Il costo del silenzio: perché i CFO non possono ignorare il rischio informatico

value through insight™

IL RISCHIO INFORMATICO SI È ORMAI ALLONTANATO DI GRAN LUNGA DALLA SALA SERVER.

Oggi riguarda proprio gli aspetti che preoccupano maggiormente i CFO: flusso di cassa, fiducia dei clienti, continuità operativa, conformità, valore aziendale e la capacità dell'azienda di andare avanti quando qualcosa va storto.

Ecco perché la vecchia distinzione tra "rischio IT" e "rischio aziendale" non è più valida. Un grave incidente informatico può bloccare le operazioni commerciali, ritardare la produzione, esporre dati sensibili, coinvolgere i dirigenti in azioni legali e normative, compromettere i fornitori e minare la fiducia dei clienti. Può inoltre generare costi improvvisi e imprevisti proprio nel momento in cui l'azienda ha meno controllo.

Il vero pericolo non è solo l'attacco in sé, ma la tranquilla sicurezza che lo circonda: la convinzione che la copertura assicurativa esistente sia sufficiente, che il piano di continuità rifletta ancora la realtà, che i fornitori siano pronti e che l'organizzazione possa riprendersi entro gli stessi tempi previsti un anno fa.

Paul Gravatt, specialista in rischi e assicurazioni di ERA Group, descrive la criminalità informatica come una delle maggiori minacce globali dal punto di vista del rischio e delle assicurazioni. Non si tratta più di singoli individui isolati che causano disagi da dietro un laptop. Sempre più spesso, la criminalità informatica è organizzata, motivata politicamente e altamente sofisticata.

Questo cambia la prospettiva. La criminalità informatica non è solo un problema tecnico. È un'esposizione finanziaria. E il costo di un errore raramente si traduce in una semplice voce di bilancio.

L'opportunità nascosta nel rischio

L'ultima indagine britannica sulle violazioni della sicurezza informatica sottolinea la portata del problema. Nel 2025/26, il 43% delle aziende ha segnalato una violazione o un attacco informatico, con il phishing che da solo ha colpito il 38%. In totale, l'indagine stima che circa 612.000 aziende britanniche abbiano identificato almeno una violazione o un attacco nel corso dell'anno.

Questo è il quadro preoccupante. Ma non si tratta solo di un aumento delle minacce. È anche una questione di tempismo.

Secondo Paul, sebbene la gravità e la visibilità degli attacchi informatici siano aumentate, molte organizzazioni stanno diventando anche più resilienti. In alcuni segmenti del mercato, i premi delle assicurazioni contro i rischi informatici sono in calo, il che offre alle aziende un'occasione concreta per valutare se una copertura più solida, limiti più elevati o una protezione più ampia possano ora essere più accessibili rispetto al passato.

Per i CFO, ciò non significa acquistare una copertura informatica a sé stante o semplicemente aggiungere un'altra voce di costo. Significa esaminare il costo totale del rischio dell'organizzazione e porsi una domanda più pertinente: i risparmi in altri settori assicurativi, nei costi dei fornitori o nelle spese operative potrebbero essere utilizzati per finanziare una maggiore resilienza informatica?

Quando si pensa al rischio informatico, spesso si immagina il ransomware: sistemi bloccati, schermi congelati, attività di trading interrotte e una richiesta di riscatto sul tavolo. Questo accade, naturalmente. Ma il costo più doloroso si trova spesso in un ambito completamente diverso.

Si manifesta quando non è possibile emettere fatture, elaborare ordini o servire i clienti. Si manifesta quando le linee di produzione si fermano, non è possibile rifornire le scorte, si ricorre a fornitori di emergenza a tariffe maggiorate e i team dirigenziali perdono giorni in attività legali, normative e di comunicazione. Anche dopo il ripristino dei sistemi, il danno reputazionale può continuare a persistere.

È qui che il dibattito deve andare oltre la sicurezza informatica per concentrarsi sulla continuità operativa.

Paul sottolinea che le interruzioni più estese della catena di approvvigionamento hanno cambiato il quadro del ripristino. Sostituire le attrezzature, reperire materiali da costruzione o rifornire le scorte può ora richiedere più tempo di quanto molte aziende presumano. Un piano di ripristino che un anno fa sembrava ragionevole potrebbe essere già obsoleto. L'assicurazione contro l'interruzione dell'attività deve essere valutata alla luce di questa realtà, in particolare per quanto riguarda i periodi di indennizzo e la durata effettiva del periodo in cui un'azienda potrebbe aver bisogno di sostegno.

Un'azienda può avere una copertura assicurativa, ma è sufficiente? Può avere un piano di ripristino, ma è ancora valido? Può aver previsto i tempi di inattività, ma ha tenuto conto dell'attuale situazione della catena di approvvigionamento? Può presumere che le attrezzature sostitutive arrivino nel giro di poche settimane, ma cosa succede se ci vogliono mesi?

Il costo del silenzio è spesso nascosto in queste ipotesi.

Il rischio informatico non si limita al proprio ambito

Azunna Anyanwu, consulente di ERA Group negli Stati Uniti, offre un punto di vista importante. Per i direttori finanziari, il costo del rischio informatico non è solo finanziario. L'impatto finanziario è spesso il risultato visibile di fallimenti in altri ambiti: reputazione, operazioni o conformità.

Questo è importante perché il danno non si ferma una volta che il problema tecnico è stato contenuto.

Il rischio reputazionale è uno degli aspetti più difficili da quantificare correttamente e uno dei più facili da sottovalutare. Una violazione può danneggiare il marchio dell'organizzazione, l'immagine pubblica, la fiducia degli stakeholder e quella dei clienti. Questi effetti possono poi tradursi in conseguenze finanziarie molto concrete, quali perdita di ricavi, minore fidelizzazione, maggiori costi di acquisizione e riduzione del valore aziendale.

Questo fenomeno è diventato più marcato poiché i gruppi di ransomware utilizzano sempre più spesso i dati rubati come leva. La minaccia non è sempre «pagateci o i vostri sistemi rimarranno inattivi». Può diventare «pagateci o pubblicheremo ciò che abbiamo trovato». Azunna descrive questo fenomeno come «caccia alla vergogna», in cui l'esposizione pubblica di informazioni sensibili diventa la tattica di pressione, piuttosto che la sola interruzione operativa.

Il rischio operativo può essere più silenzioso, ma altrettanto dannoso. È il processo che fallisce, il sistema non disponibile, l'account e-mail compromesso, il problema di un partner che improvvisamente diventa un vostro problema. Il Business Email Compromise e i pagamenti errati ai fornitori ne sono ottimi esempi, perché dall'esterno non sempre appaiono drammatici. Un pagamento viene inviato al destinatario sbagliato, un processo di un fornitore fallisce, il denaro esce dall'azienda e l'impatto è dolorosamente reale.

Anche la catena di fornitura è un aspetto importante. Un'azienda non deve necessariamente essere l'obiettivo diretto per subire le conseguenze di un incidente informatico. Se un fornitore chiave, un partner logistico, un fornitore di tecnologia o un processo esternalizzato viene compromesso, l'interruzione può ripercuotersi rapidamente sui propri ricavi, sull'erogazione dei servizi, sulla produttività della forza lavoro e sugli impegni nei confronti dei clienti.

Poi c'è la questione della conformità. Gli incidenti informatici possono comportare responsabilità legali, controlli normativi, obblighi contrattuali e standard specifici del settore. Un inadempimento in questo ambito può generare responsabilità impreviste, spese legali, costi di transazione e, nei settori regolamentati, la perdita di future opportunità commerciali.

Per le organizzazioni statunitensi, questo aspetto di governance sta diventando sempre più difficile da ignorare. Le società quotate in borsa operano secondo le norme della SEC in materia di informativa sulla sicurezza informatica, che richiedono la comunicazione degli incidenti di sicurezza informatica rilevanti tramite il Modulo 8-K entro quattro giorni lavorativi dalla determinazione della rilevanza, oltre alla rendicontazione annuale sulla gestione del rischio informatico, sulla strategia e sulla governance.

Anche l'esposizione finanziaria è impressionante. L'Internet Crime Complaint Center dell'FBI ha ricevuto 859.532 denunce nel 2024, con perdite segnalate che hanno superato i 16,6 miliardi di dollari.

Cosa dovrebbero chiedersi ora i CFO

La giusta conversazione sulla sicurezza informatica non parte dal software. Parte dall'esposizione.

Un direttore finanziario non ha bisogno di conoscere ogni dettaglio tecnico dell'ambiente informatico, ma deve comprendere quali sarebbero le conseguenze di un incidente grave per l'azienda dal punto di vista finanziario, operativo e commerciale.

Cosa accadrebbe se i sistemi fossero indisponibili per una settimana? Quali flussi di ricavi si interromperebbero per primi? Sarebbe ancora possibile emettere fatture? Si potrebbero ancora elaborare le buste paga? Quali fornitori diventerebbero immediatamente critici? L'assicurazione risponderebbe nel modo in cui l'azienda si aspetta? I periodi di indennizzo sono sufficientemente lunghi? I limiti di copertura per i rischi informatici sono realistici? L'organizzazione è esposta a rischi tramite terze parti? Qualcuno ha verificato le ipotesi su cui si basa il piano di ripristino?

Queste domande non hanno lo scopo di creare panico, ma di garantire visibilità.

La visibilità offre ai CFO delle opzioni. Consente loro di mettere in discussione le coperture assicurative, valutare i fornitori, migliorare i piani di continuità operativa, rafforzare la tutela contrattuale e decidere dove sono realmente necessari gli investimenti. Consente inoltre di esaminare la base di costo nel suo complesso e individuare dove i risparmi potrebbero finanziare una maggiore resilienza senza limitarsi ad aggiungere ulteriori costi all'azienda.

Come può aiutarti ERA Group

ERA Group aiuta le organizzazioni ad analizzare il rischio informatico da una prospettiva commerciale.

Non sostituiamo i team IT interni, i CISO o gli specialisti tecnici in materia di sicurezza informatica. Non è questo il nostro ruolo. Il nostro lavoro si affianca al loro, aiutando i CFO e i team dirigenziali a comprendere le implicazioni finanziarie, operative, assicurative e relative ai fornitori del rischio informatico.

Ciò può significare rivedere l'assicurazione contro i rischi informatici e il costo totale del rischio, effettuare un'analisi comparativa del mercato, verificare i limiti e le esclusioni e valutare se i risparmi ottenuti in altre linee assicurative possano essere utilizzati per rafforzare la protezione informatica.

Può anche significare considerare insieme la copertura per l'interruzione dell'attività e la pianificazione della continuità operativa, anziché trattarle come attività separate. Se i tempi di ripristino sono cambiati a causa delle pressioni sulla catena di approvvigionamento, della disponibilità delle attrezzature, della dipendenza dai fornitori o della complessità operativa, il programma assicurativo deve riflettere tali cambiamenti.

Dal punto di vista tecnologico, ERA può aiutare le organizzazioni a comprendere l'andamento della spesa per il cloud e l'IT, se la fatturazione è strutturata in modo efficace e dove i costi possono essere ottimizzati senza compromettere la resilienza.

La revisione dei fornitori e dei contratti è un altro aspetto fondamentale del quadro. Il rischio informatico spesso si propaga attraverso terze parti, quindi è importante capire quali fornitori siano critici, quali responsabilità siano previste dal contratto, se i livelli di servizio siano chiari e se gli aumenti dei costi o gli accordi di trasferimento del rischio siano ragionevoli.

L'obiettivo non è quello di spaventare le aziende per indurle a spendere di più, ma di aiutarle a spendere meglio.

ERA aiuta i clienti a individuare valore all'interno della loro struttura dei costi, in modo che possano rafforzare la propria resilienza senza considerare la sicurezza informatica come un semplice costo inevitabile.

Parliamone

Il rischio informatico non sta scomparendo. Sta diventando più sofisticato, più interconnesso con le catene di approvvigionamento e più visibile per autorità di regolamentazione, assicuratori, clienti e investitori.

Per i direttori finanziari, il pericolo non è solo che accada qualcosa. Il rischio maggiore è scoprire troppo tardi che l'azienda non aveva compreso il costo di ciò che avrebbe potuto accadere.

La copertura era troppo limitata. Il periodo di indennizzo era troppo breve. L'esposizione dei fornitori era maggiore del previsto. L'ambiente cloud era più complesso di quanto chiunque si rendesse conto.

Il costo del silenzio è già presente nei registri dei rischi, nei programmi assicurativi, nei contratti con i fornitori, nelle fatture relative al cloud, nei processi di pagamento e nei piani di continuità operativa.

Le organizzazioni che agiscono ora saranno in una posizione migliore per proteggere non solo i propri sistemi, ma anche il flusso di cassa, la reputazione e la resilienza.

Want to know more?
eragroup.com

value through insight™