SICUREZZA DELLE INFORMAZIONI E CONFORMITÀ LEGALE: LA RICERCA DI ELEMENTI COMUNI

Un whitepaper che illustra gli elementi comuni alle varie leggi e normative in materia di sicurezza delle informazioni: riservatezza, integrità e disponibilità dei dati.

Scritto da Michael R. Overly Esq., CISA, CISSP, CIPP, ISSMP, CRISC

Sommario

Introduzione

1.0

Nel migliore dei casi, conformarsi a tutti gli obblighi legali può rivelarsi per le aziende un lavoro a tempo pieno, mentre nella peggiore delle ipotesi può comportare multe, sanzioni e processi a loro carico.

Le aziende oggi devono gestire l'impresa quasi insormontabile di garantire la conformità a una complessa serie di leggi e normative in materia di sicurezza e privacy dei dati, vigenti a livello locale, statale, nazionale e persino internazionale. Il problema non interessa solo le aziende di grandi dimensioni. Di fatto, persino una piccola azienda con una presenza geografica circoscritta può essere soggetta alle leggi di altri stati ed, eventualmente, di altre nazioni in virtù della sua presenza su Internet.

In molti casi, si tratta di leggi e normative vaghe e ambigue e spesso le linee guida per il raggiungimento della conformità risultano carenti. A complicare ulteriormente la situazione, vi è il fatto che le leggi di giurisdizioni diverse possono risultare, e spesso lo sono realmente, in conflitto. Uno stato o paese può richiedere misure di sicurezza completamente diverse da quelle di un altro stato o paese. Nel migliore dei casi, conformarsi a tutti questi obblighi legali può rivelarsi per le aziende un lavoro a tempo pieno, mentre nella peggiore delle ipotesi può comportare multe, sanzioni e processi a loro carico.

Per rispondere alle crescenti minacce alla sicurezza dei dati, le autorità di regolamentazione in ogni singola giurisdizione hanno attuato, o si stanno impegnando per farlo, leggi e normative finalizzate all'imposizione di obblighi relativi alla privacy e sicurezza dei dati per il settore aziendale. Persino nell'ambito di una singola giurisdizione, è possibile che una serie di diversi enti pubblici abbiano tutti l'autorità di intraprendere azioni contro un'azienda non operante in conformità alle norme vigenti. Pertanto, una singola violazione della sicurezza può far sì che un'azienda debba affrontare numerose azioni intentate da numerose autorità di regolamentazione, senza considerare le possibili richieste di risarcimento danni da parte di clienti, partner aziendali, azionisti e altri soggetti. Negli Stati Uniti, ad esempio, viene adottato un approccio settoriale alla protezione della privacy e della sicurezza dei dati personali (ad esempio, esistono leggi federali distinte per i dati personali per il settore medico e quello finanziario, il rischio di credito e studenti e bambini). Altri approcci, come ad esempio quelli adottati nell'Unione Europea, forniscono uno standard unificato, pur garantendo al contempo una protezione avanzata per specifici tipi di informazioni altamente sensibili (informazioni sanitarie, dati relativi all'iscrizione alle organizzazioni sindacali e così via). L'effettiva implementazione in leggi degli standard dipende dal paese membro. Il Canada utilizza un approccio simile nel Personal Information Protection and Electronic Documents Act (PIPEDA). La responsabilità per multe e danni potrebbe facilmente trasformarsi nell'obbligo di pagare milioni di dollari. Persino nel caso di responsabilità relativamente limitata, la reputazione dell'azienda potrebbe venire irreparabilmente compromessa a causa della pubblicità negativa, con conseguenze serie in termini di perdita di clientela e fiducia da parte dei partner aziendali.

Il 65% delle aziende su scala mondiale ritiene che le politiche BYOD costituiscano una minaccia per la propria sicurezza.[1]

Le leggi e normative hanno l'obiettivo di indurre le aziende a intraprendere azioni ragionevoli e appropriate e non a suggerire azioni inattuabili o irragionevoli.

Le minacce alla sicurezza dei dati hanno toccato un livello mai raggiunto prima. Quasi ogni settimana i giornali riportano la notizia di un'azienda rimasta vittima di una violazione della sicurezza dei propri dati. Se è vero che gli attacchi da parte degli hacker non accennano a diminuire, dagli studi condotti dall'FBI (American Federal Bureau of Investigation) emerge che l'incidenza dei fenomeni di appropriazione indebita e danneggiamento delle informazioni riservate da parte di "insider" ha raggiunto un livello senza precedenti. Oltre allo staff aziendale interno, gli insider includono anche i fornitori esterni e i partner aziendali. Per tale motivo, questo whitepaper si concentra sulle due tipologie di minacce più significative da parte di insider: situazioni in cui vengono affidati dati sensibili ai partner e fornitori di un'azienda e iniziative Bring Your Own Device (BYOD) che consentono l'accesso ai dati aziendali da dispositivi sui quali l'azienda ha un controllo decisamente limitato. Nel primo caso, gli insider che fanno insorgere il rischio che deve essere mitigato sono terze parti (ovvero, fornitori e partner aziendali) Nel secondo, gli insider che fanno insorgere il rischio sono dipendenti aziendali.

Anche se non esistono soluzioni semplici per il problema, questo whitepaper si propone diversi obiettivi:

- Far comprendere chiaramente che, in materia di informazioni personali, la privacy rappresenta solo uno dei molteplici aspetti della conformità. Le aziende hanno l'obbligo di proteggere anche molti altri tipi di dati (ad esempio, segreti commerciali, dati e informazioni relativi ai partner aziendali, informazioni finanziarie private e così via).
- Esaminare le diverse leggi e normative in materia di privacy e sicurezza dei dati al fine di individuare tre semplici elementi comuni a molte di loro:
  1. Requisito di riservatezza, integrità e disponibilità (CIA)
  2. Agire "in maniera ragionevole" oppure adottare misure "appropriate" o "necessarie"
  3. Adattare le misure di sicurezza in base alla sensibilità delle informazioni e alla portata della minaccia

  Avendo un quadro chiaro di questi importanti concetti generali, le aziende possono comprendere meglio gli obblighi di conformità che nel complesso sono tenute a rispettare. Tuttavia, vi è un punto fondamentale: le leggi in materia di privacy e sicurezza delle informazioni non richiedono l'impossibile. La perfetta sicurezza è lungi dall'essere un requisito, bensì rappresenta un obiettivo da raggiungere. In effetti, come verrà più volte sottolineato più avanti, le leggi e normative in questo campo hanno l'obiettivo di indurre le aziende a intraprendere azioni ragionevoli e appropriate e non a suggerire azioni inattuabili o irragionevoli. Se un'azienda raggiunge tale standard e ciononostante si verifica una violazione, in genere non sarà interessata da un problema di conformità.
- Evidenziare i potenziali rischi correlati al mancato raggiungimento della conformità (ad esempio, processi, multe, sanzioni e così via) e prendere in esame le convinzioni errate più diffuse relative alle leggi in materia di privacy e sicurezza delle informazioni.
- Fornire due esempi di situazioni reali relativi all'applicazione di questi principi, suggerendo le azioni necessarie per la mitigazione dei rischi e il rispetto degli obblighi di conformità:
  1. Nel primo esempio viene illustrato come integrare meglio il principio della sicurezza delle informazioni nelle relazioni con fornitori e partner aziendali.
  2. Nel secondo esempio viene descritto come tenere sotto controllo il rischio durante l'attuazione di un'iniziativa Bring Your Own Device (BYOD).

1 Kaspersky Lab - Rapporto sui rischi globali IT 2013

Quali tipi di dati è necessario proteggere?

2.0

Il 60% degli eventi di perdita dei dati ha un impatto negativo sulla capacità operativa delle aziende.[2]

Generalmente, pensando alle leggi e normative in materia di sicurezza delle informazioni, alla stragrande maggioranza delle persone vengono immediatamente in mente i dati identificabili e riconducibili alla persona o le informazioni personali. Anche se è vero che la maggior parte delle leggi e normative riguarda principalmente le informazioni personali, non si tratta dell'unico tipo di dati per il quale le aziende possono avere obblighi legali. Quasi ogni azienda dispone di una varietà molto ampia di informazioni altamente sensibili da proteggere. Tra gli esempi di tali informazioni figurano:

Informazioni riservate generali dell'azienda

Può trattarsi di informazioni finanziarie, piani di marketing, potenziali attività promozionali, informazioni per il contatto, informazioni sugli investitori, piani per nuovi prodotti, liste clienti e così via.

Proprietà intellettuale

La proprietà intellettuale spesso comprende una delle risorse principali (se non addirittura quella più importante in assoluto) delle aziende. Una violazione della sicurezza potrebbe compromettere definitivamente la capacità dell'azienda di esercitare i propri diritti di proprietà intellettuale. Ad esempio, i segreti commerciali sono definiti informazioni sensibili per un'azienda e il loro valore risiede nel fatto che di norma non accessibili al resto del settore. Pertanto, sono informazioni che ricevono una particolare attenzione da parte dell'azienda, che si impegna costantemente per garantirne la riservatezza (ad esempio, la formula della Coca-Cola®). Se un segreto commerciale viene reso noto al pubblico, perde lo stato e il valore di segreto commerciale. Quasi ogni azienda possiede segreti commerciali, tra cui liste clienti, codice sorgente del software, formule, metodi operativi e così via, dei quali deve garantire la completa sicurezza.

Informazioni sanitarie

Le informazioni sanitarie rappresentano informazioni di tipo altamente sensibile e oggetto di regolamentazione. Ad esempio, la normativa Health Insurance Portability and Accountability Act (HIPAA) in vigore negli Stati Uniti regolamenta la privacy e la sicurezza delle informazioni sanitarie personali. In alcune giurisdizioni, tali informazioni ricevono una protezione di gran lunga superiore rispetto a quella applicata per altri tipi di dati personali. La European Union Data Protection Directive è la direttiva dell'Unione Europea che prevede la massima protezione delle informazioni sanitarie, attraverso l'implementazione di leggi di livello locale in ciascuno dei paesi membri. Altre leggi di questo tipo sono l'Australian Privacy Act 1988 e il recente Privacy Amendment (Enhancing Privacy Protection) Act. Un'azienda operante nel settore sanitario è sicuramente in possesso delle cartelle cliniche dei pazienti, ma anche aziende di altri settori potrebbero disporre di informazioni sanitarie dei propri dipendenti (ad esempio, informazioni relative alle richieste d'indennizzo assicurativo) che sono tenute a proteggere.

Informazioni finanziarie personali

Analogamente alle informazioni sanitarie, anche le informazioni finanziarie personali sono altamente sensibili e oggetto di intensa regolamentazione. Negli Stati Uniti, è in vigore il Gramm-Leach-Bliley Act (GLBA) in materia di privacy e sicurezza delle informazioni finanziarie personali. In altri paesi, le informazioni personali vengono definite in maniera dettagliata in leggi di ampio respiro che abbracciano pressoché tutti i possibili tipi di dati personali, tra cui ovviamente figurano anche le informazioni finanziarie. Un esempio di legge di questo tipo è il Personal Information Protection Act giapponese. Come nel caso delle informazioni sanitarie, anche in questo caso non è necessario che un'azienda appartenga al settore dei servizi finanziari per essere in possesso di questo tipo di informazioni. Tutti i datori di lavoro dispongono di informazioni finanziarie relative ai loro dipendenti (ad esempio, informazioni sulle retribuzioni, numeri di previdenza sociale e altri codici di identificazione personale, numeri di conti correnti bancari e così via).

Informazioni di sicurezza

Persino le informazioni di sicurezza sono di natura sensibile e devono essere protette. I criteri di sicurezza, i rapporti sui controlli della sicurezza, i piani di disaster recovery e business continuity e altre informazioni simili sono dati altamente sensibili che, qualora vengano compromessi, potrebbero essere utilizzati per lo sfruttamento delle vulnerabilità dell'azienda.

2 Kaspersky Lab - Rapporto sui rischi globali IT 2013

Perché la protezione è importante

3.0

L'impatto finanziario tipico di una violazione della sicurezza dei dati è di circa 50.000 dollari per le PMI e 649.000 dollari per le aziende di grandi dimensioni.[3]

La conformità legale è sicuramente il principale motivo per il quale le aziende scelgono di adottare misure di sicurezza delle informazioni tese alla protezione dei dati sensibili. Tuttavia, esiste una serie di altri importantissimi motivi per i quali le aziende devono mitigare tale rischio.

Protezione delle informazioni aziendali

Come menzionato nella sezione precedente, oltre ai dati identificabili e riconducibili alla persona, ogni azienda dispone anche di altri tipi di informazioni proprietarie da proteggere (ad esempio, proprietà intellettuale, piani di marketing, piani per nuovi prodotti, informazioni relative agli investitori, informazioni finanziarie e così via). Tali informazioni rappresentano risorse aziendali preziose che richiedono un impegno in termini di protezione.

Pratiche di due diligence

Numerose leggi e normative includono il concetto per il quale le aziende sono tenute ad attuare pratiche di dovuta diligenza nella protezione dei dati sensibili. Lo stesso concetto è rinvenibile a un livello più generale nell'obbligo da parte dei dirigenti aziendali di esercitare dovuta cura e ragionevole giudizio nella loro attività di gestione, che implica l'attuazione di pratiche di dovuta diligenza nella protezione dei dati aziendali. Le leggi in vigore e questo standard di governance aziendale più generale non richiedono la perfezione. Di fatto, l'azienda e i suoi dirigenti devono dimostrare di avere agito in maniera ragionevole e appropriata, attuando pratiche di dovuta diligenza nella protezione delle informazioni aziendali. Attraverso l'implementazione e la documentazione di un approccio ponderato alla mitigazione dei rischi per la sicurezza, le aziende e i dirigenti aziendali potranno dare dimostrazione del proprio modo efficiente di operare in caso di violazione.

Protezione della reputazione aziendale

Essere oggetto di una violazione della sicurezza può compromettere in maniera significativa la reputazione di un'azienda. Una pubblicità negativa di questo tipo potrebbe mettere irrimediabilmente a repentaglio le sorti un'azienda. I clienti e i partner aziendali possono perdere fiducia nella capacità dell'azienda di proteggere i loro dati e sistemi.

Riduzione della responsabilità potenziale

In ultima analisi, il motivo più ovvio per l'implementazione di un approccio ponderato alla sicurezza delle informazioni è quello di ridurre al minimo la responsabilità potenziale. La responsabilità può assumere numerose forme: multe elevate da diverse autorità di regolamentazione, sanzioni statutarie, azioni legali da parte degli azionisti e cause civili intentate da partner e clienti (inclusa la possibilità di costose azioni di class action) contro l'azienda e i suoi dirigenti.

3 Kaspersky Lab – Rapporto sui rischi globali IT 2013

Convinzioni errate sulla conformità per la sicurezza delle informazioni

4.0

“

Le leggi e normative in questo campo non richiedono la perfezione, bensì hanno l'obiettivo di indurre le aziende a intraprendere azioni ragionevoli e appropriate.

La conformità per la sicurezza delle informazioni è un argomento caratterizzato da scarsa chiarezza e numerose convinzioni errate. Le due convinzioni errate più diffuse sono che si tratti "*solo* una questione di dati" e "*solo* di una questione di riservatezza". Se i dati e la riservatezza sono di importanza cruciale, l'adozione di un approccio più olistico diventa in questo caso un fattore indispensabile. Un'azienda deve concentrarsi sui suoi dati, ma deve mostrare un'uguale attenzione verso i sistemi sui quali sono archiviati. Inoltre, la riservatezza è solo una delle tre forme di protezione fondamentali richieste per una sicurezza davvero efficace.

Chiunque sia coinvolto in iniziative tese a garantire la sicurezza delle informazioni deve avere familiarità con l'acronimo "CIA" (Confidentiality, Integrity and Avalaibility, ovvero riservatezza, integrità e disponibilità), dal momento che la sicurezza delle informazioni viene garantita solo se si è in grado di soddisfare tutti e tre questi elementi. Per "riservatezza" si intende la protezione dei dati contro il rischio di accesso e divulgazione non autorizzati. Per "integrità" si intende la certezza della precisione dei dati e del fatto che non siano stati alterati da terzi non autorizzati. Infine, per "disponibilità" si intende che i dati sono disponibili per l'accesso e l'uso in base alle esigenze. È alquanto inutile disporre di dati riservati e integri, ma che non risultino accessibili quando un utente ne ha bisogno. Per soddisfare questo requisito, i sistemi sui quali sono archiviati i dati devono essere caratterizzati da specifici livelli di servizio per disponibilità, tempi di risposta e così via. Ciò si dimostra estremamente importante nel caso in cui i dati vengano mantenuti da un fornitore terzo per conto dell'azienda.

L'importanza del requisito CIA non sarà mai evidenziata abbastanza. Non si tratta semplicemente di un concetto che trova spazio nei saggi e nelle discussioni sul tema della sicurezza delle informazioni. Di fatto, i legislatori hanno integrato direttamente il concetto in specifiche leggi e normative in materia di sicurezza delle informazioni e le aziende che non riescono a soddisfare il requisito CIA per i loro dati potrebbero essere riconosciute colpevoli di violazione di tali leggi.

Infine, un'altra convinzione errata relativa alle leggi in materia di privacy e sicurezza dei dati è che tali norme richiedano la perfezione (ovvero, qualsiasi violazione, indipendentemente dal livello di diligenza attuato dall'azienda, creerà una responsabilità a carico dell'azienda). Non è affatto così. Le leggi e normative in questo campo hanno l'obiettivo di indurre le aziende a intraprendere azioni ragionevoli e appropriate. Se l'azienda raggiunge tale standard e ciononostante si verifica una violazione, in genere non sarà interessata da un problema di conformità.

Trovare gli elementi comuni alle leggi e normative in materia di conformità

5.0

Il numero e la varietà di leggi e normative applicabili anche alle piccole aziende che gestiscono informazioni sensibili possono intimidire, se non addirittura sembrare opprimenti. In taluni casi, può rivelarsi quasi impossibile per un'organizzazione complessa e di grandi dimensioni individuare tutte le leggi applicabili, venire a capo delle eventuali incongruenze e quindi implementare un programma di conformità. L'obiettivo di questa sezione non è illustrare ogni singola legge e normativa, ma individuare gli elementi comuni a molte di loro. Attraverso la comprensione di tali elementi, le aziende sono in grado di giungere più facilmente a un quadro chiaro dei loro obblighi di conformità essenziali.

Oltre a leggi e normative, tali elementi comuni interessano anche standard contrattuali come lo standard PCI DSS (Payment Card Industry Data Security Standard) e standard di settore per la sicurezza delle informazioni pubblicate dalle organizzazioni come gli standard CERT della Carnegie Mellon University e ISO (International Standards Organization). L'inclusione di questi elementi comuni nella progettazione e nell'implementazione di un programma di sicurezza delle informazioni consentirà di migliorare in maniera sostanziale la capacità di un'azienda di raggiungere la conformità generale a leggi, normative e altri requisiti (ad esempio, PCI DSS, standard di settore e così via) applicabili alla stessa.

Riservatezza, integrità e disponibilità (CIA)

Come illustrato nella sezione 4, il concetto del requisito CIA da tempo noto e presente in qualsiasi manuale sulla sicurezza delle informazioni è stato codificato attraverso numerose leggi e normative. I tre aspetti del concetto riguardano gli obiettivi fondamentali della sicurezza delle informazioni: i dati/le informazioni devono essere mantenuti sicuri, protetti contro modifiche non autorizzate e disponibili per l'uso in base alle esigenze degli utenti. La mancata applicazione di uno dei suddetti tipi di protezione avrà un impatto concreto sulla conformità e sul valore delle informazioni aziendali.

Agire in "maniera ragionevole" oppure adottare le misure "appropriate" o "necessarie"

Il concetto dell'agire in "maniera ragionevole" è presente in un ampio numero di leggi statali di Stati Uniti, Australia molti altri paesi. Il concetto correlato dell'agire attraverso l'adozione delle misure "appropriate" o "necessarie" è diffuso nell'Unione Europea e in molte altre aree geografiche. Unitamente, i due concetti costituiscono il fulcro di quasi tutte le leggi in materia di sicurezza delle informazioni e privacy dei dati. Un'azienda è tenuta ad agire in maniera ragionevole oppure a intraprendere qualsiasi azione necessaria o appropriata per la protezione dei propri dati. Tuttavia, è opportuno ricordare che ciò non impone all'azienda l'obbligo della perfezione, bensì l'esigenza di valutare il potenziale rischio e di adottare tutte le misure ragionevoli o necessarie per mitigarlo. Tuttavia, qualora si verifichi una violazione e l'azienda abbia soddisfatto tale requisito di base, non verrà ritenuta colpevole di aver violato le corrispondenti leggi o normative vigenti.

Adattare le misure di sicurezza in base alla natura dei dati e della minaccia

Un concetto strettamente correlato a quello che prevede di agire in maniera ragionevole o di adottare misure appropriate, è l'idea di adattare le misure di sicurezza in base alla natura della minaccia e alla sensibilità dei dati. In tal modo, un'azienda non è costretta a spendere l'intero budget destinato alla sicurezza per gestire una minaccia a basso rischio. Tuttavia, se il rischio è considerevole, soprattutto a fronte del grande volume e/o della elevata sensibilità dei dati, l'azienda ha la necessità di farsi carico di un impegno e di investimenti superiori. Un database contenente solo nomi e indirizzi fisici potrebbe non richiedere lo stesso livello di sicurezza di un database che include nomi, indirizzi e numeri di previdenza sociale. Per comprendere chiaramente tale concetto, è possibile fare riferimento agli estratti di due leggi in cui viene spiegato cosa si intende per "adattamento":

Primo esempio

Un'azienda è tenuta a implementare *misure di protezione appropriate (a) alle dimensioni, alla portata e al tipo di azienda della persona con l'obbligo di tutelare le informazioni personali ai sensi di un programma di sicurezza delle informazioni di così ampio respiro; (b) alla quantità di risorse disponibili per tale persona; (c) alla quantità dei dati archiviati; e (d) all'esigenza di garantire la sicurezza e la riservatezza delle informazioni relative a consumatori e clienti*

Secondo esempio

Le iniziative nel campo della sicurezza devono considerare:
(i) Le dimensioni, la complessità e le capacità dell'azienda.
(ii) Le capacità dell'azienda di garantire la sicurezza di software, hardware e infrastruttura tecnica.
(ii) I costi legati alle misure di sicurezza.
(iv) La probabilità e il livello di criticità dei potenziali rischi per i dati.

Tali concetti verranno illustrati nelle due sezioni che seguono in due esempi estrapolati da situazioni reali e applicabili ad aziende di qualsiasi tipo e dimensioni. Nel primo esempio viene illustrato come integrare meglio il principio della sicurezza delle informazioni nelle relazioni con fornitori e partner aziendali. Ovvero, nel caso in cui un fornitore possa accedere o sia in possesso delle informazioni altamente sensibili di un'azienda, quali azioni l'azienda è tenuta a intraprendere per garantire la protezione delle informazioni. Nel secondo esempio viene descritto come tenere sotto controllo il rischio durante l'attuazione di un'iniziativa Bring Your Own Device (BYOD) progettata per i dipendenti di un'azienda.

Gestione della sicurezza delle informazioni nelle relazioni con fornitori e partner aziendali

6.0

Quasi ogni settimana viene riportata la notizia di un'azienda che, dopo avere affidato le proprie informazioni altamente sensibili a un fornitore o partner aziendale, realizza che sono state danneggiate per la mancata adozione di adeguate misure di protezione da parte del fornitore in questione. Inoltre, a peggiorare ulteriormente la situazione, in questi casi spesso si scopre che le aziende hanno attuato solo limitatamente pratiche di due diligence, o le hanno ignorate del tutto nelle loro relazioni con i fornitori, e non hanno incluso la questione della sicurezza delle informazioni nei contratti con essi stipulati, ritrovandosi pertanto impossibilitate ad avanzare rivendicazioni per l'eventuale danneggiamento delle informazioni da parte dei fornitori.

Nell'attuale scenario normativo, le aziende devono mostrare una cautela di gran lunga maggiore in quelle relazioni con i fornitori in cui vengono messe a rischio le informazioni sensibili. In questa sezione vengono descritti tre strumenti di cui le aziende possono avvalersi per ridurre significativamente i rischi legati alla sicurezza delle informazioni sollevati dai rispettivi fornitori e partner aziendali, seguire e documentare pratiche di dovuta diligenza e risolvere i problemi che insorgono in caso di danneggiamento delle informazioni.

Si tratta dei seguenti strumenti:

- **Questionario sulla dovuta diligenza dei fornitori**
- **Protezioni contrattuali fondamentali**
- Utilizzo, nei casi appropriati, di un **documento sui requisiti di sicurezza delle informazioni**.

Quando un fornitore o partner aziendale può accedere alla rete, alle risorse o ai dati di un'azienda, è necessario uno o più di questi strumenti.

In tal modo, le aziende possono soddisfare il requisito CIA per i loro dati, dimostrare di avere agito in maniera ragionevole/appropriata nella gestione del rischio e adattare il loro approccio in base al livello di rischio (ad esempio, richiedendo protezioni contrattuali e pratiche di due diligence più o meno efficaci a seconda che il fornitore sia rispettivamente in possesso di una grande o di una limitata quantità di dati sensibili).

> Tuttavia, nell'attuale scenario aziendale e normativo, questo approccio ad hoc alla due diligence non si rivela più né appropriato né ragionevole.

Due diligence: il primo strumento

Sebbene la maggior parte delle aziende tenda ad attuare pratiche di due diligence prima di affidare i propri dati sensibili ai fornitori o di consentire loro di accedere ai propri sistemi, spesso tali pratiche vengono implementate in maniera non sistematica, non uniforme e non chiaramente documentata. Sono rari i casi in cui il requisito di due diligence viene integrato nei contratti stipulati con i fornitori. Tuttavia, nell'attuale scenario aziendale e normativo, questo approccio ad hoc alla due diligence risulta non essere né appropriato né ragionevole.

Al fine di garantire la corretta documentazione e uniformità del processo di due diligence, le aziende devono ideare un "questionario sulla due diligence" che deve essere compilato da ogni potenziale fornitore o partner aziendale con accesso alle informazioni personali o ai dati aziendali riservati o sensibili. Il questionario prende in esame i seguenti temi: responsabilità sociale, copertura assicurativa, condizioni finanziarie, gestione del personale, criteri di sicurezza delle informazioni, sicurezza fisica, sicurezza logica, disaster recovery e business continuity e una serie di altri temi di particolare rilievo.

L'uso di un questionario standardizzato offre molteplici importanti vantaggi:

- Fornisce un quadro di riferimento uniforme e pronto all'uso per l'attuazione della due diligence
- Offre un confronto tra risposte comparabili dei fornitori
- Assicura che vengano presi in considerazione tutti gli aspetti chiave relativi alla due diligence
- Fornisce uno strumento di facile uso per integrare le informazioni relative alla due diligence direttamente nel contratto. Il questionario completato è un documento generalmente allegato al contratto finale.

I fornitori devono da subito essere messi a conoscenza del fatto che le informazioni da essi fornite nell'ambito del processo di due diligence e, in particolare, nelle risposte al questionario sulla due diligence dei fornitori verrano (i) considerate fondamentali per la scelta dei fornitori; e (ii) integrate nel contratto finale. Per essere più efficace, il questionario deve essere presentato ai potenziali fornitori fin dalla fase iniziale della relazione. Deve essere incluso in tutti i documenti di richiesta di offerta (RFP) o, in assenza di questi ultimi, come documento indipendente durante le discussioni preliminari con il fornitore.

Tra i temi principali per il questionario sulla dovuta diligenza dei fornitori figurano i seguenti:

- **Condizioni finanziarie del fornitore.** Il fornitore è un'azienda privata o pubblica? Sono disponibili copie degli ultimi rendiconti finanziari? Sebbene le condizioni finanziarie non rappresentino un fattore cruciale per la sicurezza delle informazioni, l'eventualità che un fornitore dichiari bancarotta o semplicemente cessi di operare mentre è in possesso delle informazioni altamente sensibili di un'azienda può fare insorgere un rischio considerevole. In casi di questo tipo, potrebbe essere difficile, se non addirittura impossibile, recuperare i dati e garantire che vengano definitivamente rimossi dai sistemi del fornitore. Analogamente, la possibilità di intentare causa per danni contro un fornitore insolvente risulterà vanificata qualora il fornitore non abbia le disponibilità finanziarie per il risarcimento dei danni.
- **Copertura assicurativa.** Quali tipi di copertura usa il fornitore? Quali sono i limiti e gli altri termini della copertura? Si tratta di un modello di copertura basato sulla ricezione delle richieste di risarcimento oppure sull'insorgenza del danno? Dal momento che le polizze di responsabilità generale disponibili sul mercato di solito non coprono le violazioni della sicurezza delle informazioni, è consigliabile richiedere al fornitore un'assicurazione contro la pirateria informatica o per la rete di sicurezza, che sono tipi di polizze sempre più diffusi.
- **Responsabilità aziendale.** Ci sono state di recente condanne penali, controversie materiali o casi in cui il fornitore abbia subito un considerevole danneggiamento della sicurezza o violazioni della privacy oppure sia stato sottoposto a controlli con risultati negativi e così via?
- **Subappalto.** Il fornitore avrà l'esigenza di ricorrere a subappaltatori o aziende affiliate per la fornitura dei suoi servizi? Farà ricorso a subappaltatori o aziende affiliate di altri paesi? In quali paesi si trovano i subappaltatori o le aziende affiliate? Quali tipi di servizi forniranno? Quali eventuali informazioni l'azienda invierà a tali entità?
- **Procedure di sicurezza aziendale.** Il fornitore si avvale di un programma di sicurezza delle informazioni completo e accuratamente documentato? Quali criteri per la gestione delle informazioni utilizza?? Il fornitore si avvale di un team di sicurezza delle informazioni dedicate? Si avvale di un team di risposta agli incidenti? Quali pratiche in materia di sicurezza delle informazioni utilizza per i fornitori esterni e gli agenti (ad esempio, dovuta diligenza, accordi di non divulgazione, specifici obblighi contrattuali per la sicurezza delle informazioni e così via)?
- **Sicurezza fisica e controlli logici.** Quali procedure e misure per la sicurezza fisica vengono utilizzate dal fornitore? Il fornitore ha implementato un controllo dell'accesso al sistema sui suoi sistemi per restringere l'accesso alle informazioni solo al personale appositamente autorizzato?
- **Controlli per lo sviluppo del software.** Se il fornitore è un'azienda di sviluppo software, quali procedure di sviluppo e manutenzione utilizza? Quali controlli della sicurezza vengono implementati durante il ciclo di vita di sviluppo? Il fornitore conduce test di sicurezza sul suo software? Mantiene ambienti separati per le attività di test e produzione? Prende in licenza il codice di terze parti per integrarlo nei suoi prodotti? In caso affermativo, quali tipi di codice?
- **Questioni legate alla privacy.** Se le informazioni personali di clienti, consumatori o altri individui sono a rischio, il fornitore utilizza un'informativa sulla privacy per gestire la situazione? Qual è la cronologia delle revisioni dell'informativa? Esistono casi in cui il fornitore abbia dovuto contattare i clienti in merito a una violazione della sicurezza? Il fornitore offre ai suoi dipendenti una formazione specifica per la gestione delle informazioni personali? In caso affermativo, con quale frequenza?
- **Disaster recovery e business continuity.** Quali piani di business continuity/disaster recovery utilizza il fornitore? Quando sono stati testati l'ultima volta? Quando sono stati controllati l'ultima volta? I controlli condotti sui piani hanno generato risultati negativi? Le carenze sono state risolte? Qual è la cronologia delle revisioni dei suoi piani? Quali procedure di sicurezza vengono attuate presso il sito di recovery?

Protezioni contrattuali fondamentali: il secondo strumento

Nella stragrande maggioranza dei casi, il contratto stipulato tra un'azienda e i suoi fornitori prende in considerazione in maniera limitata, o ignora completamente, il tema della sicurezza delle informazioni. Al massimo, sono inclusi un veloce riferimento a requisiti di sicurezza vaghi e una clausola di base sulla riservatezza delle informazioni. Tuttavia, le best practice di settore (ad esempio, gli standard CERT e ISO) e le leggi e normative in materia di sicurezza delle informazioni attuali suggeriscono un'inclusione più specifica di questo tema nelle relazioni con i fornitori. È consigliabile considerare l'inclusione delle seguenti protezioni nei contratti con i fornitori:

Riservatezza. Una clausola di riservatezza dettagliata deve costituire l'elemento fondamentale per la sicurezza delle informazioni in qualsiasi contratto e deve fare riferimento a tutte le informazioni che l'azienda desidera mantenere riservate. Devono essere inclusi specifici esempi di informazioni protette (ad esempio, codice sorgente, piani di marketing, informazioni relative a nuovi prodotti, segreti commerciali, informazioni finanziarie, informazioni personali e così via). Laddove per la durata della protezione relativa alla riservatezza è possibile stabilire una scadenza (ad esempio, cinque anni), è necessario fornire esplicitamente una protezione continua su base permanente per le informazioni personali e i segreti commerciali dell'azienda. I requisiti che impongono che l'azienda segnali specifiche informazioni come "riservate" o "proprietarie" devono essere evitati perché non realistici nel contesto della maggior parte delle relazioni con i fornitori. Spesso le parti si rifiutano di ottemperare a questi requisiti, esponendo a rischio le informazioni riservate e proprietarie.

Garanzie. Oltre alle eventuali garanzie standard relative alla modalità di fornitura dei servizi e all'autorità di stipulare il contratto, è necessario prendere in considerazione le seguenti garanzie per la sicurezza delle informazioni:

- Garanzia che richiede al fornitore di conformarsi alle "best practice di settore relative alla sicurezza delle informazioni".
- Conformità a tutte le leggi e normative in materia di sicurezza delle informazioni, privacy, protezione dei consumatori e ad altre leggi simili.
- Conformità all'informativa sulla privacy dell'azienda per la gestione e l'utilizzo delle informazioni personali.
- Garanzia a tutela del rischio che le informazioni riservate dell'azienda diventino disponibili per subappaltatori esterni o aziende affiliate, fatto salvo in presenza di autorizzazione scritta da parte dell'azienda.
- Garanzia che le risposte fornite dal fornitore nel questionario sulla dovuta diligenza dei fornitori, da includere come documento allegato al contratto, sono veritiere ed esatte, che verranno aggiornate a seguito di una ragionevole richiesta da parte dell'azienda e che resteranno esatte e veritiere per l'intera durata del contratto tra le parti.

Obblighi di sicurezza generali. È opportuno considerare l'idea di includere informazioni generali sugli obblighi del fornitore di: adottare misure ragionevoli tese a proteggere i suoi sistemi contro il rischio di accesso non autorizzato o intrusione; condurre test periodici sui sistemi e le risorse esistenti finalizzati all'identificazione delle vulnerabilità; segnalare prontamente tutte le violazioni o le potenziali violazioni della sicurezza dell'azienda; partecipare a controlli della sicurezza condotti in maniera congiunta e collaborare con le autorità di regolamentazione dell'azienda per l'analisi delle pratiche di sicurezza delle informazioni seguite dal fornitore.

Il fornitore deve proteggere l'azienda dal rischio di processi ed eventuali altre rivendicazioni risultanti dall'incapacità del fornitore di garantire un'adeguata protezione dei propri sistemi.

Indennizzo. Nelle situazioni in cui una violazione della sicurezza del fornitore può esporre l'azienda a potenziali rivendicazioni da parte di terze parti (ad esempio, una violazione delle informazioni personali può dare luogo a richieste di risarcimento da parte dei clienti dell'azienda), il contratto deve includere una clausola di indennizzo che richieda al fornitore di evitare richieste di risarcimento, danni e spese a carico dell'azienda conseguenti a una violazione della sicurezza del fornitore. Pertanto, il fornitore deve proteggere l'azienda dal rischio di processi ed eventuali altre rivendicazioni risultanti dall'incapacità del fornitore di garantire un'adeguata protezione dei propri sistemi.

Limitazione di responsabilità. La maggior parte dei contratti prevede una clausola di "limitazione di responsabilità" appositamente ideata per limitare le tipologie e l'entità dei danni a cui possono essere esposte le parti contraenti. Non è inusuale che tali disposizioni neghino la responsabilità del fornitore per gli eventuali danni consequenziali (ad esempio, riduzione dei profitti, danneggiamento della reputazione dell'azienda e così via) e che limitino le altre responsabilità a una minima parte delle multe pagate. È pressoché impossibile eliminare questi tipi di clausole dalla maggior parte dei contratti, pur essendo tuttavia possibile richiedere al fornitore di non applicare limitazioni, quanto meno, di fornire sia una maggiore responsabilità per i danni derivanti dalla violazione della riservatezza che l'obbligo di indennizzo per le rivendicazioni risultanti dall'incapacità del fornitore di garantire un'adeguata protezione dei propri sistemi. Sostanzialmente, senza tali esclusioni, le protezioni contrattuali descritte sarebbero solo di tipo illusorio. Se il fornitore non si assume alcuna responsabilità per la violazione della riservatezza poiché la "limitazione della responsabilità" limita i danni a carico del fornitore a una cifra irrisoria, la clausola di riservatezza si rivela inutile.

Documento sui requisiti di sicurezza delle informazioni: il terzo strumento

L'ultimo strumento che consente di ridurre al minimo i rischi per la sicurezza è un documento o piano di lavoro che consente di definire i requisiti di sicurezza per una particolare transazione. Ad esempio, il documento sui requisiti di sicurezza delle informazioni può imporre al fornitore il divieto di trasmettere le informazioni aziendali su reti wireless interne (ad esempio, 802.11a/b/g) oppure di trasferirle su supporti rimovibili che possono essere facilmente persi di vista o smarriti. Tale documento può contenere anche specifici requisiti per l'uso della crittografia e la rimozione delle autorizzazioni relative all'hardware e ai supporti di archiviazione sui quali sono presenti le informazioni per garantire che queste ultime possano essere rimosse correttamente dall'hardware e dai supporti. È necessario identificare altre misure di sicurezza fisica e logica specifiche per una particolare transazione.

Le aziende risultano esposte a rischi elevati quando affidano le loro informazioni proprietarie e riservate a fornitori, partner aziendali e altre terze parti. È possibile ridurre al minimo tali rischi attraverso l'impiego degli strumenti descritti in precedenza: pratiche di dovuta diligenza appropriate e costanti, utilizzo di specifiche protezioni contrattuali relative alla sicurezza delle informazioni e potenziale utilizzo di documenti o altri allegati al contratto in cui vengono descritti in maniera dettagliata i requisiti di sicurezza da imporre al fornitore.

Iniziative Bring Your Own Device (BYOD)

7.0

“

Il 71% degli intervistati ritiene che le iniziative BYOD sono in grado di migliorare il morale dei dipendenti.

Con il termine BYOD si intendono quei programmi aziendali che autorizzano i dipendenti a utilizzare i dispositivi privati (ad esempio, smartphone, tablet, laptop, netbook) sia per le attività personali che per quelle lavorative. Generalmente, il dipendente può utilizzare il dispositivo privato anche per collegarsi alla rete della propria azienda.

Le iniziative BYOD offrono un'ampia serie di importanti vantaggi: potenziale riduzione dei costi aziendali per l'acquisizione e il mantenimento delle risorse IT, maggiori capacità per i lavoratori mobili, supporto del nuovo ambiente di lavoro con disponibilità 24 ore su 24, 7 giorni su 7 presso molte aziende e miglioramento tanto della collaborazione quanto del morale dei dipendenti. Un recente studio condotto da Unisys mette in particolare evidenza alcuni di questi vantaggi:

- Il 71% degli intervistati ritiene che le iniziative BYOD siano in grado di migliorare il morale dei dipendenti
- Il 60% ritiene che miglioreranno la produttività
- Il 44% considera un'offerta di lavoro più allettante se l'azienda fornisce il supporto per gli iPad.

Le iniziative BYOD sono per loro stessa natura rischiose, dal momento che permettono di archiviare e accedere sia a dati aziendali che personali da un unico dispositivo sul quale l'azienda non esercita alcun controllo o solo un controllo limitato. Questo rischio viene sottolineato da due studi recenti:

- **Studio di Dell KACE:** l'87% delle aziende non è in grado di proteggere in maniera efficace i dati aziendali e la proprietà intellettuale perché i dipendenti utilizzano i dispositivi privati, tra cui laptop, smartphone e tablet, per le attività lavorative.
- **Studio di eWeek:** il 62% degli amministratori IT ritiene di non disporre degli strumenti necessari per gestire correttamente i dispositivi privati.

Il rischio legato alle iniziative BYOD può essere mitigato concentrandosi sugli elementi comuni per la conformità illustrati in precedenza.

I rischi principali correlati alle iniziative BYOD

Al momento di decidere se attuare o meno un'iniziativa BYOD, un'azienda deve valutare e tentare di mitigare i rischi illustrati di seguito, appurando al tempo stesso i vantaggi conseguibili in termini di risparmi, morale dei dipendenti e così via.

Archiviazione dei dati aziendali e personali su un unico dispositivo. Rappresenta sicuramente uno dei principali problemi. Attualmente vi sono soluzioni, come la soluzione per i dispositivi mobili di Kaspersky, che consentono di definire "contenitori" per i dati personali e aziendali su un dispositivo BYOD. Tuttavia, solo un numero ristretto di esse permette di applicare separatamente i criteri di sicurezza per i due tipi di dati (ad esempio, in caso di smarrimento o furto del dispositivo, un processo di cancellazione dei dati avviato da remoto dall'azienda comporterà l'eliminazione di tutte le informazioni in esso archiviate, sia aziendali che personali). Le aziende e il personale aziendale devono prestare particolare attenzione a questi tipi di problemi.

Di seguito sono riportati alcuni esempi, estrapolati da situazioni reali, dei problemi che potrebbero verificarsi:

- **Le foto del matrimonio:** il primo esempio riguarda lo smartphone di un dipendente che si credeva smarrito. L'azienda ha eseguito un processo di cancellazione remota di tutti i dati presenti sul telefono per garantire l'integrità delle informazioni sensibili. In questo modo, è stato disattivato il telefono, che in realtà non era stato smarrito ma semplicemente perso di vista. La moglie del dipendente ha presentato una richiesta di risarcimento all'azienda dichiarando che quest'ultima aveva provocato l'eliminazione dell'unica copia esistente di fotografie di famiglia a cui teneva molto. Non considerando il fatto che il dipendente e la moglie avrebbero dovuto creare una copia di backup di queste fotografie così importanti, l'azienda si è ritrovata in una posizione difficile non disponendo di alcuna misura di protezione contro la rivendicazione presentata. È possibile fare riferimento alla sezione riportata più avanti relativa al "problema di amici e familiari".
- **Il romanzo perduto:** un altro esempio è quello di un datore di lavoro che ha consentito ai dipendenti di utilizzare i propri laptop. Dopo che il datore di lavoro ha installato un nuovo software di sicurezza sul laptop di ogni dipendente, uno di essi lo ha accusato di aver provocato la perdita dell'unica copia esistente del romanzo frutto di molti anni di lavoro. In questo caso, il datore di lavoro non disponeva di criteri appropriati in grado di proteggerlo contro rivendicazioni di quel tipo e alla fine ha dovuto risarcire il dipendente.
- **Servizi BYOC (Bring Your Own Cloud):** i servizi di backup online stanno diventando sempre più diffusi. Molti sono interoperabili e alcuni direttamente integrati con i sistemi operativi degli smartphone. Di recente si sono verificati molti casi in cui i dipendenti hanno utilizzato questi servizi "Bring Your Own Cloud" per eseguire una copia di backup dei loro dati personali, creando al contempo accidentalmente una copia dei dati aziendali sensibili (pertanto, i dati aziendali sono stati copiati sui server di terze parti sui quali l'azienda non esercitava alcun controllo o di cui non conosceva neanche l'esistenza e le terze parti utilizzavano misure di sicurezza speciali).

Problemi relativi alle licenze software. Le aziende devono impegnarsi per garantire che i dipendenti dispongano della licenza appropriata per il software di terze parti utilizzato per i dispositivi BYOD: un dipendente non può acquistare la versione "home" della licenza di un programma di elaborazione dati e poi usare il programma sul proprio laptop BYOD per svolgere le attività lavorative quotidiane. Se lo facesse, verrebbe sicuramente violato l'accordo di licenza di terze parti relativo al software. Un altro esempio è quello in cui il dispositivo BYOD utilizza una connessione VPN (Virtual Private Network) per accedere a un software di terze parti installato sui sistemi del datore di lavoro (ad esempio, applicazione di contabilità, software CRM, software di immissione ordini e così via). In casi di questo tipo, è necessario verificare sempre che gli accordi di licenza di terze parti consentano tale accesso remoto. Talvolta possono essere applicati costi di licenza aggiuntivi.

Pertanto, un dipendente deve valutare tanto i vantaggi conseguibili che gli svantaggi causati dall'uso del dispositivo privato.

Istruzione probatoria/Controversia legale. Al momento di decidere se prendere parte o meno all'iniziativa BYOD del proprio datore di lavoro, un dipendente deve valutare tanto i vantaggi conseguibili che gli svantaggi causati dall'uso del dispositivo privato. Nello specifico, il dipendente deve avere ben chiaro che il datore di lavoro e, potenzialmente, delle terze parti potrebbero aver bisogno di accedere ai dati presenti sul suo dispositivo nel contesto di una controversia legale. Sul dispositivo potrebbero essere archiviate informazioni quali e-mail, fotografie, dati di geolocalizzazione e così via. Inoltre, il dipendente deve essere a conoscenza del fatto che, in specifiche circostanze, il datore di lavoro potrebbe avere il giusto motivo per procedere alla cancellazione remota dei contenuti del dispositivo. A meno che il dipendente non abbia creato una copia di backup dei contenuti del dispositivo, tale processo di cancellazione potrebbe comportare la perdita di tutti i suoi dati personali. Questi sono fattori importanti, che è necessario valutare con particolare attenzione prima di accettare di prendere parte a un'iniziativa BYOD.

Stress da lavoro ripetitivo e altri tipi di infortuni sul lavoro. L'attuazione di una politica BYOD efficace richiede l'attenta valutazione di problemi quali il "pollice da BlackBerry" o altri tipi di condizioni generate dallo stress da lavoro ripetitivo che insorge con l'uso di smartphone, tablet e altri dispositivi simili. Ad esempio, è necessario chiedere ai dipendenti che aderiscono all'iniziativa di leggere le informazioni ergonomiche fornite con la maggior parte dei dispositivi, informare i partecipanti che il dipendente non può essere ritenuto responsabile per gli eventuali infortuni correlati dall'uso di tali dispositivi e così via. L'azienda deve anche esaminare l'assicurazione contro gli infortuni sul lavoro e altri tipi di assicurazione per verificare che sia prevista una copertura anche per gli infortuni derivanti dall'uso di dispositivi non forniti dall'azienda.

Uso condiviso dei dispositivi con persone che non siano colleghi: il problema relativo ad amici e familiari. In genere, i dispositivi BYOD dei dipendenti vengono tranquillamente utilizzati anche dai loro amici e familiari. Pertanto, queste terze parti possono potenzialmente accedere a tutte le informazioni aziendali archiviate su tali dispositivi. Situazioni di questo tipo non possono essere impedite. E, fattore che peggiora ulteriormente le cose, non è disponibile una tecnologia che consenta di mitigare in maniera tempestiva questo rischio.

Il problema consiste nel fatto che queste terze parti non vengono vincolate dall'azienda attraverso l'obbligo di non divulgazione o altri obblighi di riservatezza e che non hanno sottoscritto la politica aziendale relativa all'uso del dispositivo BYOD. Ciò comporta che l'azienda non dispone di protezioni contrattuali con le terze parti in questione.

Ad esempio, se le terze parti inviano e ricevono e-mail personali utilizzando il dispositivo e in seguito l'azienda dovrà accedere al dispositivo nel contesto di una controversia legale, è possibile che l'azienda violi i diritti alla privacy delle terze parti nel momento in cui accederà, pur se accidentalmente, alle loro e-mail personali. Analogamente, se l'azienda ha il giusto motivo per procedere alla cancellazione remota dei contenuti del dispositivo, il dipendente non potrà presentare alcuna richiesta di risarcimento contro l'azienda poiché avrà sottoscritto una politica che contempla questa possibilità, mentre i familiari e gli amici potranno avanzare rivendicazioni contro l'azienda perché non avranno sottoscritto tale politica. In questo caso, se con il processo di cancellazione dei dati vengono eliminate importanti informazioni delle terze parti, queste ultime potrebbero presentare una richiesta di risarcimento per danni contro l'azienda.

Smaltimento del dispositivo da parte del dipendente. È indispensabile adottare misure tese a garantire che il datore di lavoro possa verificare che siano stati rimossi tutti i dati aziendali sensibili prima dello smaltimento di un dispositivo. Le aziende devono essere consapevoli del fatto che i dipendenti sono sempre alla ricerca degli ultimi smartphone, tablet o laptop e che i dispositivi da essi utilizzati potrebbero essere restituiti in permuta, venduti su eBay o smaltiti in altro modo con un preavviso minimo al datore di lavoro o addirittura senza alcun preavviso. Accedere al dispositivo potrebbe rivelarsi particolarmente difficile nelle situazioni in cui il rapporto lavorativo sia stato estinto bruscamente. Il dipendente potrebbe rifiutarsi di concedere l'accesso ai contenuti del dispositivo. In casi di questo tipo, il datore di lavoro potrebbe non avere altre alternative se non la cancellazione remota dei dati del dispositivo.

Elementi fondamentali della strategia BYOD

Per gestire i tre elementi comuni della conformità illustrati in precedenza (requisito CIA, azioni ragionevoli/appropriate e adattamento), è necessario che un'iniziativa BYOD abbracci tre componenti: politica, formazione e tecnologia/applicazione dei criteri di sicurezza.

Politica. Ogni iniziativa BYOD è regolamentata dal documento contenente una politica chiara e di facile comprensione. Tale politica illustra in maniera dettaglia i diritti e gli obblighi del dipendente correlati all'iniziativa, tra cui la comunicazione al dipendente che la sua eventuale partecipazione all'iniziativa comporterà l'annullamento di specifici diritti. Ad esempio, i dati archiviati sul suo dispositivo mobile, tra cui i dati personali, potrebbero venire esaminati durante il processo di istruzione probatoria correlato a una controversia legale oppure i dati personali potrebbero venire irrecuperabilmente smarriti durante un processo di cancellazione remota realizzato con il fine di proteggere le informazioni aziendali in caso di eventuale perdita o danneggiamento di altro tipo del dispositivo.

La maggior parte delle aziende distribuisce ai dipendenti tale politica e ne richiede la sottoscrizione prima di consentire l'adesione all'iniziativa. Nella politica deve essere chiaramente menzionato che l'azienda ha la facoltà di revocare l'iniziativa in qualsiasi momento. Ad esempio, l'azienda potrebbe optare per la cessazione dell'iniziativa o stabilire che l'utilizzo del dispositivo da parte di un determinato dipendente faccia insorgere un eccessivo rischio per la sicurezza. In casi di questo tipo, l'azienda deve avere l'incontestabile diritto di interrompere l'iniziativa o di escludere un dipendente dall'iniziativa.

Numerose organizzazioni inviano occasionalmente dei messaggi di promemoria in cui vengono messi in particolare evidenza specifici punti della politica. Ad esempio, un datore di lavoro può inviare un promemoria in cui vengono descritti particolari rischi o divieti correlati alla creazione di copie di backup dei dati aziendali negli account di backup online di un dipendente (ad esempio, DropBox, iCloud e così via).

Formazione. La formazione dei dipendenti è un altro dei fattori fondamentali per un'efficace iniziativa BYOD. Generalmente, non si rivela sufficiente consegnare ai dipendenti un documento che descrive la politica, dal momento che potrebbero anche non leggerla. È invece preferibile condurre una o più sessioni di formazione per informare i dipendenti sui diritti e obblighi correlati alla loro adesione all'iniziativa. In base al livello di sensibilità delle informazioni alle quali può accedere il dipendente, queste sessioni di formazione possono anche essere ripetute periodicamente.

Tecnologia/Applicazione della politica. L'ultimo componente riguarda l'uso della tecnologia e degli altri strumenti necessari per l'applicazione della politica. Ciò può comportare semplicemente la richiesta ai dipendenti di utilizzare solo i dispositivi BYOD che supportino l'applicazione remota della politica di sicurezza (ad esempio, password obbligatorie, timeout, cancellazione remota e così via). Sono ora disponibili anche altre tecnologie più avanzate, tra cui la possibilità di separare i dati personali da quelli aziendali.

Come illustrato nelle sezioni relative ai tre elementi comuni per la conformità, l'azienda deve investire in questi componenti in base al tipo di informazioni che verranno esposte a rischio tramite l'iniziativa BYOD.

Conclusioni

8.0

A fronte del costante aumento del numero di leggi e normative in materia di privacy e sicurezza delle informazioni sempre più complesse, le aziende dovrebbero apprezzare alcuni elementi comuni a molte di loro. Questo whitepaper ha illustrato tre degli elementi comuni più diffusi e importanti. Una volta compreso che la legge vigente non richiede la perfezione, ma solo una dovuta cura, azioni ragionevoli e misure di adattamento dell'approccio in base alla sensibilità dei dati esposti a rischio, le aziende possono compiere progressi considerevoli verso il traguardo della conformità.

Nelle sezioni relative alla sicurezza delle informazioni nelle relazioni con i fornitori e allo sviluppo di un'efficace iniziativa BYOD è stato descritto in che modo questi punti comuni sono applicabili a situazioni reali. Un uso ponderato di formazione, criteri e tecnologia consente di ridurre in maniera decisamente significativa il rischio complessivo legato alla conformità.

Informazioni sull'autore
Michael R. Overly è un partner che lavora nell'Information Technology and Outsourcing Group dell'ufficio di Los Angeles di Foley & Lardner LLP. Overly è autore di numerosi documenti e partecipa con grande frequenza a conferenze sui temi della negoziazione e progettazione di transazioni tecnologiche e dei problemi legali correlati all'uso della tecnologia nel luogo di lavoro, all'e-mail e alle prove digitali. Ha scritto un'ampia serie di testi e articoli su questi argomenti ed è spesso presente come commentatore sui mezzi di informazione nazionali (ad esempio, New York Times, Chicago Tribune, Los Angeles Times, Wall Street Journal, ABCNEWS.com, CNN e MSNBC). Oltre a condurre seminari di formazione negli Stati Uniti, in Norvegia, in Giappone e in Malesia, Overly ha testimoniato davanti al Congresso degli Stati Uniti nel corso di cause relative a problemi della realtà online. È autore, tra gli altri, dei seguenti testi: "Guide to IT Contracting: Checklists, Tools and Techniques" (CRC Press 2012), "E-Policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets" (AMACOM 1998), "Overly on Electronic Evidence" (West Publishing 2002), "The Open Source Handbook" (Pike & Fischer 2003), "Document Retention in The Electronic Workplace" (Pike & Fischer 2001), e "Licensing Line-by-Line" (Aspatore Press 2004).

Kaspersky Endpoint Security for Business

Kaspersky offre una piattaforma di sicurezza completa in grado di garantire la massima protezione dell'azienda, consentendo di proteggere e controllare gli endpoint (fisici, mobili e virtuali), proteggere server e gateway oppure gestire da remoto l'intero ambiente di sicurezza.

Kaspersky Endpoint Security for Business vanta una gamma completa di tecnologie e strumenti tra cui anti-malware, controlli degli endpoint, crittografia, Mobile Device Management (MDM), gestione dei sistemi, gestione della patch e inventari di licenze. Inoltre, mentre un numero sempre crescente di aziende capisce i vantaggi dell'adozione di un'iniziativa Bring Your Own Device (BYOD) che consenta ai dipendenti di utilizzare dispositivi mobili privati per attività aziendali, è possibile abilitare l'approccio BYOD tramite la soluzione Mobile Security e lo strumento MDM.

I prodotti di Kaspersky sono progettati affinché l'amministratore possa avvalersi di una posizione centralizzata per visualizzare e gestire l'intero scenario di sicurezza. Sono tutti perfettamente interoperabili e supportati dal servizio basato su cloud Kaspersky Security Network, per offrire alle aziende l'avanzato livello di protezione di cui hanno bisogno per contrastare al meglio le più sofisticate e diversificate minacce informatiche.

Kaspersky offre una piattaforma realizzata in modo integrato che consente agli amministratori IT di osservare, controllare e proteggere l'ambiente IT con la massima semplicità. I moduli di sicurezza, gli strumenti e la console di amministrazione di Kaspersky sono sviluppati internamente in modo da poter garantire stabilità, criteri integrati, reporting efficiente e strumenti intuitivi.

Kaspersky Endpoint Security for Business è l'unica vera piattaforma di sicurezza del settore realizzata in modo integrato.

Informazioni su Kaspersky
Kaspersky Lab è il maggior fornitore privato di soluzioni per la protezione degli endpoint al mondo. L'azienda è tra i primi quattro fornitori mondiali di soluzioni di sicurezza per utenti endpoint. Da 15 anni, Kaspersky Lab è pioniere della sicurezza IT e offre soluzioni efficaci per la sicurezza digitale a privati e piccole, medie e grandi imprese. L'azienda è attualmente presente in quasi 200 paesi e territori a livello globale e offre soluzioni di protezione a oltre 300 milioni di utenti in tutto il mondo.

Ulteriori informazioni sul sito Web www.kaspersky.it/business