese prevedono un aumento del 14%.

Ancora una volta, ci sono alcune differenze tra le aree geografiche, come ad esempio per le piccole e medie imprese in Giappone che prevedono un aumento inferiore (7%) dei loro budget per la sicurezza IT. All'estremo opposto, le microimprese in America Latina prevedono che i propri budget per la sicurezza aumenteranno del 22%, un dato superiore alle aziende Enterprise e alle PMI in Medio Oriente, Turchia e Africa (19%) e in Russia (18%).

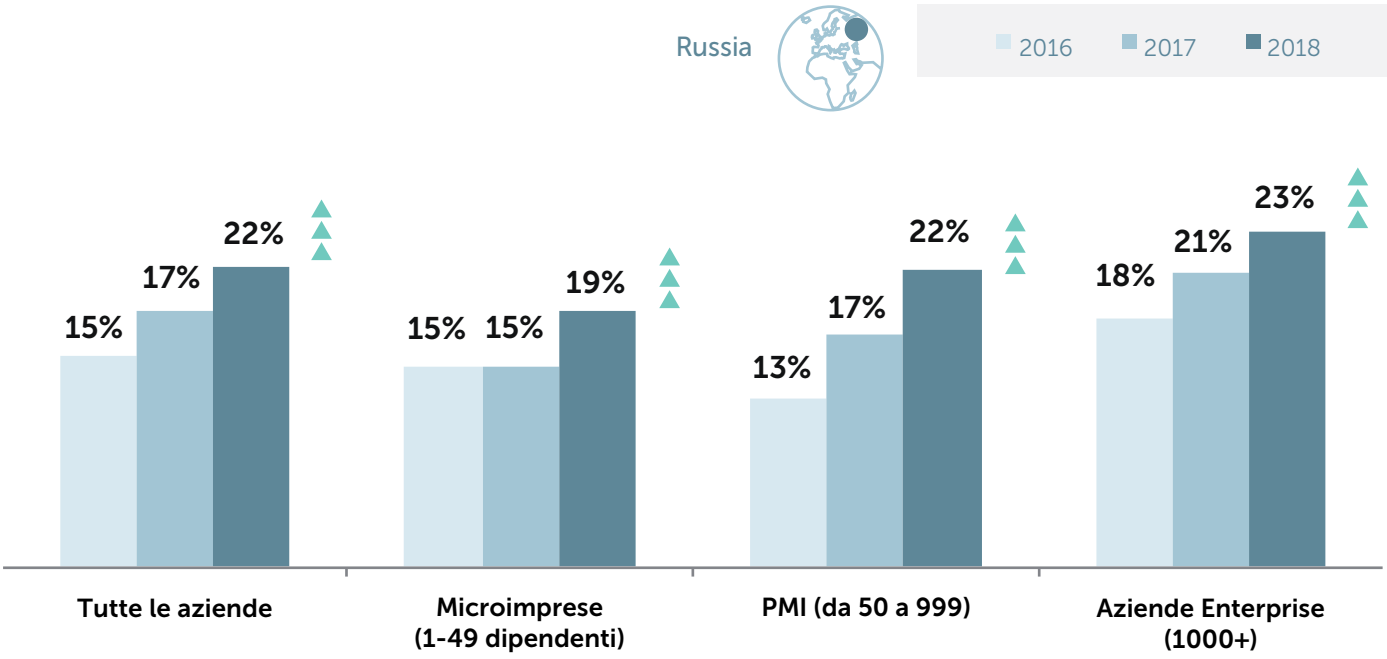



***Figura 16:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Russia*

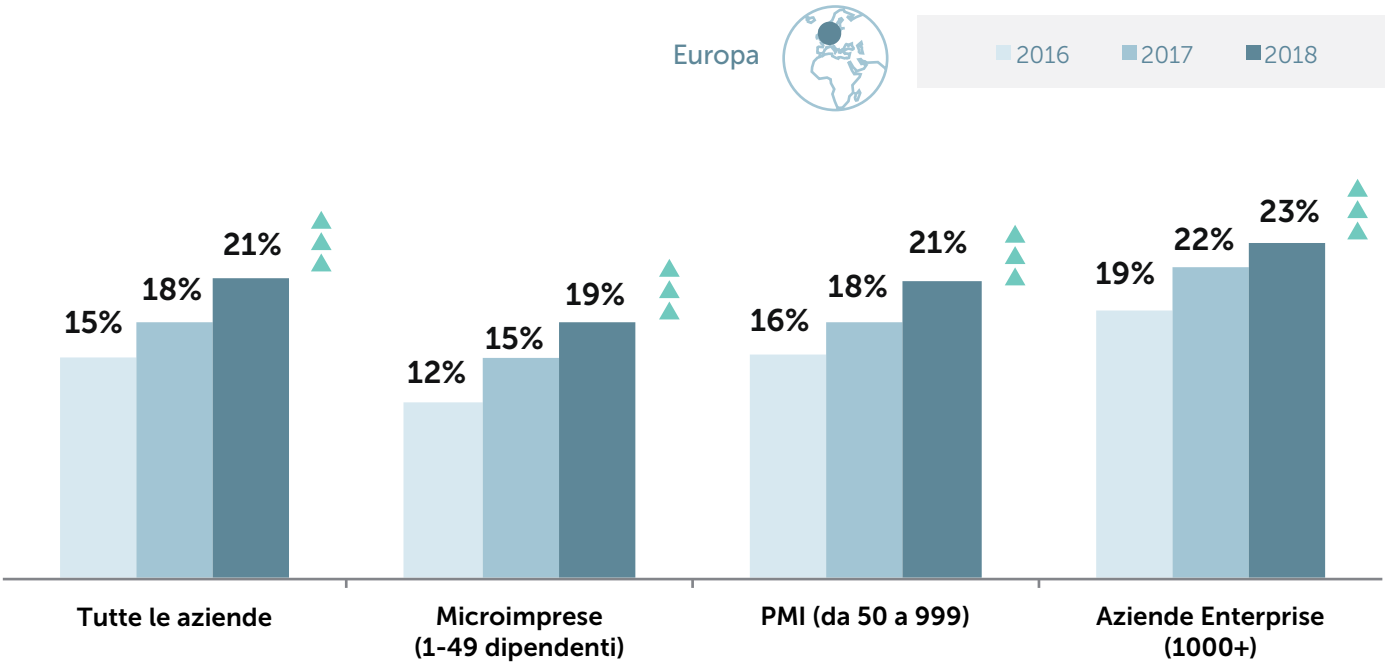



***Figura 17:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Europa*

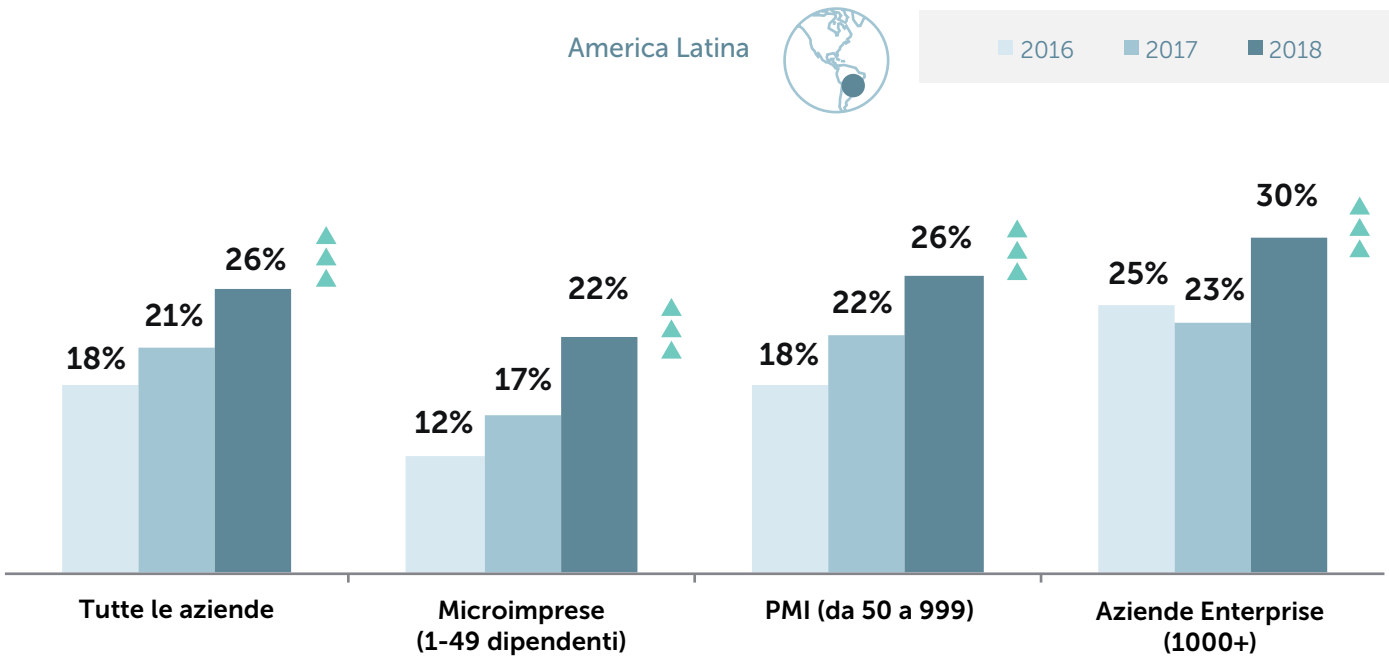
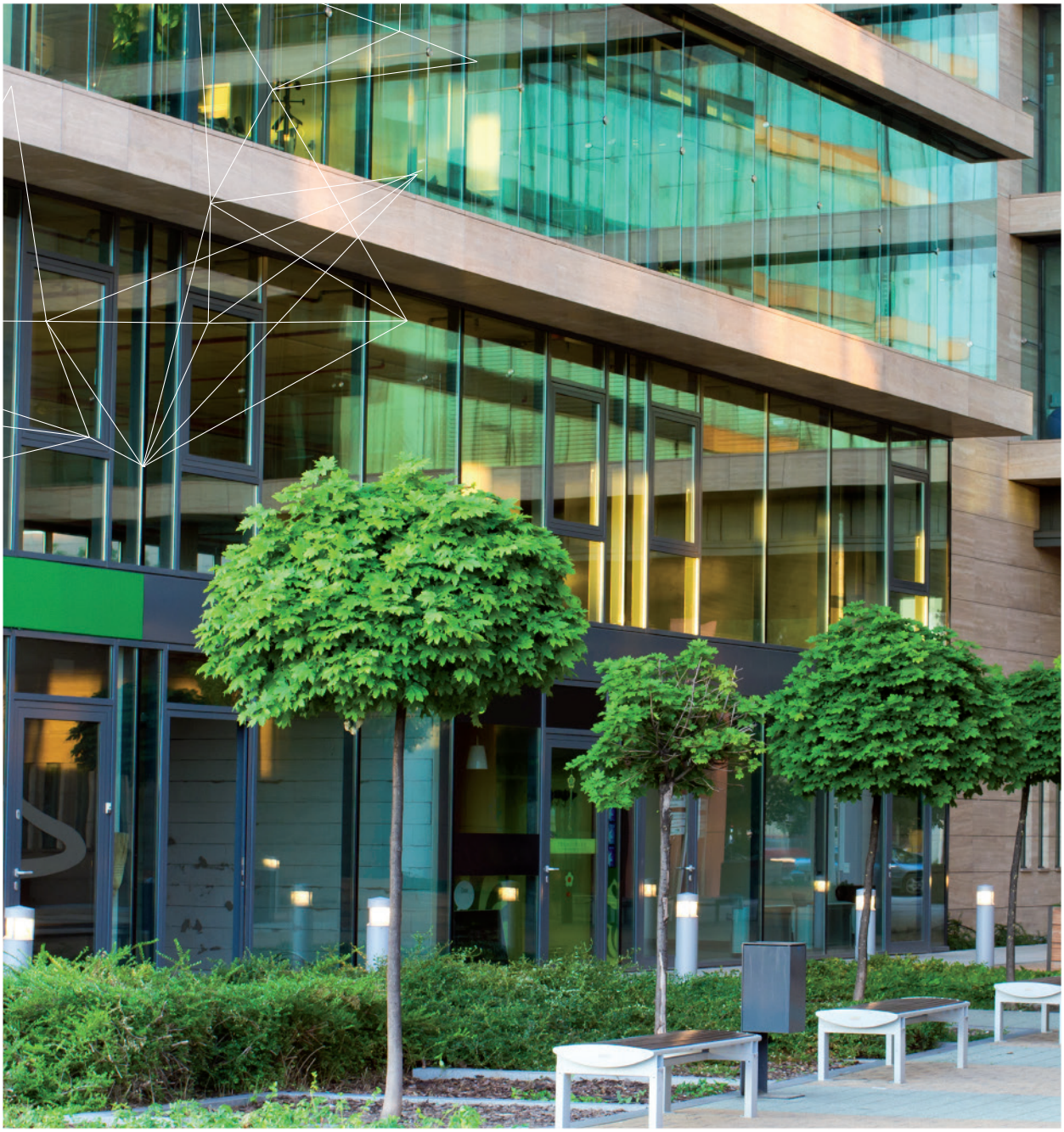



***Figura 18:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in America Latina*

# Motivazioni per investire nella sicurezza IT



**Con aziende di diverse dimensioni, diversi settori e diverse esigenze da prendere in considerazione, la domanda principale che abbiamo voluto fare alle imprese era esattamente che cosa le spinge a investire nella cybersecurity.**

Con una previsione di continua crescita dei budget IT nei prossimi tre anni, le imprese sono consapevoli del fatto che vi è una chiara necessità di investire nella sicurezza IT sia ora che in futuro. Come rilevato dal nostro report vi sono alcuni fattori chiave che motivano le imprese a investire il proprio denaro dove è necessario.

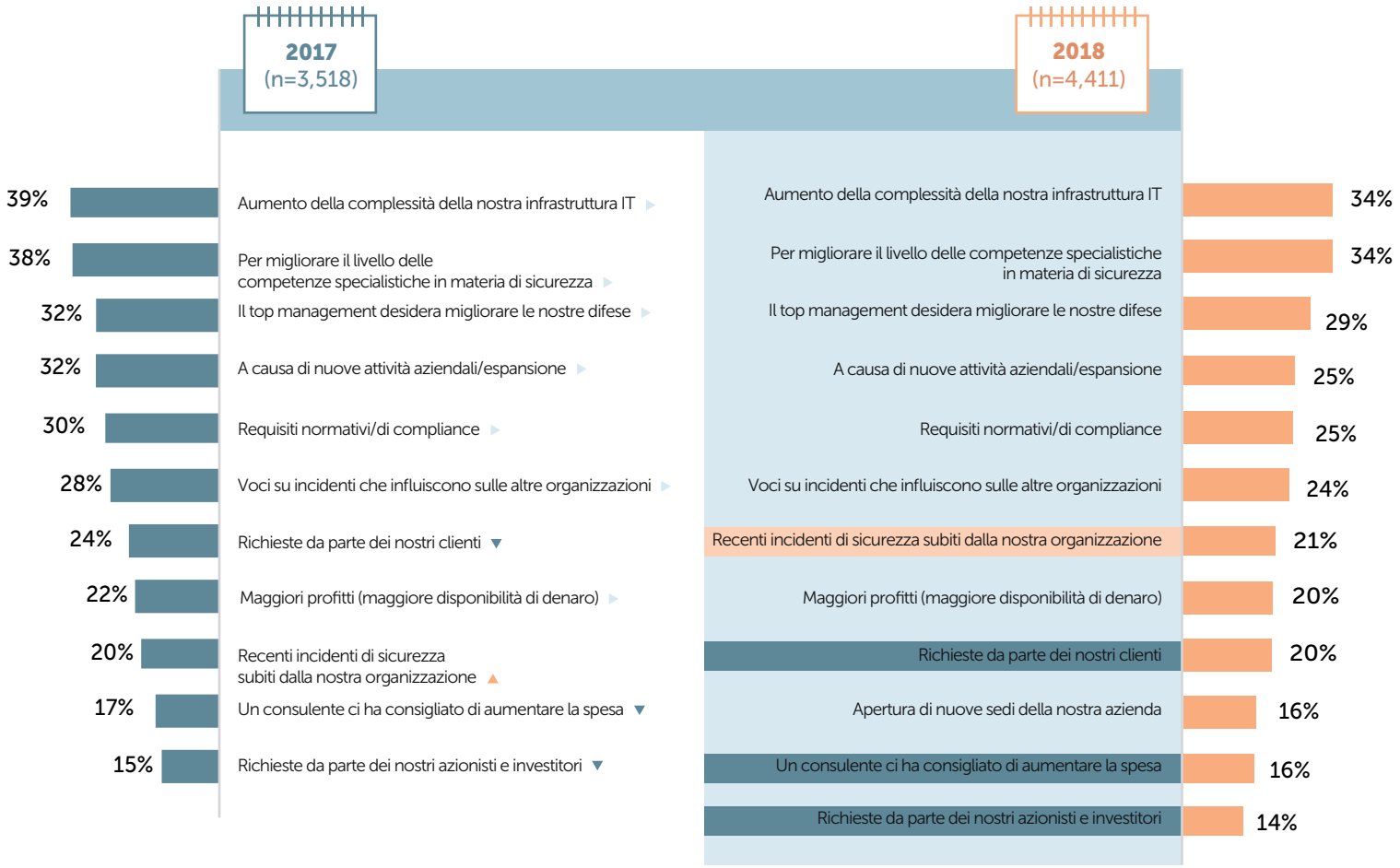



***Figura 20:*** *Tre motivazioni principali per investire nella sicurezza IT in tutte le aree geografiche*

Come mostra il grafico in alto, la maggiore complessità dell'infrastruttura IT ha conservato la prima posizione, insieme al miglioramento delle competenze specialistiche in materia di sicurezza (entrambe al 34%), nella classifica dei principali fattori di motivazione per investire nella sicurezza IT in tutte le aree geografiche. Seguono le pressioni del top management (29%) (suggerendo che i business leader si stanno interessando maggiormente alla cybersecurity) e l'impatto delle nuove attività aziendali nonché l'adeguamento ai requisiti di compliance (25%).

La richiesta da parte di azionisti e investitori (14%) è stata identificata come il motivatore meno importante per un investimento nella sicurezza IT, appena dietro quelle aziende che hanno aumentato la spesa per la sicurezza su consiglio di un consulente (16%).

Poiché questa è un'analisi in cui i fattori geografici possono avere un influsso significativo, abbiamo preso in considerazione anche i tre principali fattori di motivazione per ciascuna area geografica da identificare e le somiglianze o le differenze che potrebbero spiegare come diverse aziende percepiscono l'importanza della cybersecurity.

Non sorprende che l'aumento della complessità delle infrastrutture IT si è classificato tra le prime tre motivazioni in tutte le aree geografiche, al primo posto in Nord America (34%), America Latina (33%) ed Europa (29%). Altrettanto importante è il miglioramento delle competenze specialistiche in materia di sicurezza, che rappresentava la principale motivazione degli investimenti in quattro delle aree geografiche incluse nello studio: Giappone (48%), Asia Pacifica con la Cina (41%), Medio Oriente, Turchia e Africa (37%) e Russia (36%). È probabile che questo risultato sia così basso in classifica per le già discusse lacune nelle competenze nel settore della cybersecurity. Gli esperti di sicurezza scarseggiano, il che significa che le imprese di tutti i settori si stanno impegnando a trovare persone con le competenze necessarie a contrastare i cyberattacchi più sofisticati.

| | Russia ++ | Nord America | Medio Oriente, Turchia e Africa | Asia Pacifica con la Cina | Giappone | America Latina | Europa |
|---|---|---|---|---|---|---|---|
| TOP-1 | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(36%)** | Aumento della complessità della nostra infrastruttura IT **(34%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(37%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(41%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(48%)** | Aumento della complessità della nostra infrastruttura IT **(33%)** | Aumento della complessità della nostra infrastruttura IT **(29%)** |
| TOP-2 | Aumento della complessità della nostra infrastruttura IT **(33%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(31%)** | Il top management desidera migliorare le nostre difese **(29%)** | Aumento della complessità della nostra infrastruttura IT **(41%)** | Aumento della complessità della nostra infrastruttura IT **(34%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(28%)** | Per migliorare il livello delle competenze specialistiche in materia di sicurezza **(27%)** |
| TOP-3/4 | Il top management desidera migliorare le nostre difese **(29%)** | Il top management desidera migliorare le nostre difese **(30%)** | Aumento della complessità della nostra infrastruttura IT **(29%)**<br>Voci su incidenti che influiscono sulle altre organizzazioni **(28%)** | Il top management desidera migliorare le nostre difese **(35%)** | Requisiti normativi/ di compliance **(26%)** | Apertura di nuove attività aziendali/ espansione **(26%)**<br>Il top management desidera migliorare le nostre difese **(25%)** | Requisiti normativi/di compliance **(25%)**<br>Il top management desidera migliorare le nostre difese **(24%)** |

***Figura 13:*** *Rilevamento della percentuale del budget IT speso per la sicurezza in Medio Oriente, Turchia e Africa*

È anche evidente il ruolo crescente della sicurezza IT nelle attività del top management. Le pressioni da parte dei vertici rappresentano la seconda principale motivazione per le imprese nell'area geografica META (29%) e la terza o la quarta principale decisione in altre cinque aree geografiche: Asia Pacifica con la Cina (35%), Nord America (30%), Russia (29%), America Latina (25%) ed Europa (24%).

I risultati indicano anche che i cambiamenti normativi stanno avendo un impatto finanziario per le imprese in determinate aree geografiche. Un quarto (25%) delle imprese europee ha identificato i requisiti normativi/di compliance come un fattore chiave degli investimenti per la cybersecurity, il che non sorprende data l'attenzione per il GDPR, in vigore da maggio 2018.

Le organizzazioni in Europa probabilmente adottano una prospettiva a lungo termine per il raggiungimento della compliance. Con le sanzioni previste da GDPR, che possono raggiungere fino a **20 milioni di euro** o il 4% del fatturato annuale globale dell'azienda, investire nella sicurezza IT ora potrebbe realmente far risparmiare alle imprese un'enorme quantità di denaro nel lungo periodo.

Lo stesso vale per le imprese in Giappone, il cui governo ha recentemente aggiornato la legge sulla tutela dei dati personali (una delle normative in materia di tutela dei dati più datate in Asia) e ha stabilito un nuovo Garante per la protezione dei dati personali (PPC) per regolare la compliance aziendale.

# Conclusione

Il nostro studio ha dimostrato che la sicurezza IT sta acquisendo un ruolo sempre più strategico nel moderno panorama aziendale.

Una delle ragioni è che le spese derivanti da data breach e incidenti di sicurezza sono ancora in aumento: il livello più alto raggiunto è pari a **$ 1,23 milioni** per le aziende Enterprise e **$ 120.000** per le PMI. Solo questo dovrebbe essere sufficiente per mostrare a ogni azienda il valore finanziario di avere strumenti per la cybersecurity in loco.

Ma la nostra ricerca dimostra chiaramente che la minaccia dei costi non è il solo fattore che ha introdotto la sicurezza nell'ordine del giorno del top management. L'IT gioca un ruolo sempre più importante negli affari, con le aziende sempre più alla ricerca delle strategie di digital transformation per tenere il passo con la concorrenza e le aspettative dei consumatori. In questo ambiente, un bug di sistema o un incidente potrebbe avere un impatto rapido e diretto sul fatturato.

I responsabili aziendali comprendono sempre più che se la loro strategia di digital transformation viene messa a rischio, ad esempio il passaggio al cloud, la migrazione a una nuova piattaforma o lo sconvolgimento delle attuali pratiche di lavoro, anche la stessa azienda è in pericolo.

In definitiva, molte aziende si pongono una semplice domanda: un maggiore investimento strategico per la sicurezza IT consentirà di pagare i dividendi dell'azienda a lungo termine?

**A quanto pare la risposta è un deciso "sì".**