kyndryl

Risultati del sondaggio

Cosa dicono i responsabili delle decisioni IT sullo stato di rischio dell'IT

Il rischio IT è diventato un argomento di discussione a livello di consiglio di amministrazione.

In un mondo in cui le organizzazioni si affidano a sistemi IT ibridi, complessi e distribuiti in varie aree geografiche, un'interruzione della rete, un attacco malware o un disservizio del sistema di altro tipo può avere effetti devastanti sulla produttività, la reputazione e il risultato economico finale di un marchio.

Per questo, i consigli di amministrazione di molte aziende stanno facendo pressioni sui loro team dirigenziali per ottenere informazioni dettagliate sulla preparazione in vista di un simile incidente.

Considerata l'alta posta in gioco, abbiamo cercato di valutare le percezioni del rischio IT e le iniziative intraprese dalle organizzazioni per abilitare la resilienza informatica. Abbiamo intervistato un gruppo a livello mondiale di responsabili delle decisioni IT e professionisti nel campo del rischio e della conformità per conoscere le avversità che hanno vissuto, i rischi IT che li preoccupano maggiormente e le iniziative intraprese dalle loro organizzazioni per anticipare, proteggere, opporsi e ripristinare in caso di rischi.

I risultati di questo sondaggio costituiscono il report sullo stato di rischio dell'IT per il 2023.

I nostri risultati confermano che i sistemi IT delle organizzazioni stanno effettivamente subendo interruzioni. Abbiamo scoperto qual è l'ostacolo più frequente agli sforzi volti ad attenuare le interruzioni. Abbiamo anche riscontrato, e ne siamo rimasti sorpresi, elevati livelli di fiducia tra i leader IT nelle capacità delle loro organizzazioni di gestire interruzioni IT ed attuare un ripristino dopo tali eventi.

Invitiamo a considerare i risultati come parametro di riferimento per la propria strategia di attenuazione del rischio IT. In aggiunta ai risultati del sondaggio, presentiamo una procedura in nove passi per tracciare un percorso verso la resilienza informatica.

Su The Progress Report, ho anche discusso i risultati con Ricardo Morales, CISO di Banorte, una delle maggiori banche commerciali messicane.

Come abbiamo ottenuto i dati

Abbiamo incaricato una società di ricerca terza di condurre un sondaggio online coinvolgendo 300 responsabili delle decisioni IT di grandi aziende (con oltre 1.000 dipendenti). Le risposte sono state raccolte da marzo ad aprile 2023.

Ripartizione dei settori d'industria:

→ 65% Nord America
→ 19% Regno Unito
→ 16% India

Ripartizione dei settori d'industria:

→ 18% Servizi finanziari
→ 17% Pubblica amministrazione
→ 17% Industria manifatturiera
→ 14% Telecomunicazioni
→ 14% Media
→ 20% Altro

L'autore

Kris Lovejoy è il Global Practice Leader di Kyndryl per la sicurezza e la resilienza.

Le organizzazioni si affidano all'IT per svolgere processi business-critical.

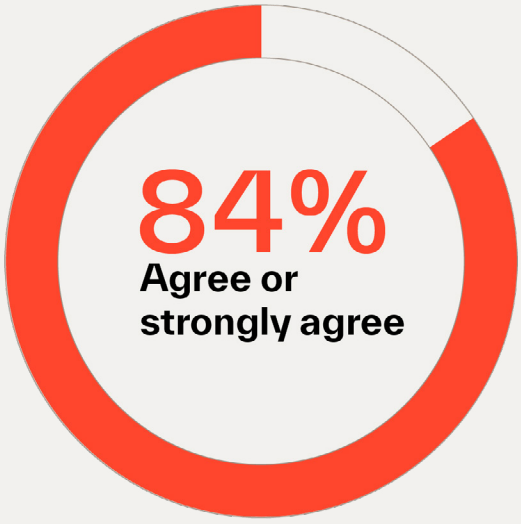
Per condurre la discussione sul rischio IT, abbiamo chiesto agli intervistati di suggerire in che misura la loro attività aziendale quotidiana faccia affidamento sull'IT.

L'84% è d'accordo o fortemente d'accordo sul fatto che la propria organizzazione faccia molto affidamento sugli asset IT per svolgere processi business-critical.

Il risultato non sorprende, considerati i commenti dilaganti e quotidiani sulla trasformazione digitale.

Forse, la cosa più sorprendente è che la risposta non sia stata ancora più enfatica.

D: Quanto siete d'accordo o in disaccordo con l'affermazione: "La mia organizzazione fa grande affidamento sulle risorse IT per gestire i processi aziendali critici".



La maggior parte delle organizzazioni ha subito interruzioni dei propri sistemi IT.

Abbiamo non solo confermato la criticità dei sistemi IT, ma anche che le interruzioni sono una conseguenza naturale. Il 92% degli intervistati ha affermato che la propria organizzazione ha subito un evento avverso negli ultimi due anni, che ha compromesso o interrotto i sistemi IT. Sì, gestire un'azienda significa assumersi il rischio IT.

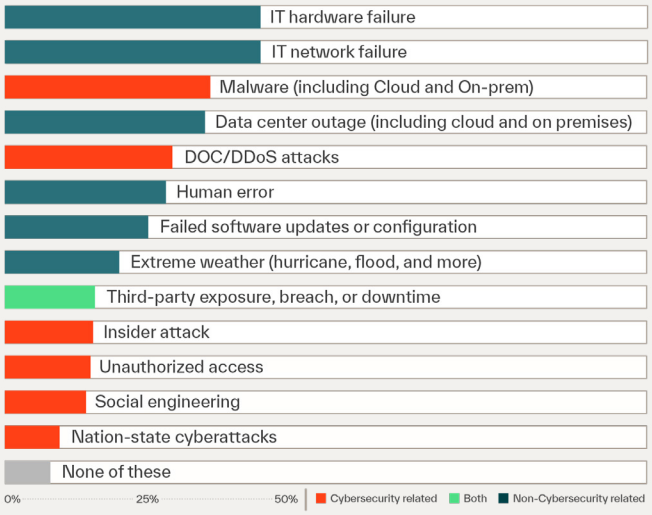
La maggior parte degli intervistati ha affermato di aver subito tre o quattro tipi differenti di eventi di interruzione. Sebbene gli attacchi informatici tendano a fare notizia, i risultati indicano che è giustificata un'apertura molto più ampia quando si discute e ci si occupa del rischio IT.

Mentre il 71% degli intervistati dichiara di aver vissuto un evento correlato alla sicurezza informatica, l'88% riferisce di aver subito un evento avverso non correlato alla sicurezza informatica (questi raggruppamenti non sono di tipo l'uno o l'altro). In effetti, tre dei primi cinque eventi avversi riscontrati non erano correlati alla sicurezza informatica:

- Malfunzionamento dell'hardware IT
- Malfunzionamento della rete IT
- Interruzione delle operazioni del data center

In particolare, anche l'errore umano rimane una delle cause principali di interruzione: è il n° 6 tra i 13 disservizi specifici di cui abbiamo chiesto ed è risultato costantemente tra i primi 3 per gli intervistati appartenenti al settore dei servizi finanziari.

D: Negli ultimi 24 mesi, uno dei seguenti eventi avversi ha compromesso o interrotto i vostri sistemi/dati informatici?



Le interruzioni dei sistemi IT hanno danneggiato marchi, provocato sanzioni e altro ancora.

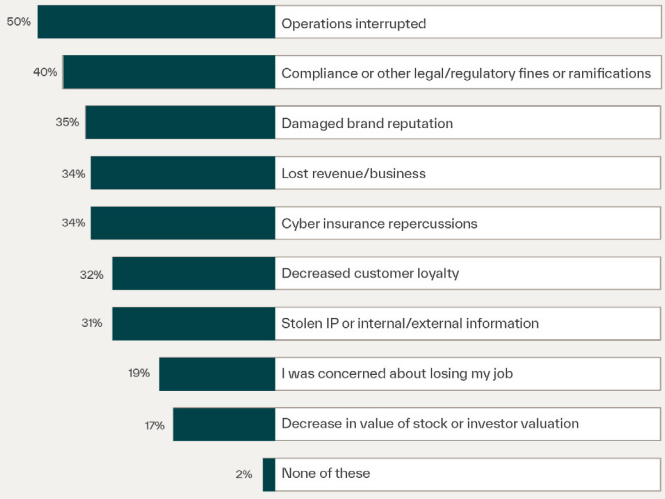
Basandosi sulla criticità dell'IT per le operazioni quotidiane, gli intervistati hanno classificato le interruzioni operative come l'impatto più comune sperimentato come conseguenza di eventi IT avversi.

La conformità o altre sanzioni o conseguenze legali o normative sono state indicate come il secondo impatto più sperimentato. Ciò è risultato particolarmente vero per gli intervistati appartenenti ai settori dei servizi finanziari, della pubblica amministrazione e dei media.

Non solo le interruzioni operative ed eventi legati alla categoria della conformità sono stati gli incidenti più sperimentati, ma gli intervistati hanno anche classificato queste due categorie di eventi come quelle con gli impatti più preoccupanti, nel caso in cui gli asset IT dovessero risultare non disponibili o compromessi in futuro. Le interruzioni dovute ad attacchi denial of service e le perdite di dati, ad esempio, possono portare a sanzioni costose.

Il 35% degli intervistati ha affermato che la reputazione del marchio della propria organizzazione è stata danneggiata come conseguenza delle interruzioni dell'IT. Questo risultato si è dimostrato particolarmente vero tra gli intervistati provenienti dalle organizzazioni dei media, il 63% dei quali ha notato tale impatto. Il ciclo delle notizie sempre attivo e l'attività dei clienti sui social media oggi rendono qualsiasi evento avverso più visibile che mai.

D: Quali dei seguenti impatti ha subito la sua organizzazione a causa di eventi avversi [negli ultimi 24 mesi]?



Quindi, cosa impedisce ai responsabili delle decisioni IT di giocare d'anticipo sui rischi IT?

Abbiamo anticipato che la carenza globale di competenze IT si classifica ai primi posti tra le attenuanti, ma non proprio al primo posto dell'elenco. La mancanza di capacità di ripristinare sistemi e dati da un backup crittografato e pulito è stata spesso rappresentata come una delle principali sfide che gli intervistati hanno dovuto affrontare nel gestire l'impatto degli eventi avversi. Lo riscontriamo spesso anche tra le organizzazioni che si informano sui nostri servizi. Li incoraggiamo a:

- → Investire nell'automazione e nell'orchestrazione dei processi di ripristio
- → Valutare e stabilire il modo migliore per ridurre l'errore umano nel ripristino a partire dai backup
- → Sottoporre a test i piani di risposta all'incidente, ripetutamente e spesso

A completare le prime tre sfide indicate dagli intervistati per quanto riguarda l'attenuazione del rischio erano incluse l'espansione dello spazio occupato dall'IT e la capacità di rimanere aggiornati sulle minacce emergenti. Al quarto posto si colloca la mancanza di personale IT qualificato.

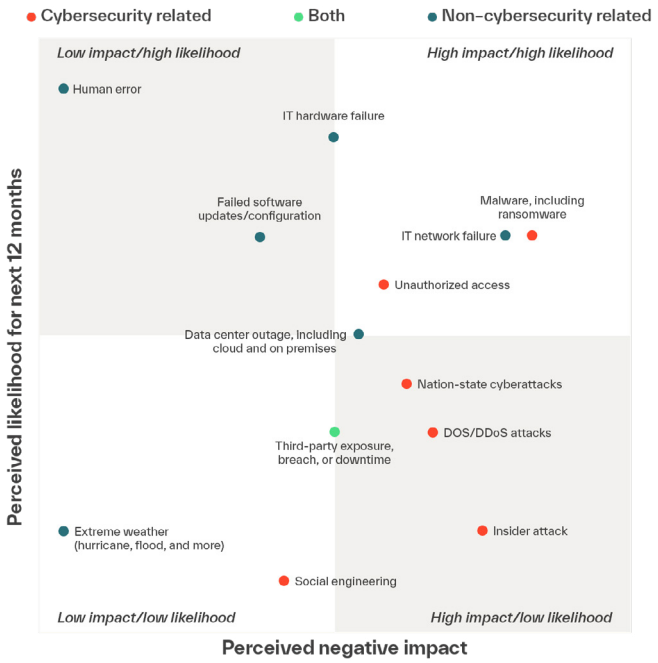
D: Quali sono le tre principali sfide che dovete affrontare nella gestione dell'impatto degli eventi avversi?

Guardando ai prossimi 12 mesi, gli eventi malware vengono percepiti come il rischio informatico con la massima probabilità di verificarsi e l'impatto più negativo.

Abbiamo chiesto agli intervistati di indicarci gli eventi avversi che si aspettano con maggiore probabilità nei prossimi 12 mesi, oltre al livello di impatto che questi eventi avrebbero sulle loro organizzazioni se dovessero verificarsi.

L'errore umano è stato considerato come l'evento con la massima probabilità di verificarsi, ma l'impatto previsto è inferiore rispetto alla maggior parte degli altri eventi. Il malware, peraltro, si è rivelato il rischio informatico maggiormente previsto e più minaccioso.

Considerato l'aumento del malware, in particolare del ransomware, il risultato non sorprende. In vista delle suddette sfide legate al ripristino dei dati a partire da backup crittografati e puliti, questo suggerisce anche un motivo di accresciuta attenzione. Indipendentemente dal fatto che la propria organizzazione sia o meno messa in difficoltà dai backup, una complicazione è rappresentata dal fatto che gli autori di attacchi ransomware prendono sempre più di mira i backup. In questi scenari, quando i backup sono stati compromessi, le organizzazioni non solo non possono ripristinare i sistemi, ma non possono nemmeno verificare la presenza di malware. Di conseguenza, il rischio e i potenziali impatti aumentano a dismisura.



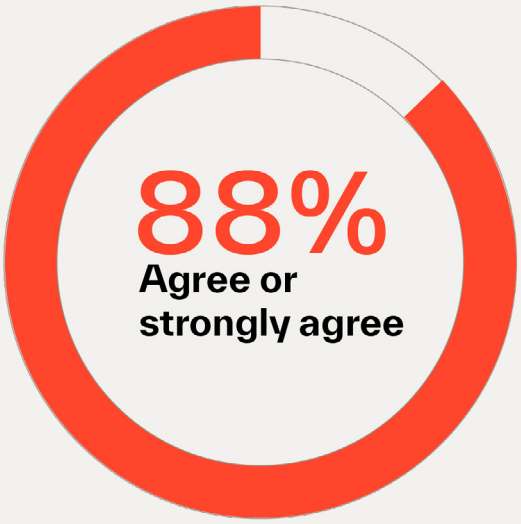
Si ritiene che anche un altro rischio con elevata probabilità e potenzialmente di grande impatto, ovvero l'accesso non autorizzato, abbia conseguenze negative significative. I principi dell'approccio zero-trust svolgeranno un ruolo costantemente importante nella gestione dell'accesso non autorizzato. Questi principi richiedono che le organizzazioni identifichino i loro asset di alto valore, determinino l'accesso privilegiato e utilizzino efficacemente tecnologie, quali l'autenticazione a più fattori, per la convalida.

Nonostante i rischi percepiti, i responsabili delle decisioni IT continuano ad essere fiduciosi.

In precedenza in questo report, abbiamo espresso sorpresa per la fiducia dimostrata dai responsabili delle decisioni IT, considerati gli eventi globali e le sfide rilevate. In effetti, l'88% degli intervistati ha concordato sul fatto che la propria organizzazione è adeguatamente preparata alla gestione e al ripristino di fronte a qualsiasi condizione avversa, attacco o compromissione che interrompa le operazioni degli asset IT dell'organizzazione.

Alla richiesta di confrontarsi con i peer, il 65% ha valutato la preparazione della propria organizzazione al verificarsi di eventi avversi superiore rispetto ad altre organizzazioni. Solo l'8% si considera almeno un po' indietro rispetto agli altri. L'alto livello di fiducia cattura particolarmente la nostra attenzione, considerato il già citato 92% che ha anche confermato che le proprie organizzazioni hanno subito eventi avversi. Il dualismo è quantomeno curioso, se non rappresenta addirittura una ragione per chiedersi se tale confidenza sia giustificata.

D: Quanto è d'accordo o in disaccordo? La mia organizzazione è ben preparata a gestire e a riprendersi da eventuali condizioni avverse, attacchi o compromissioni che compromettono le risorse IT della mia organizzazione.



9 passi per i leader IT per tracciare un percorso verso la resilienza informatica

Abbiamo intrapreso questo studio per mettere a confronto il modo in cui i responsabili delle decisioni IT percepiscono lo stato attuale del rischio IT e quali azioni, nell'ambito dei quattro pilastri della resilienza informatica, le loro organizzazioni intraprendono per attenuare tali rischi.

- → **Anticipare:** azioni per valutare e comprendere la posizione rispetto al rischio IT, per trovare un modo più efficace per attenuare le possibili minacce e orientarsi tra le potenziali normative.
- → **Proteggere:** azioni di rafforzamento delle difese degli asset IT per garantire una protezione continua da eventi avversi.
- → **Opporsi:** azioni per gestire le interruzioni e ridurne l'impatto.
- → **Ripristinare:** azioni per contribuire ad attenuare l'impatto dopo eventuali interruzioni e ripristinare rapidamente ambienti IT critici.

Gli intervistati hanno costantemente valutato le prestazioni delle loro organizzazioni come eccellenti, da qui i punteggi di alta confidenza. In media, considerando tutte le attività, il 75% degli intervistati ha valutato le prestazioni da molto buone a eccellenti. Una sfumatura che abbiamo riscontrato, è che gli intervistati che hanno riferito un forte sostegno da parte dei dirigenti per quanto riguarda gli investimenti nella sicurezza erano più propensi ad assegnare a se stessi voti alti per le attività correlate alla resilienza informatica.

Per aiutare ad ottenere questo sostegno, inoltre, presentiamo nove passi fondamentali per tracciare un percorso verso la resilienza informatica.

1 **Coinvolgere l'azienda fin dall'inizio.**

Le organizzazioni IT troppo spesso operano in isolamento, separate dagli altri settori dell'azienda. Il percorso più sicuro affinché una strategia di resilienza informatica abbia successo è rompere l'isolamento. Invitare al tavolo voci esterne all'IT e agganciare le conversazioni sulla resilienza informatica alla mission dell'organizzazione. Rendere questo argomento parte della cultura dell'organizzazione.

2 **Allinearsi sulla tolleranza al rischio.**

Un livello di tolleranza al rischio è spesso dettato dal settore d'industria. Ad esempio, il livello di tolleranza per un istituto finanziario estremamente regolamentato sarebbe probabilmente molto basso. Qualunque sia il livello, definire la tolleranza al rischio per la propria organizzazione e comunicarla ai team.

3 **Stabilire il proprio MVC (minimun viable company - livello di funzionamento minimo dell'azienda).**

Il livello di funzionamento minimo dell'azienda rappresenta le parti dell'organizzazione che sono fondamentali per supportare le operazioni e avanzare verso gli obiettivi di business. La strategia di resilienza informatica non dovrebbe solo individuare gli elementi critici, ma anche le tolleranze all'impatto per determinare la rapidità con cui i dati sottostanti per questi sistemi dovrebbero essere nuovamente online.

4 **Eseguire un inventario.**

Come dimostrato dai risultati del sondaggio, molte organizzazioni devono affrontare la sfida di uno spazio occupato dall'IT in continua espansione. Identificare e mappare gli asset IT fondamentali per il livello di funzionamento minimo dell'azienda. Questi asset avranno la massima priorità dal punto di vista della protezione e, nel caso peggiore, del ripristino a seguito di un evento avverso.

5 **Passare a un framework zero-trust.**

Consigliamo lo standard di negazione per impostazione predefinita per garantire che solo coloro che hanno bisogno di accedere ai sistemi possano ottenere tale accesso, mentre coloro che non ne hanno bisogno non possano farlo.

6 **Stabilire un piano di gestione della crisi.**

Qualche volta, gli eventi avversi sono inevitabili. (Esempio tipico: l'errore umano come causa più probabile di interruzioni). Definire ruoli e responsabilità nei team, stabilire un processo di comunicazione, documentare i processi e migliorare la trasparenza spesso aiuta a ridurre l'impatto di un evento avverso.

7 **Esercitarsi per un'interruzione.**

Troppo spesso i piani vengono creati, ma poi accantonati e raramente messi in pratica. Quando si verifica un evento avverso, un piano non sottoposto a test genera confusione e tempi di risposta lenti, inoltre l'impatto diventa più grave.

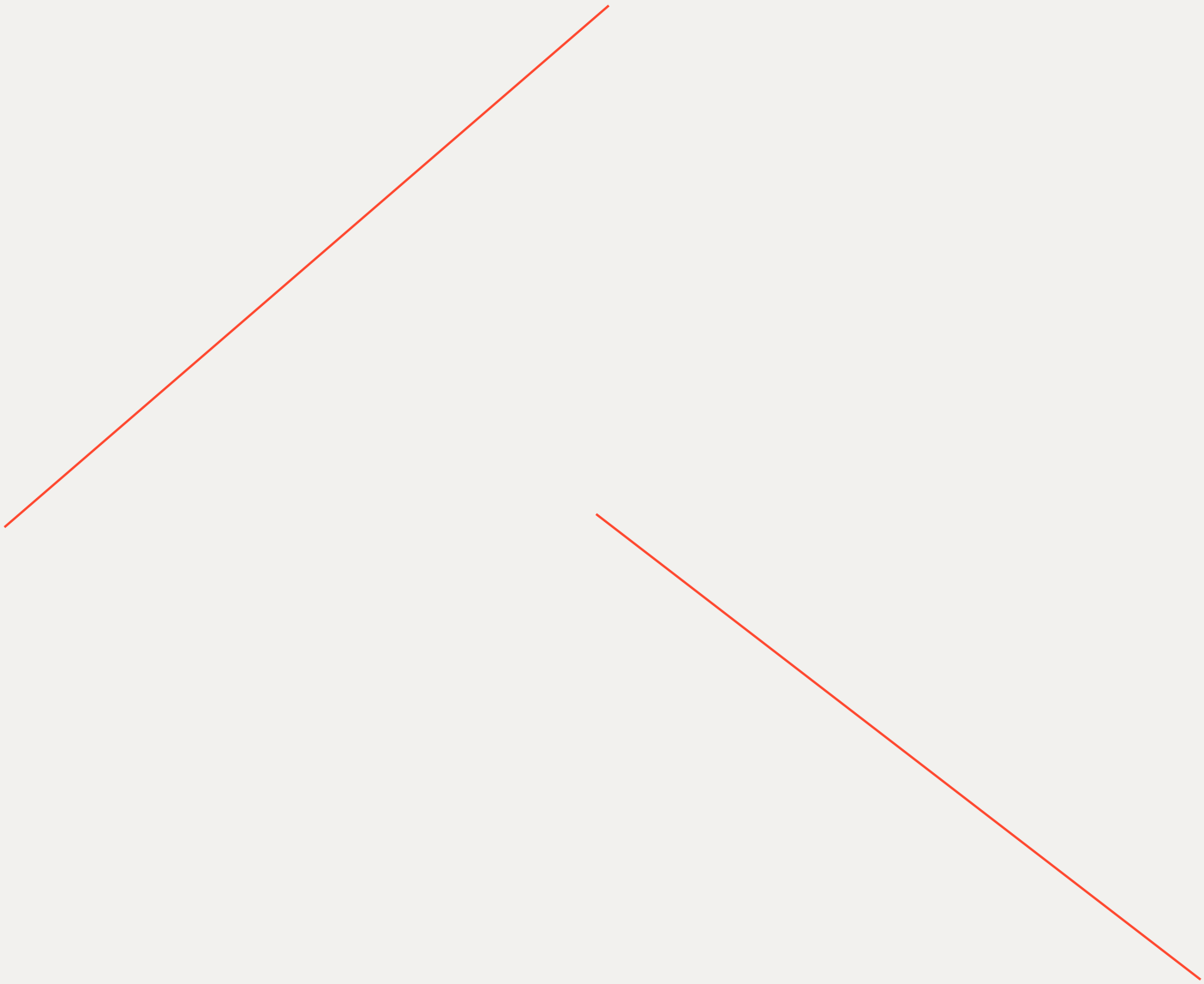
8 **Modernizzare continuamente la propria strategia di resilienza informatica.**

Le organizzazioni sono entità viventi. Gli obiettivi di business cambiano, il patrimonio IT diventa più complesso e le forze esterne (le normative, ad esempio) possono richiedere modifiche. Per garantire l'efficacia della strategia di resilienza informatica, questi passi devono diventare argomenti di una discussione continua.

9 **Creare consapevolezza a livello di consiglio di amministrazione.**

Concludiamo questo report sul sondaggio da dove abbiamo iniziato, richiamando l'attenzione sul fatto che la resilienza informatica è diventata un argomento di discussione a livello di consigli di amministrazione in tutto il mondo.

Tenere informato il consiglio di amministrazione sui rischi IT e sui piani per attenuare tali rischi può aiutare a promuovere l'allineamento organizzativo dall'alto verso il basso e fornire supporto per apportare le modifiche necessarie per garantire che i sistemi informatici possano rimanere operativi durante eventi avversi.



kyndryl