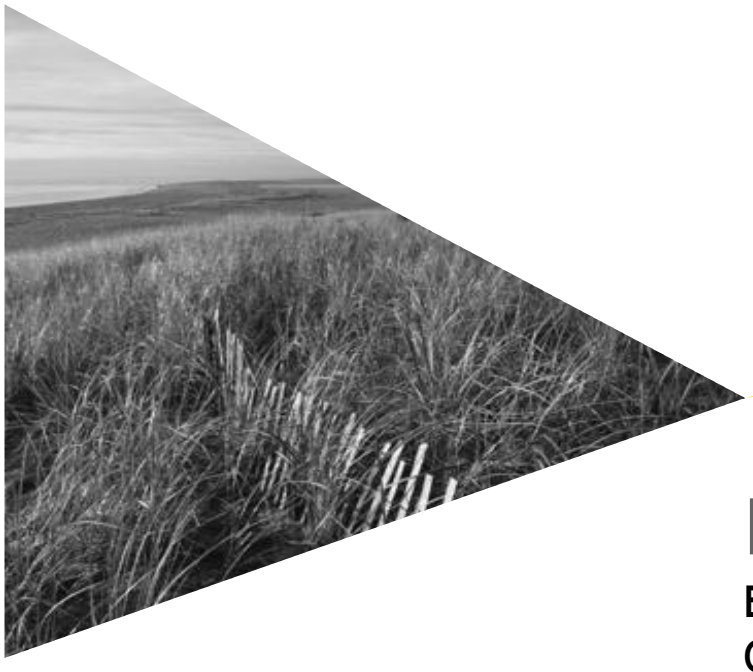


Borderless security

Ernst & Young's 2010 Global Information Security Survey

Presentazione dei risultati

24 Marzo 2011

Ernst & Young
Quality In Everything We Do

Ernst & Young's Global Information Security Survey

La Global Information Security Survey (GISS) di Ernst & Young, giunta alla sua tredicesima edizione, è una consolidata ricerca diventata nel corso degli anni punto di riferimento per la comprensione dei principali driver, trend e sfide inerenti la sicurezza informatica ed offre ai partecipanti l'opportunità di confrontare la propria situazione aziendale in materia di sicurezza con quella di aziende similari .

La survey 2010 è stata condotta tra giugno e luglio ed ha visto la partecipazione di circa 1600 aziende (80 a livello italiano) in 56 Paesi del mondo, rappresentative di tutti i principali settori industriali.

Agenda

Introduzione

Borderless security

Mobile computing

Cloud computing

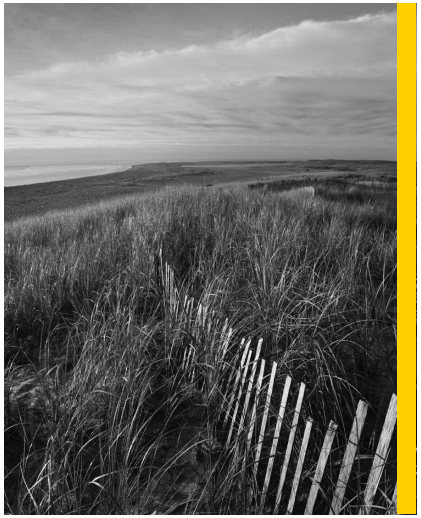
Social media

Principali risultati

Il nostro punto di vista

Appendice: profilo dei partecipanti

Introduzione



Nel corso degli ultimi anni si è assistito ad un aumento significativo nell'uso da parte delle aziende di fornitori di servizio esterni e nell'adozione da parte del business di nuove tecnologie come il cloud computing, il social networking ed il Web 2.0.

Si sono anche potuti riscontrare i progressi tecnologici che hanno fornito ad una forza lavoro mobile sempre più in aumento modalità apparentemente infinite di connettersi ed interagire con i colleghi e le terze parti. Nel complesso, questi cambiamenti stanno estendendo l'impresa, rendendo sfocati i confini tra casa ed ufficio, collega e concorrente e rimuovendo i confini tradizionali dell'azienda.

È questo ambiente di business in continuo cambiamento che viene esaminato dalla nostra global information security survey del 2010, ed in particolare come le organizzazioni stanno modificando i programmi di information security per adattarli alle nuove esigenze del business.

Risultati della survey

Borderless security

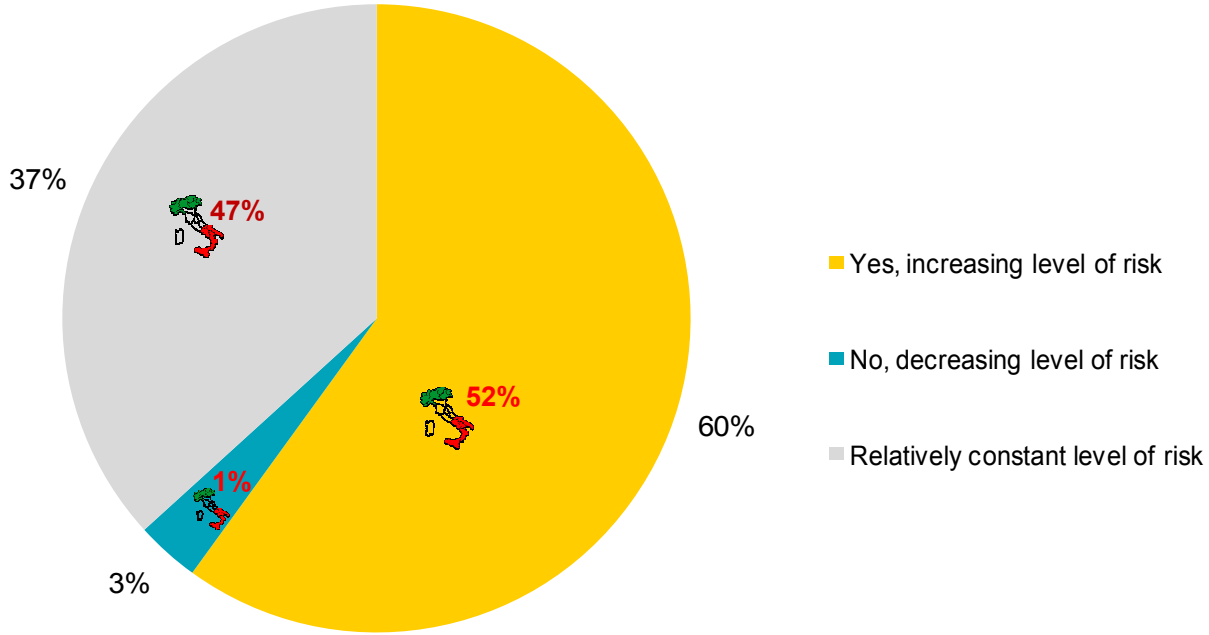
Borderless security

L'adozione delle nuove tecnologie comporta anche nuovi rischi che devono essere presi in esame

Le nuove tecnologie rappresentano una opportunità per l'IT di soddisfare le esigenze del business, ma sono anche fonte di **nuovi rischi**.

A **livello globale, con** il 60%, ed in **Italia,** con il 52% degli intervistati, viene percepito un significativo aumento del livello di rischio derivante dall'uso degli strumenti di **social networking, cloud computing e di device mobili** personali all'interno dell'azienda.

Given current trends towards the use of such things as social networking, cloud computing and personal devices in the enterprise, have you seen or perceived a change in the risk environment facing your organization?



Shown: percentage of participants

Borderless security

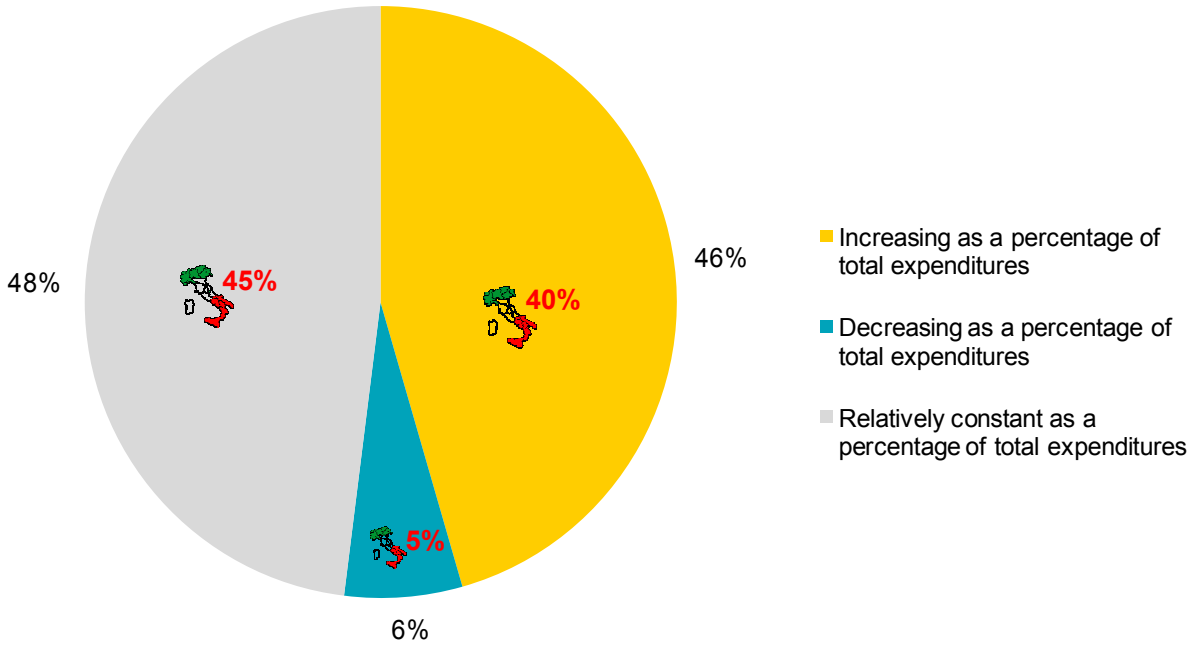
Le aziende non riducono le proprie spese in information security

Nonostante la continua pressione alla riduzione dei costi, le aziende stanno **investendo molto** per **indirizzare i rischi** legati alla sicurezza, inclusi quelli derivanti dalle **nuove tecnologie**.

A **livello globale e italiano** oltre il 40% dei partecipanti ha indicato che intende **incrementare** i propri investimenti in sicurezza informatica, mentre meno del 6% prevede di diminuirli.

In particolare tale tendenza si riscontra nel settore Telco, dove la percentuale dei partecipanti che prevede investimenti crescenti **sale al 57%**

Which of the following statements best describes your organization's annual investment in information security?



Shown: percentage of participants

Borderless security

La nostra prospettiva

- Stabilire un programma completo di gestione del rischio IT che identifichi ed affronti i rischi associati alle nuove tecnologie e a quelle emergenti.
- Intraprendere un esercizio di risk assessment per identificare le potenziali esposizioni alle nuove minacce e declinare risposte appropriate basate sul rischio.
- Avere una vista "informazione-centrica" della sicurezza, che sia ancor più allineata con i flussi di business ed informativi dell'organizzazione

La Nostra Prospettiva

Risultati della survey

Mobile computing

Mobile computing

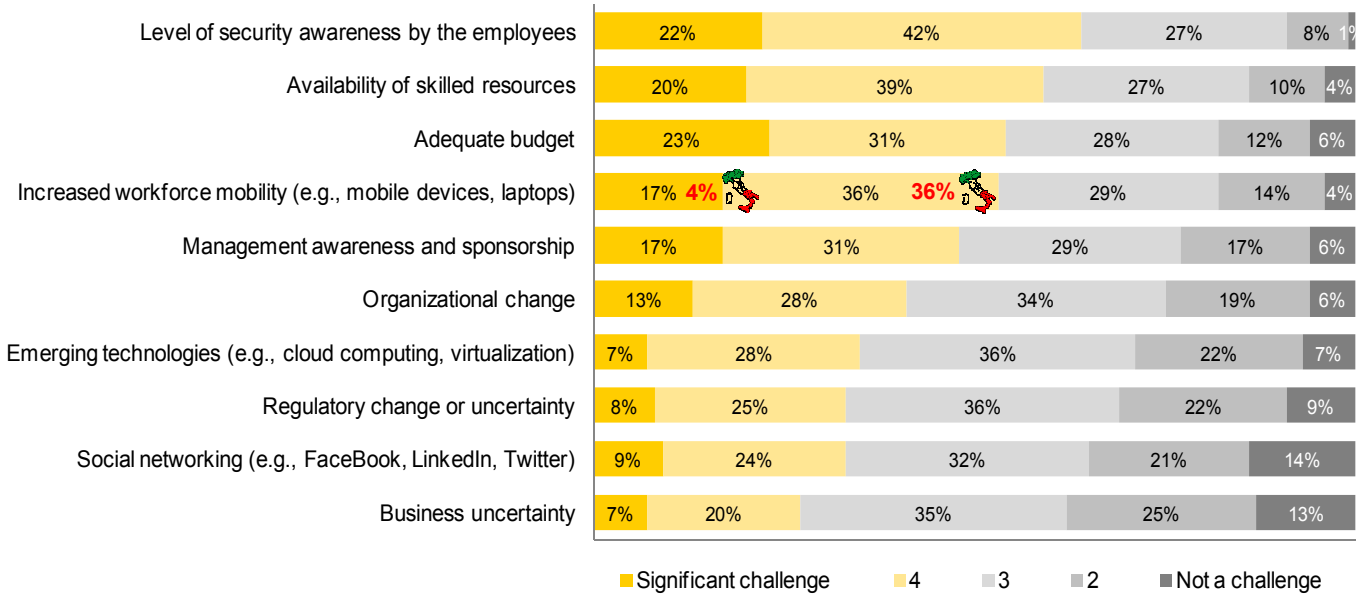
La domanda di mobilità della forza lavoro richiede di modificare le modalità di protezione delle informazioni aziendali

I device di **mobile computing** (laptop, tablet, smartphone, ecc.) sono sempre più diffusi all'interno delle aziende, consentendo alle persone di accedere e distribuire le informazioni in qualunque momento e ovunque si trovino.

A livello **globale** il 53% dei partecipanti (il 40% in **Italia**), ritiene che l'**aumento dei dispositivi mobili** sia una delle principali sfide per la gestione efficace della sicurezza, insieme alla disponibilità di budget e di risorse adeguate.

Per il settore **Industrial Products**, questa percentuale sale al 60%, mentre per gli altri settori analizzati i risultati sono allineati con quelli globali.

What is the level of challenge related to effectively delivering your organization's information security initiatives for each of the following?



Shown: percentage of participants

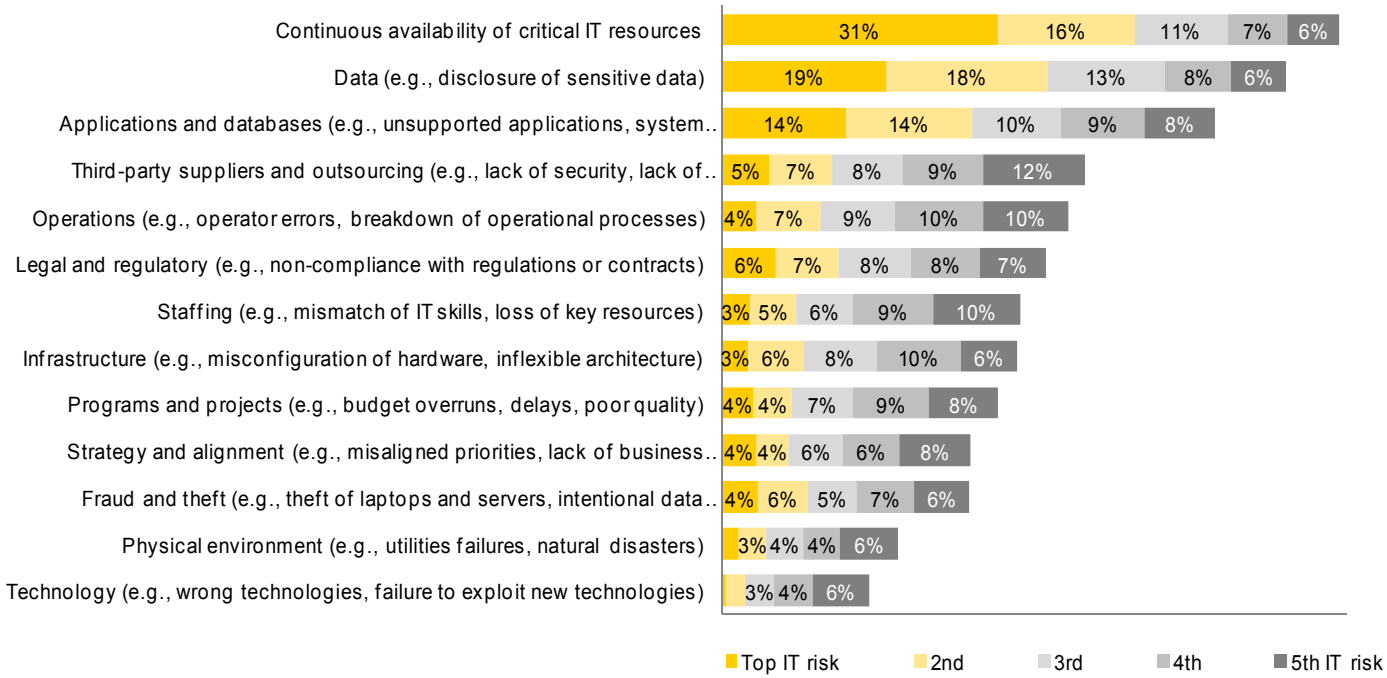
Mobile computing

Il principale rischio associato al mobile computing è la potenziale perdita di confidenzialità delle informazioni aziendali

L'aumento di utilizzo dei device di mobile computing rende gli stessi dispositivi sempre più esposti a **nuove minacce** (malware) ed al rischio di **smarrimenti e furti**.

Sia a livello **globale** che **italiano**, le maggiori aree di rischio sono rappresentate dalla potenziale perdita di riservatezza delle informazioni di business e dalla **continuità operativa** (mediante la costante disponibilità delle risorse IT critiche).

From the following list, which are the top five areas of IT risk for your organization?



Shown: percentage of participants

Mobile computing

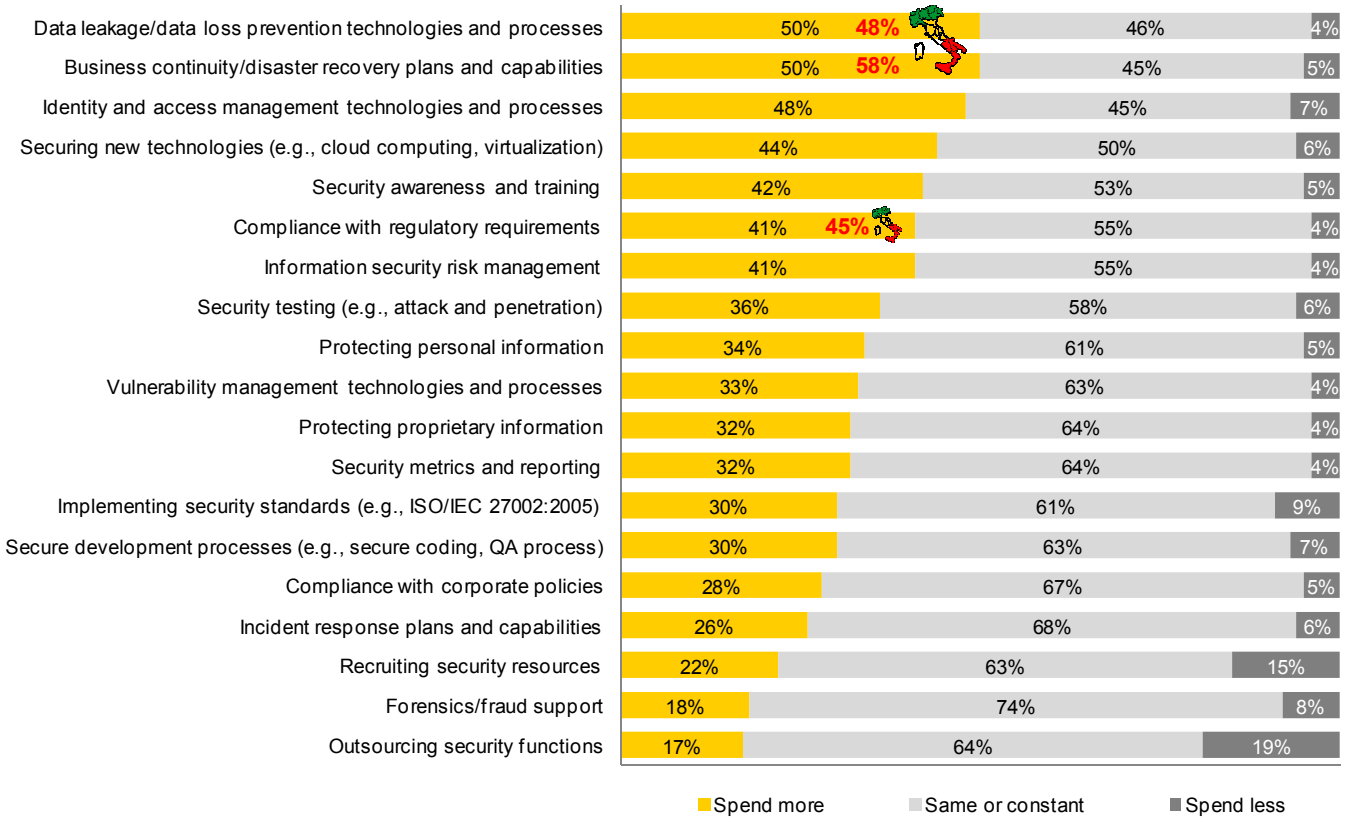
Le aziende riconoscono che il rischio legato al mobile computing è in forte aumento e iniziano a definire dei piani di azione per indirizzarlo

Le aziende stanno percependo sempre più il rischio legato alle nuove tecnologie ed hanno iniziato ad attivare progettualità al fine di ridurre il rischio derivante dalla **perdita di informazioni**.

A livello **globale** il 50% dei partecipanti ha pianificato nel prossimo anno di aumentare le spese relative a processi e tecnologie di **data leakage prevention**, così come di rafforzare i programmi di **business continuity e disaster recovery**.

Risultati simili si riportano per il panorama **italiano**, dove anche le spese di **compliance** alle normative risultano in crescita.

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the next year for the following activities?



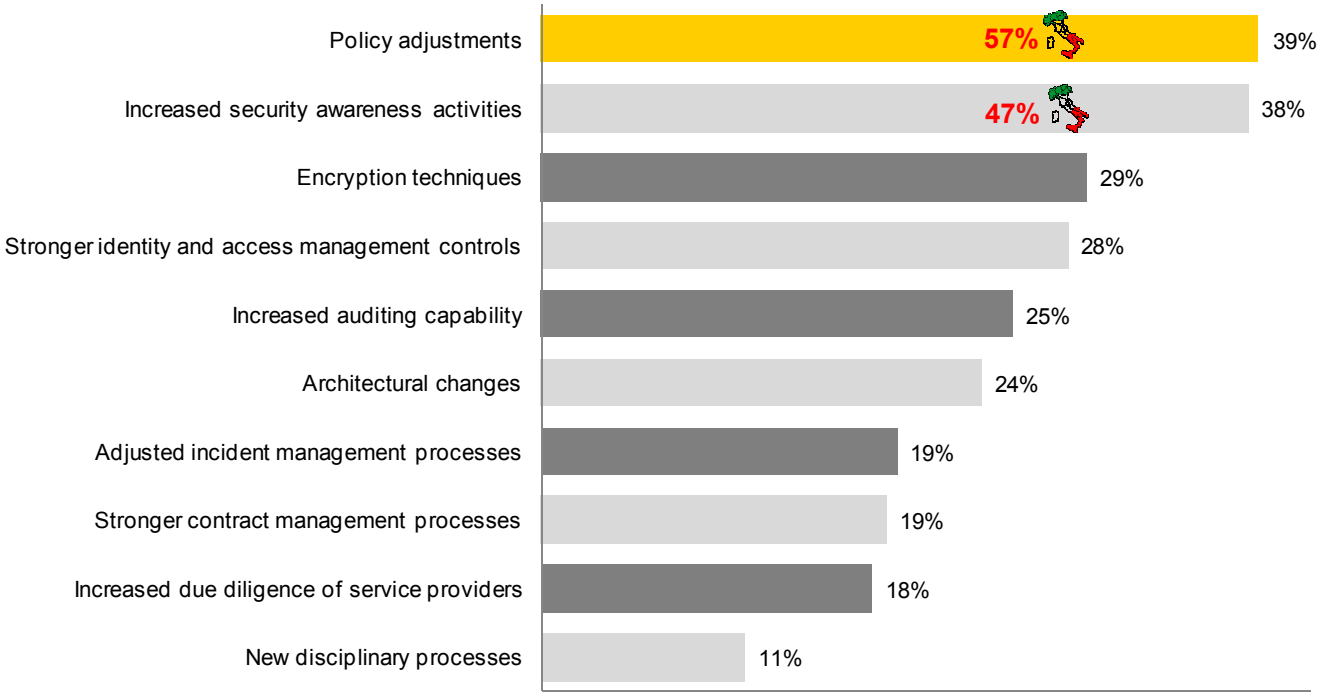
Shown: percentage of participants

Mobile computing

I principali controlli definiti dalle aziende per mitigare i nuovi rischi sono legati all'aggiornamento delle policy, alla sensibilizzazione del personale e all'utilizzo di soluzioni tecnologiche (es. crittografia)

Sia a livello **globale** che **italiano**, i partecipanti segnalano di aver implementato l'aggiornamento di **policy e procedure** per indirizzare correttamente i nuovi rischi, nonché di aver **sensibilizzato** maggiormente il personale sui nuovi rischi introdotti dalle nuove tecnologie.

Which of the following controls have you implemented to mitigate the new or increased risks?



Shown: percentage of participants

Mobile computing

La nostra prospettiva

- Aumentare gli investimenti in tecnologie di data leakage prevention, in crittografia, ed in soluzioni di Identity & Access Management, focalizzandosi sulle persone che utilizzano la tecnologia stessa.
- Ottenere una comprensione dei rischi creati dall'uso di nuove tecnologie, incluse le tecnologie adottate personalmente dai dipendenti che possano essere utilizzate a fini di business.
- Revisionare ed adattare le policy di Information Security in modo appropriato per stabilire l'utilizzo accettabile dei dispositivi mobili e qualsiasi restrizione specifica ad essi associata.
- Aumentare le attività di sensibilizzazione in tema di security per la forza lavoro mobile.
- Trasferire la sicurezza aziendale verso i dispositivi finali al fine di proteggere le informazioni critiche di business e fornire un miglior allineamento con il profilo di rischio dell'organizzazione.

Risultati della survey

Cloud computing

Cloud computing

I servizi di cloud computing si stanno espandendo rapidamente

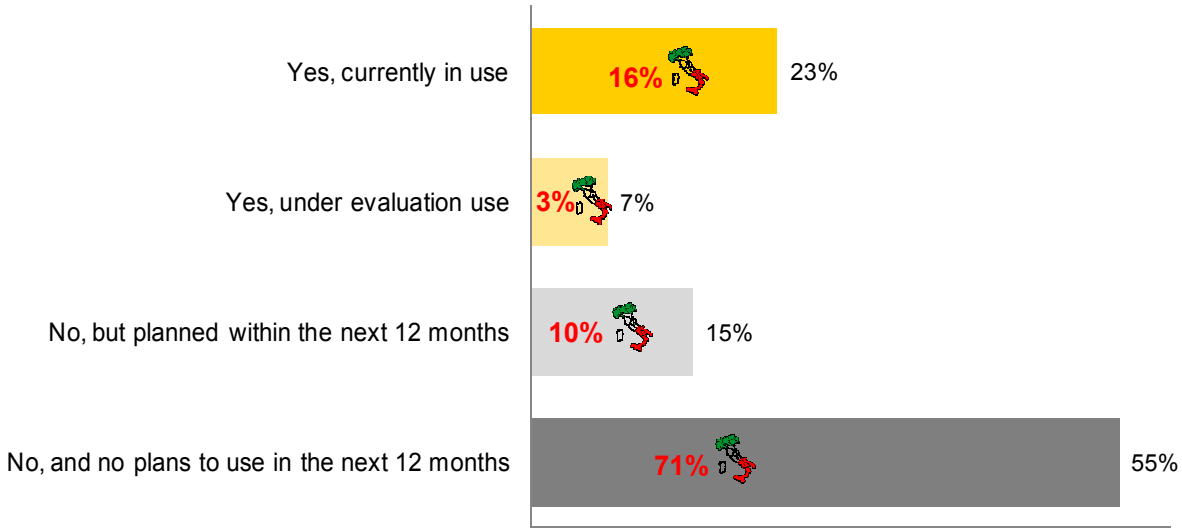
Spinte da una costante pressione a **ridurre i costi IT** ed aumentare la flessibilità e la velocità di implementazione, molte aziende si stanno orientando al'utilizzo di **servizi esternalizzati**.

Complessivamente il 45% dei partecipanti sta già utilizzando o ha già pianificato entro un anno l'adozione di soluzioni di **cloud computing**.

Per l'**Italia** invece, ben il 71% dei partecipanti si dichiara **non intenzionato ad utilizzare soluzioni di cloud computing** entro un anno.

Tra i vari settori industriali, più del 70% delle società appartenenti al **Banking** non prevede l'adozione di soluzioni cloud.

Does your organization currently use cloud computing-based delivery solutions?



Shown: percentage of participants

Cloud computing

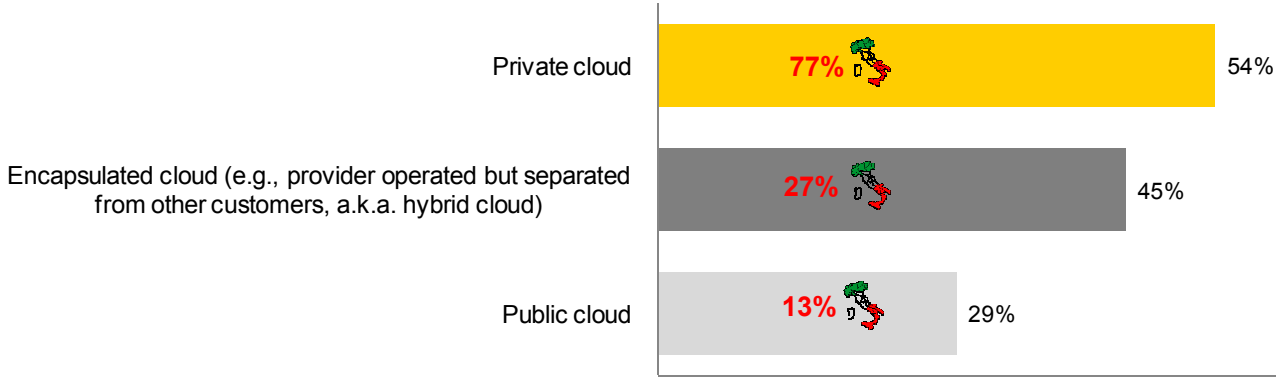
Le aziende stannno adottando tecnologie di cloud computing di tipo privato dando meno fiducia a quelle di tipo pubblico

I principali servizi di cloud computing utilizzati sono riconducibili all'utilizzo di applicazioni su infrastrutture accessibili da diverse tipologie di client (**Software as a Service**).

A livello **globale**, con il 54%, ed in **Italia,** con il 77% dei partecipanti, è emerso che chi utilizza servizi di cloud computing predilige servizi dedicati all'azienda (**private cloud**) in quanto offrono maggiori garanzie di sicurezza, affidabilità e governance.

Il settore **Industrial Products** esprime invece la preferenza per i servizi **encapsulated cloud** (55%).

Which kind of cloud technology are you using or do you plan to use?



Note: multiple responses permitted

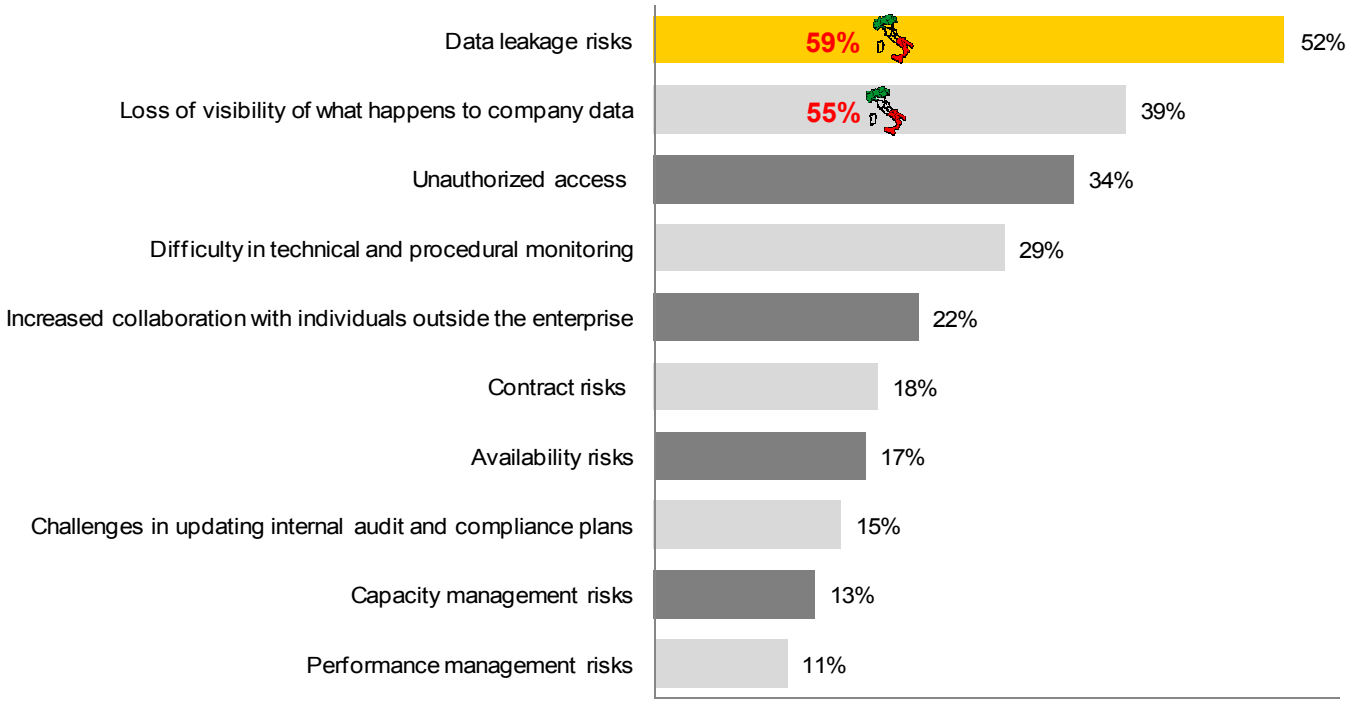
Shown: percentage of participants

Cloud computing

I rischi associati al cloud computing devono essere analizzati ed indirizzati prima che le applicazioni di business siano spostate in ambiente cloud

Sia a livello **globale** che **italiano**, i partecipanti dichiarano di aver identificato nella perdita delle informazioni (**data leakage**) e nella **perdita di visibilità** sui dati aziendali i principali rischi legati all'utilizzo dei servizi di cloud computing.

Which of the following "new" or increased risks have you identified?



Note: multiple responses permitted

Shown: percentage of participants

Cloud computing

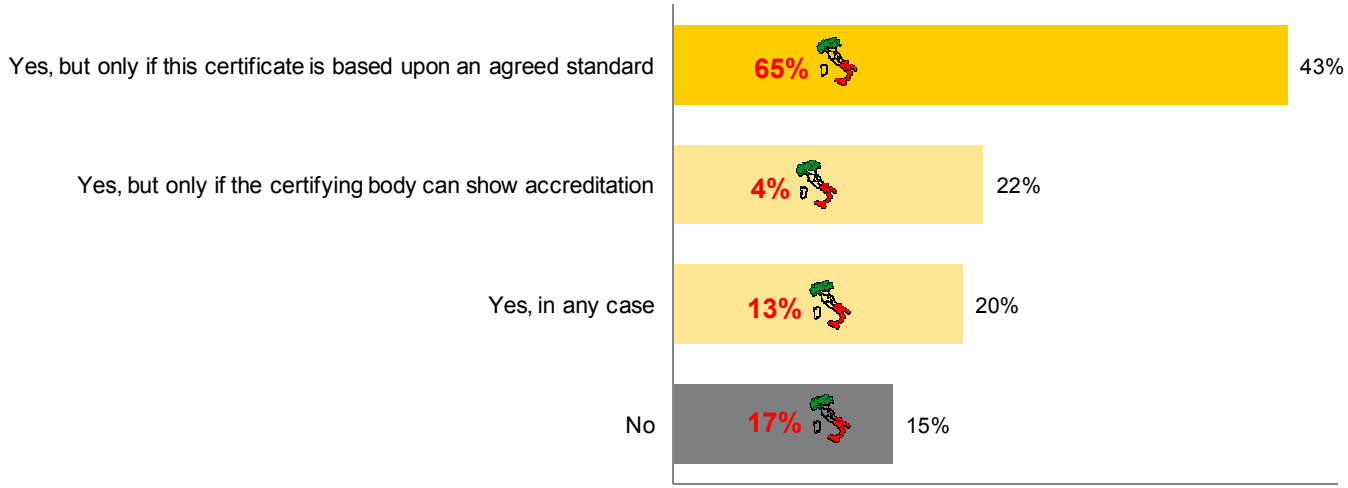
La certificazione dei servizi di cloud computing può aumentare il livello di fiducia verso i fornitori

Le aziende devono **definire standard e requisiti di sicurezza** per i servizi di cloud computing e verificare che i fornitori li rispettino.

Complessivamente, sia a livello **globale** che **italiano**, oltre l'80% dei partecipanti ritiene utile una **certificazione esterna** dei servizi di cloud computing.

Per il settore **Consumer Products**, tale percentuale sale oltre al 95%

Would some kind of external certification of cloud service providers increase your trust in cloud computing?



Shown: percentage of participants

Cloud computing

La nostra prospettiva

- Valutare i rischi legali, organizzativi e tecnologici così come gli aspetti di sicurezza causati dalla localizzazione delle informazioni in ambienti condivisi (public cloud computing).
- Sviluppare una strategia aziendale, un modello di governance ed un approccio operativo all'utilizzo del cloud computing, includendo la funzione Information Security nel supporto alla definizione di policy e linee guida.
- Stabilire degli standard e dei requisiti minimi al fine di permettere all'organizzazione di adottare il cloud computing nel modo più sicuro possibile.

Risultati della survey

Social media

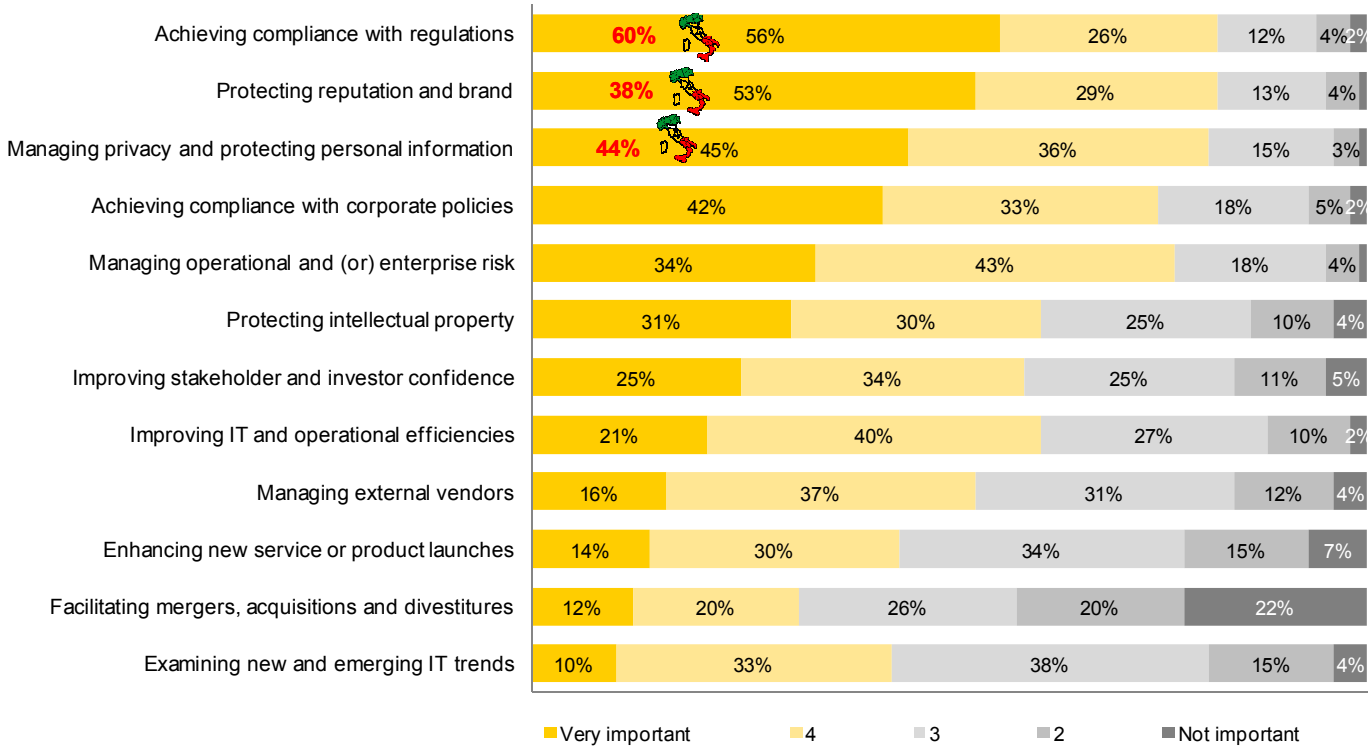
Social media

Ancora poche aziende hanno analizzato l'impatto dell'utilizzo dei social network

Molte società stanno sviluppando infrastrutture ed applicazioni che supportano l'utilizzo dei **social media** in azienda, ma ancora poche ne hanno analizzato l'**impatto in termini di sicurezza.**

Sia a livello globale che italiano, le attività più importanti legate all'information security sono relative alla **compliance** con le normative, alla **protezione del brand** aziendale ed alla gestione degli aspetti inerenti la **privacy.**

How important is information security in supporting the following activities in your organization?



Shown: percentage of participants

Social media

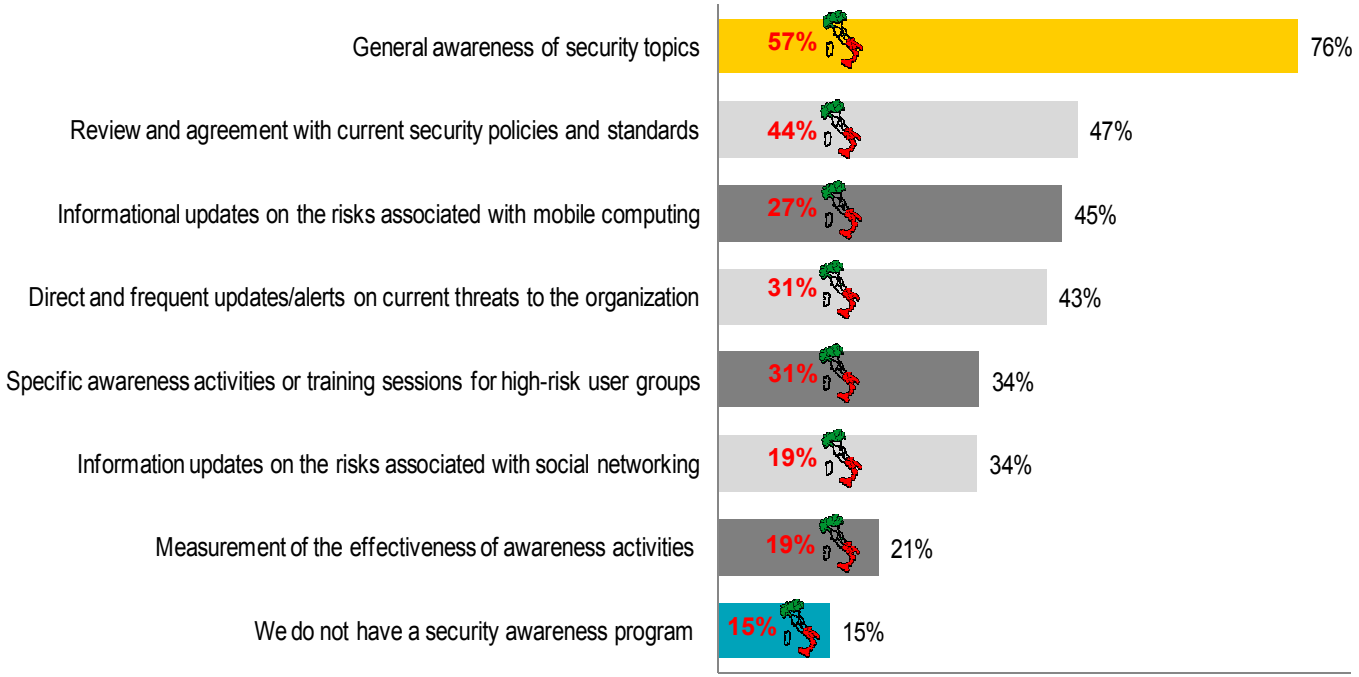
Le aziende devono aumentare il livello di sensibilizzazione del personale, in particolare relativamente all'utilizzo delle nuove tecnologie

Poche aziende non hanno ancora implementato attività di **formazione sulla sicurezza**, mentre la maggior parte dichiara di voler **aumentare** le **spese in formazione**.

Tuttavia solo il 34% dei partecipanti, a livello **globale,** include nei programmi di formazione anche gli aggiornamenti sui rischi associati all'utilizzo dei **social network**.

Questa percentuale scende al 19% per l'**Italia**, mentre sale al 40% nei settori **Industrial Products** e **Banking.**

What elements are currently covered in your organization's security awareness program?



Shown: percentage of participants

Social media

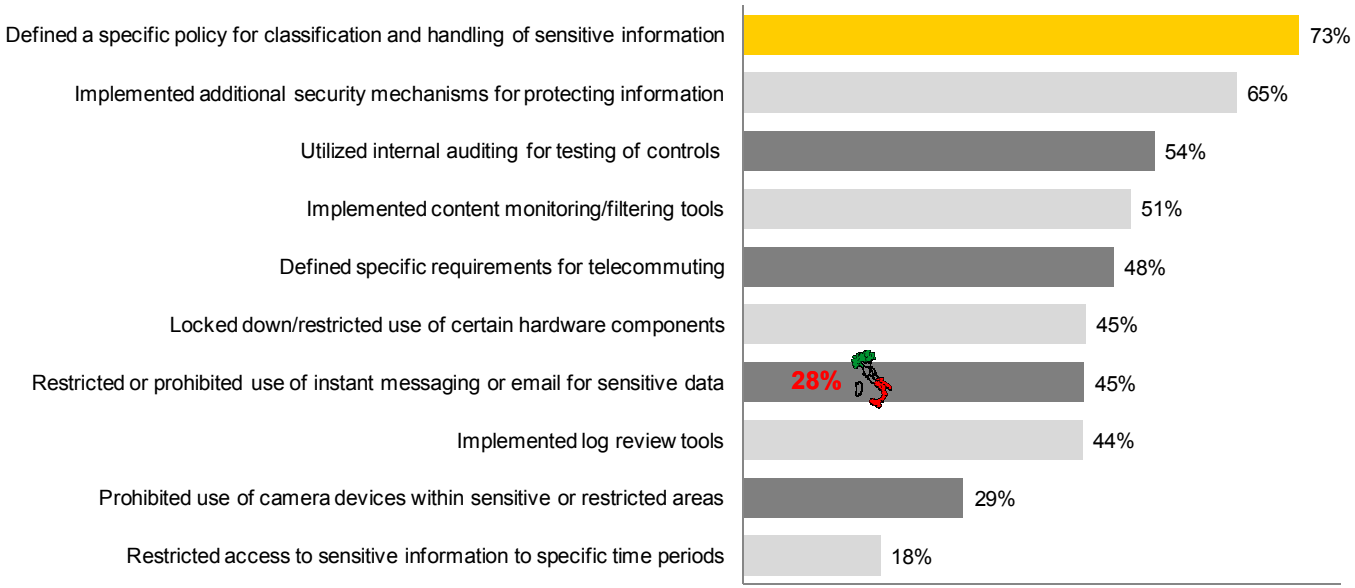
La restrizione dell'uso dei social network è una soluzione che ha un successo limitato ed anzi può causare ulteriori comportamenti indesiderati

Il 45% dei partecipanti ha indicato che ha **proibito o limitato** l'utilizzo dei sistemi di **posta elettronica e di instant messaging** per lo scambio di informazioni aziendali critiche.

In **Italia**, invece, solo il 28% degli intervistati dichiara di aver implementato misure atte a limitare o vietare l'utilizzo di posta elettronica e di instant messaging per lo scambio di informazioni aziendali critiche.

Infine per il settore **Banking** la percentuale sale al **63%.**

Which of the following actions has your organization taken to control data leakage of sensitive information?



Note: multiple responses permitted

Shown: percentage of participants

Social media

La nostra prospettiva

- Fornire l'accesso alle comunità on-line e gli strumenti di collaborazione sociale che la nuova forza lavoro si aspetta, ma secondo una visione che allinei i requisiti aziendali con la responsabilità personale al fine di proteggere informazioni sensibili per il business.
- Aumentare notevolmente la sensibilità dei dipendenti in tema di sicurezza e renderli maggiormente consapevoli delle proprie responsabilità.
- Informare tutti i membri dell'organizzazione in merito ai rischi e ai problemi legati ai social media.

La Nostra Prospettiva

Sommario

Principali risultati

Borderless security

- Il 60% degli interpellati ha percepito un incremento del livello di rischio da affrontare a causa dell'utilizzo del social networking, del cloud computing e dei dispositivi personali in azienda.
- Il 46% degli interpellati ha indicato che il proprio investimento annuale in ambito information security sta aumentando, mentre solo il 6% pensa di ridurre le spese.

Mobile computing

- Il 53% degli interpellati ha indicato che l'aumento della mobilità della forza lavoro è un fattore significativo per indirizzare le iniziative in ambito information security.
- Il 64% degli interpellati ha indicato che i dati (ovvero la divulgazione di dati sensibili) rappresentano una delle cinque maggiori aree di rischio IT.
- Il 50% degli interpellati prevede di spendere di più nel corso del prossimo anno in tecnologie e processi di prevenzione della perdita delle informazioni.
- Il 39% degli interpellati sta apportando adattamenti alle policy al fine di affrontare potenziali nuovi rischi.

Cloud computing

- Il 45% degli interpellati sta attualmente utilizzando, valutando o prevedendo di utilizzare i servizi di cloud computing entro i prossimi 12 mesi.
- Il 54% degli interpellati che utilizzano servizi di cloud computing ha indicato che sta utilizzando servizi di cloud computing in ambienti dedicati (private cloud computing).
- Il 39% degli interpellati ha citato la perdita di visibilità su quanto accade ai dati aziendali come un fattore di aumento di rischio nell'utilizzo di soluzioni basate sul cloud computing.
- L'85% degli interpellati ha indicato che la certificazione esterna potrebbe aumentare la loro fiducia nel cloud computing.

Social media

- Solamente il 10 % degli interpellati ha indicato l'esame dei nuovi ed emegenti trend nell'IT come un'importante attività da svolgere da parte della funzione Information Security.
- Il 34% degli interpellati aggiorna i propri programmi formativi sulla sicurezza con i rischi associati al social networking.
- Il 45% degli interpellati indica che viene ristretto o proibito l'utilizzo della messaggistica istantanea o dell'e-mail per le informazioni aziendali critiche.

Il nostro punto di vista

Borderless security

- Stabilire un programma dettagliato di gestione del rischio IT che identifichi ed affronti i rischi associati alle nuove tecnologie e a quelle emergenti.
- Intraprendere un esercizio di risk assessment per identificare potenziali esposizioni alle nuove minacce e declinare risposte appropriate basate sul rischio.
- Avere una vista "informazione-centrica" della sicurezza, che sia ancor più allineata con i flussi di business ed informativi dell'organizzazione

Mobile computing

- Aumentare gli investimenti in tecnologie di data leakage prevention, in crittografia, ed in soluzioni di Identity & Access Management, focalizzandosi sulle persone che utilizzano la tecnologia stessa.
- Ottenere una comprensione dei rischi creati dall'uso di nuove tecnologie, incluse le tecnologie adottate personalmente dai dipendenti che possano essere utilizzate a fini di business.
- Revisionare ed adattare le policy di Information Security in modo appropriato per stabilire l'utilizzo accettabile dei dispositivi mobili e qualsiasi restrizione specifica ad essi associata.
- Aumentare le attività di sensibilizzazione in tema di security per la forza lavoro mobile.
- Trasferire la sicurezza aziendale verso i dispositivi finali al fine di proteggere le informazioni critiche di business e fornire un miglior allineamento con il profilo di rischio dell'organizzazione.

Cloud computing

- Valutare i rischi legali, organizzativi e tecnologici così come gli aspetti di sicurezza causati dalla localizzazione delle informazioni in ambienti condivisi (public cloud computing).
- Sviluppare una strategia aziendale, un modello di governance ed un approccio operativo all'utilizzo del cloud computing, includendo la funzione Information Security nel supporto alla definizione di policy e linee guida.
- Stabilire degli standard e dei requisiti minimi al fine di permettere all'organizzazione di adottare il cloud computing nel modo più sicuro possibile.

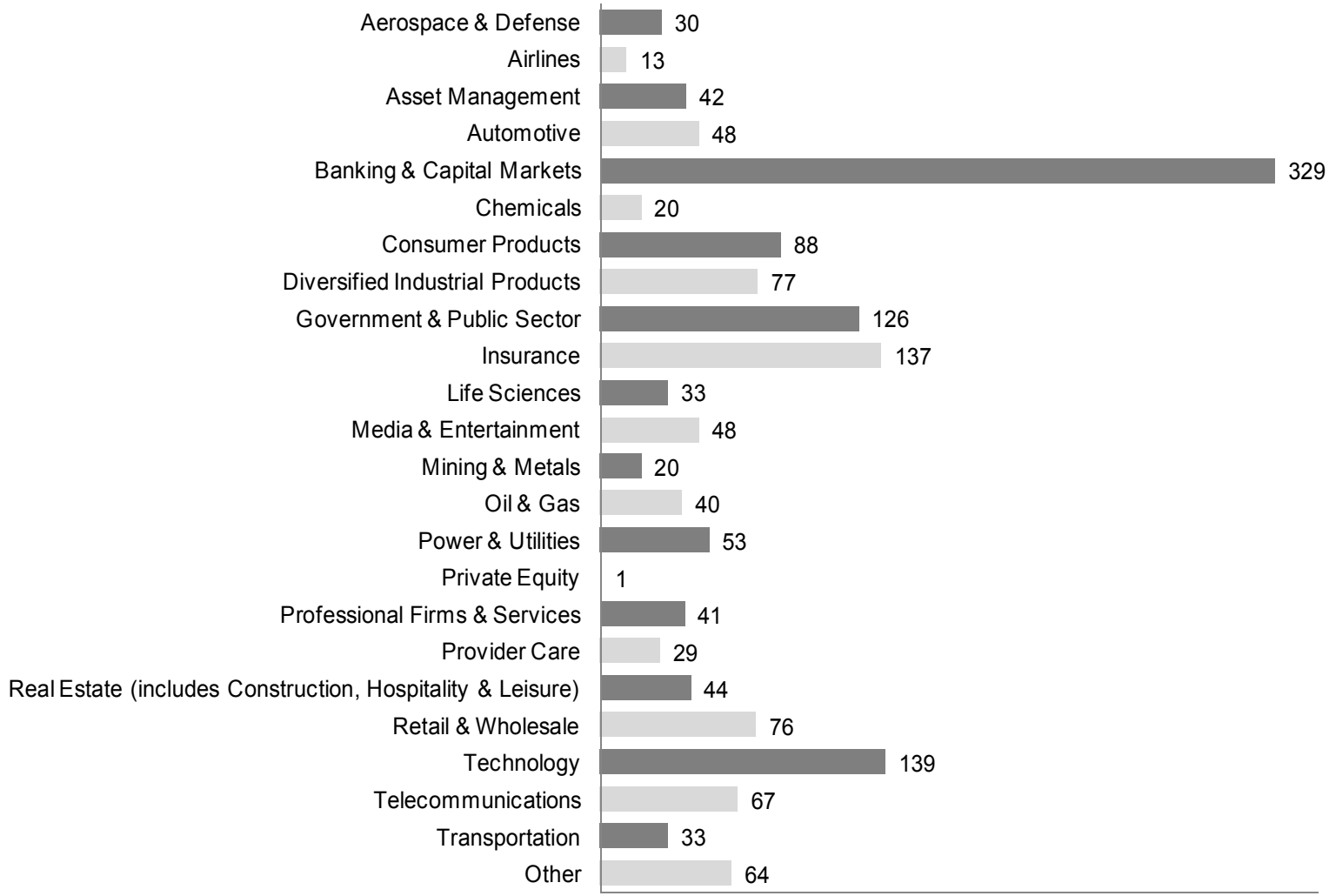
Social media

- Fornire l'accesso alle comunità on-line e gli strumenti di collaborazione sociale che la nuova forza lavoro si aspetta, ma secondo una visione che allinei i requisiti aziendali con la responsabilità personale al fine di proteggere informazioni sensibili per il business.
- Aumentare notevolmente la sensibilità dei dipendenti in tema di sicurezza e renderli maggiormente consapevoli delle proprie responsabilità.
- Informare tutti i membri dell'organizzazione in merito ai rischi e ai problemi legati ai social media.

Appendice

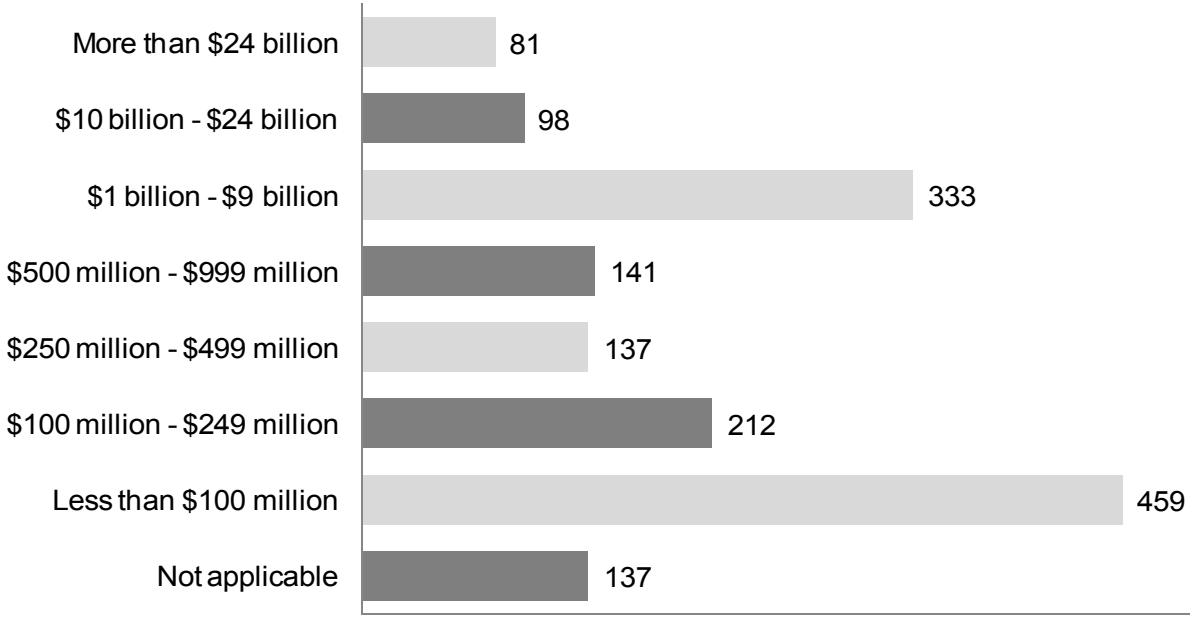
Profilo dei partecipanti

Partecipanti per settore industriale



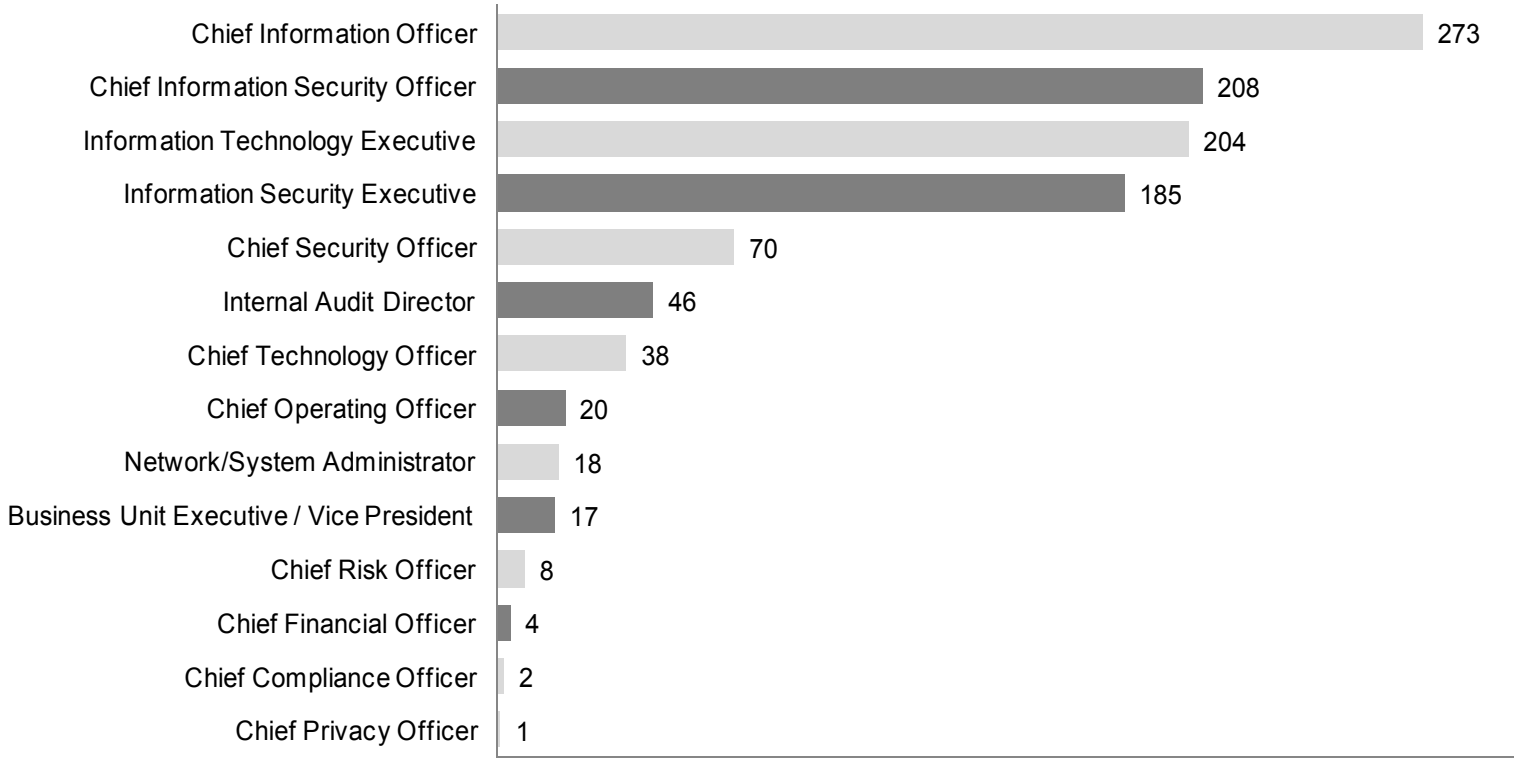
Shown: number of participants

Partecipanti per fatturato annuo



Shown: number of participants

Partecipanti per posizione organizzativa



Note: 504 participants with other titles

Shown: number of participants

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

The Ernst & Young organization is divided into five geographic areas and firms may be members of the following entities: Ernst & Young Americas LLC, Ernst & Young EMEIA Limited, Ernst & Young Far East Area Limited and Ernst & Young Oceania Limited.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 18,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization, you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.