UNA DOMANDA IMPORTANTE: CHE COSA NON SAPETE SULLA CYBERSECURITY?

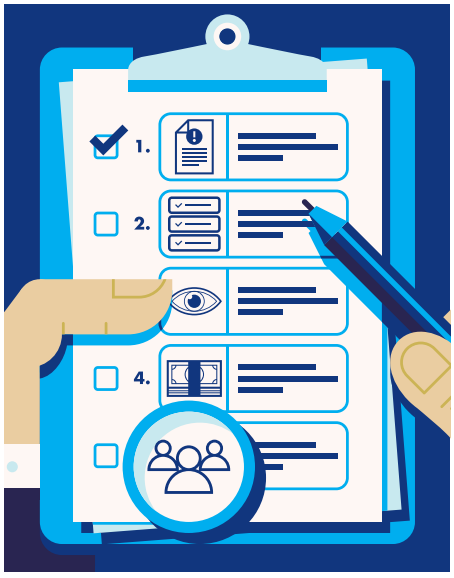
I consigli di amministrazione devono essere informati al meglio. Per questo motivo, devono sapere quali sono le domande da fare, dicono GEORGE LITTLE e SOFIA MATA-LECLERC di Brunswick

Negli ultimi tre anni, sempre più attacchi di grande entità in una vasta gamma di settori, tra cui il settore finanziario e quello sanitario, hanno divulgato i dati personali di milioni di persone e reso la sicurezza informatica una delle principali tematiche all'ordine del giorno dei consigli di amministrazione. La preoccupazione è reale. Un recente studio di IBM ha rilevato che il 94 per cento dei dirigenti ritiene probabile che le proprie società possano essere oggetto di un significativo incidente di sicurezza informatica nei prossimi due anni.

Una violazione può comportare una perdita di dati, di proprietà intellettuale e di fiducia dei clienti. Nei casi più gravi, una violazione può bloccare la capacità operativa di una società. Le ripercussioni includono danni di immagine, dimissioni, sanzioni, azioni di regolamentazione, perdite negli affari e azioni legali collettive. Il costo medio di una violazione dei dati è aumentato del 23 percento dal 2014, secondo il Ponemon Institute, un'organizzazione di ricerca sulla sicurezza dei dati.

La recente ricerca Brunswick Insight ha evidenziato che il 74 percento dei membri di consigli di amministrazione è d'accordo sull'importanza di conoscere i rischi informatici. Tuttavia Gavin Patterson, amministratore delegato del gruppo di telecomunicazioni BT, ha detto ai partecipanti al Forum economico mondiale di Davos, che la maggior parte dei consigli di amministrazione non ha ancora l'esperienza per gestire tali sfide.

"Il rischio sta mutando la sua natura e sta diventando più sofisticato", ha detto. "Anche se credo sia ormai noto ai consigli di amministrazione, non sono sempre convinto che quando parlo ad altri amministratori delegati ci sia una comprensione tecnica elevata".



Intanto, la posta in gioco sta diventando personale. Le azioni legali connesse alle violazioni di dati sono state presentate contro i consigli di amministrazione di Target, Wyndham Worldwide e Home Depot. I querelanti sostengono che i membri del consiglio di amministrazione non hanno ottemperato al loro obbligo di proteggere le informazioni dei clienti.

La sicurezza informatica è una questione complessa che può derivare da qualsiasi decisione aziendale, non solo da quelle relative al settore IT. Pur non dovendo essere degli esperti, i membri del consiglio di amministrazione devono conoscere a fondo i rischi in cui la società può incorrere e le procedure in atto per gestire un attacco informatico. I consigli di amministrazione dovrebbero ricercare all'esterno le competenze informatiche, dice Holly Gregory, partner dello studio legale aziendale Sidley Austin. Tuttavia, alla fine, la responsabilità degli effetti sulla società rimane del consiglio.

"In sostanza, la 'decisione imprenditoriale' si applica a tutte le decisioni relative alla supervisione delle questioni di sicurezza informatica", dice Gregory. In altre parole, "i dirigenti devono attenersi agli standard essenziali di precisione, lealtà e buona fede applicati generalmente alle azioni del consiglio di amministrazione".

Un dialogo regolare in merito alla gestione dei rischi informatici della società contribuisce a fare in modo che questa rimanga una priorità per la leadership. La forma e la frequenza dei briefing del consiglio varieranno in base alle dimensioni della società, al tipo di dati raccolti e alla natura delle questioni di sicurezza informatica che affronta.

Ogni consiglio deve decidere autonomamente su come strutturare il dialogo tra i suoi membri. Alcuni possono scegliere di nominare un responsabile della sicurezza informatica o creare una commissione specializzata.

A prescindere da come sia gestita, una strategia di sicurezza informatica efficace richiede più di una decisione o discussione. I consigli devono impegnarsi a rivedere e aggiornare regolarmente la loro conoscenza dei rischi.

Possono non essere degli esperti, ma devono essere informati. Per questo, devono sapere che cosa chiedere.

Cinque domande che ogni board deve porsi

1. Quali procedure sono in vigore per gestire una violazione?

Una risposta ideale dimostrerà che la società ha analizzato diversi scenari. I piani per la gestione di una violazione devono andare oltre la semplice comunicazione della situazione ai team IT e legale e dovrebbero includere il servizio clienti, le relazioni con il governo e il pubblico e le comunicazioni ai dipendenti. I dirigenti del consiglio, l'amministrazione e le varie divisioni aziendali devono comprendere il loro ruolo nel piano generale. Le multinazionali devono considerare i requisiti di segnalazione e devono tenere conto di complessità di coordinazione aggiuntive in tutte le aree.

2. Avete testato i vostri piani di intervento?

Una simulazione a tavolino consente ad un'attività di effettuare uno stress test e migliorare il modo in cui gestire una crisi. L'esercizio aiuta le società a scoprire in quali settori è necessaria maggiore preparazione. Il responsabile di queste simulazioni varierà in base alla società. Tuttavia le prove devono prevedere una partecipazione estesa a tutti i livelli nell'organizzazione, compreso l'amministratore delegato. Il gruppo deve essere sicuro che la simulazione comprenda una risposta che si rivolga a tutti i soggetti interessati, coinvolga tutte le risorse, si inserisca in tutte le procedure ed evidenzi imprevisti in una certa divisione causati da altre divisioni.

3. I clienti comprendono le vostre pratiche di raccolta e uso dei dati?

Non volete che i clienti vengano a conoscenza dei dati che avete da una comunicazione di violazione o dalla copertura mediatica. Invece, la vostra società doverebbe valutare periodicamente raccolta e uso dei suoi dati e il modo in cui potrebbe mettere a rischio l'immagine aziendale. Acssicurative che la cronologia dei vostri dati sia chiara e che stiate esprimendo al meglio il valore per i clienti. Sempre più spesso, le organizzazioni redigono le proprie politiche sulla privacy tenendo a mente questo concetto ed indicando chiaramente ciò che raccolgono e perché.

4. In che modo decidete quanto, e dove, investire nella sicurezza?

La sicurezza assoluta non è realizzabile e il solo numero di possibili canali di attacco impedisce una difesa invulnerabile. Inoltre, alcune società possono scegliere di assumersi maggiori rischi per migliorare l'esperienza dei clienti. Alla luce di questo, le società devono valutare il livello di sicurezza rispetto ai bisogni aziendali. Le società più attive stanno considerando la sicurezza all'inizio del ciclo di sviluppo del prodotto. Dovrebbero organizzare la sicurezza su più livelli, concentrando le risorse aggiuntive sui dati maggiormente sensibili e lavorando a partire da quel punto.

5. State istruendo i dipendenti in merito alle best practice sulla sicurezza informatica?

I dipendenti di una società sono sempre più visti come il collegamento più debole in qualsiasi regime di sicurezza dei dati. Sono vulnerabili agli attacchi di "spear-phishing", quando una e-mail che sembra provenire da una fonte certa - una persona o una società - richiede informazioni protette sulla società. La speranza è che il destinatario risponda in maniera automatica, servendo i dati su un piatto d'argento. Cinque grandi società su sei - quelle con più di 2.500 dipendenti - sono state oggetto di attacchi di spear-phishing nel 2014, in base al recente Internet Security Threat Report di Symantec. Si tratta di un aumento del 40 percento rispetto allo scorso anno. Per contrastare queste truffe, sempre più società scelgono di istruire i dipendenti in merito ai principali rischi di sicurezza informatica. Questi programmi devono essere associati all'uso di strumenti di controllo, tra cui i requisiti obbligatori di password complesse. L'obiettivo è rendere consapevoli i dipendenti, dando loro una conoscenza di base: come rilevare un tentativo di violazione della sicurezza, a chi rivolgersi per porre domande e chi informare quando si identifica una minaccia potenziale.

GEORGE LITTLE è un partner dell'ufficio di Washington DC di Brunswick, specializzato in questioni legate a crisi, sicurezza informatica, immagine e pubbliche relazioni.
SOFIA MATA-LECLERC è dirigente a San Francisco, specializzata in questioni legate a crisi, sicurezza informatica e immagine aziendale.

IMMAGINI: JUSTIN MEZZELL