

Salve e benvenuti a questo modulo InCyT sulla resilienza. La resilienza sta ricevendo sempre più attenzione, poiché è diventato ovvio che si verifichino violazioni e che si materializzino eventi negativi che non ci si aspettava.

Quando si parla di continuità operativa e di resilienza, si pensa ai disastri naturali o alle grandi catastrofi come interruzioni di corrente, condizioni meteorologiche avverse, terremoti, inondazioni e così via.

Ma ci sono anche altre catastrofi, che io chiamo catastrofi silenziose, che possono minacciare l'azienda e le sue attività, compresa la perdita di personale chiave. Quindi, se persone importanti o un gruppo di persone lasciano l'azienda, può essere spesso difficile sostituirle e garantire la continuità delle operazioni aziendali. Inoltre, gli attacchi di insider e lo spionaggio industriale possono rappresentare una seria minaccia per le organizzazioni, così come la perdita di informazioni critiche per l'azienda, a causa di backup inadeguati o corrotti o di guasti hardware o software. La continuità operativa è quindi fondamentale per ogni azienda.

Richiediamo un approccio strutturato perché solo un approccio strutturato può garantire che la reazione a gravi interruzioni dell'incidente funzioni anche in condizioni di stress. Per trovare soluzioni e avere una risposta efficace, è necessario avere una comprensione cristallina del funzionamento dell'organizzazione e, una volta ottenuta, l'organizzazione e il suo marchio e la sua reputazione sono protetti. È stato dimostrato che le organizzazioni che gestiscono gli incidenti in modo efficace sono considerate più preziose di prima. È inoltre importante dimostrare la dovuta attenzione e la dovuta diligenza, poiché spesso i requisiti normativi e legali obbligano le organizzazioni a dotarsi di strategie di continuità operativa e di resilienza.

Ma pensiamo che la vostra organizzazione sia colpita da un grave disastro, ad esempio un'alluvione, un'interruzione di corrente o la perdita dell'IT. Cosa succederebbe se ciò accadesse? Quale sarebbe l'effetto sui clienti? Come si ripercuoterebbe il vostro profitto? Che ne sarebbe della salute e della sicurezza, dell'ambiente e così via? La continuità aziendale consiste nel porsi queste domande per individuare le attività importanti di un'organizzazione e trovare il modo di recuperare e continuare le funzioni aziendali più importanti e vitali per garantire la sopravvivenza dell'azienda.

Analizziamo un tipico incidente. Se si verifica un incidente, normalmente il livello di operatività diminuisce. Come si può notare, se non si adottano misure di continuità operativa, il livello di operatività si riduce ulteriormente, mentre se si adottano misure di continuità operativa, si è in grado di recuperare più rapidamente e di ridurre al minimo i danni.

Abbiamo già parlato molto di business continuity, ma credo sia importante anche definire cosa sia effettivamente la business continuity. Una buona fonte per la continuità aziendale è il Business Continuity Institute, che definisce la continuità aziendale come la capacità strategica e tecnica dell'organizzazione di pianificare e rispondere agli incidenti e alle interruzioni dell'attività al fine di continuare le operazioni aziendali a un livello accettabile predefinito. Anche lo standard ISO Business Continuity ha una definizione simile. Definisce la continuità operativa come la capacità dell'organizzazione di continuare a fornire prodotti e servizi a livelli accettabili e predefiniti in seguito a un incidente di disturbo.

La norma che descrive come un sistema di gestione della continuità operativa possa essere pianificato, implementato e migliorato nel tempo è la ISO 22301 e, come tutte le norme sui sistemi di gestione, segue il ciclo Plan-Do-Check-Act o Deming per renderlo integrabile con i sistemi di gestione della sicurezza delle informazioni o della qualità. Nelle diapositive che seguono, esamineremo più in dettaglio le parti importanti degli standard.

L'analisi dell'impatto sul business è il fondamento del processo BCM. In questa parte esamineremo nel dettaglio le attività di analisi dell'impatto sul business.

Come detto, è il lavoro di base per l'intero processo aziendale e differisce un po' dalle tipiche valutazioni del rischio e simili, ma ne parleremo più avanti. L'analisi dell'impatto sul business identifica le attività, i prodotti e i risultati principali ed esamina l'evoluzione dei danni nel tempo. Copre anche le dipendenze interne ed esterne ed è l'input principale per ogni strategia di recupero. La BIA è molto importante per essere sicuri di non sottovalutare o sovrastimare determinati tempi di recupero.

Ci sono diversi termini fondamentali che vorrei approfondire. Il primo è l'interruzione massima accettabile o il periodo massimo tollerabile di interruzione. È il momento in cui il danno diventa irreversibile. Quindi, se si raggiunge questo tempo, l'azienda sarà irreversibilmente danneggiata. Per questo motivo, quando si definisce questo tempo, bisogna essere sempre molto attenti e non bisogna dimenticare la stagionalità o la variabilità dell'anno finanziario che possono influenzare l'interruzione massima accettabile. Ad esempio, le vendite natalizie o i periodi di vacanza e così via. Il secondo termine che vorrei sottolineare è l'obiettivo del tempo di ripristino, ovvero il periodo di tempo successivo a un incidente in cui un prodotto o un'attività devono essere ripresi a un livello accettabile predefinito. Sebbene l'obiettivo del tempo di ripristino sia normalmente pianificato durante la fase di progettazione o di strategia di continuità operativa, le prime stime sono normalmente richieste anche durante l'analisi dell'impatto sul business. L'ultimo termine importante è l'obiettivo del punto di ripristino. Si tratta del punto in cui le informazioni devono essere ripristinate per consentire le operazioni aziendali. Evidenzia quindi la perdita massima di dati. Ad esempio, se l'obiettivo del punto di ripristino è di un giorno, il backup non deve essere più vecchio di 24 ore.

Diamo un'occhiata alla BIA. Se state pensando a un servizio, abbiamo diversi tipi di processi e, se si verifica un incidente, abbiamo gravi impatti.

Questi impatti possono essere raggruppati in diverse categorie, come quella finanziaria, ambientale, della salute, della sicurezza, legale, del marchio e molte altre ancora. Quindi, quello che stiamo cercando di capire è se si verifica un'interruzione, quanto velocemente si verificherebbe l'impatto in queste categorie.

Inoltre, stiamo cercando di capire da quale tipo di risorse dipendono i processi. Naturalmente, anche l'interruzione di una risorsa potrebbe essere un ostacolo per un determinato processo.

Approfondiamo il processo di BIA. Di solito si inizia dando la priorità ai prodotti e ai servizi. Quindi, il top management o l'alta dirigenza dà la priorità a quei servizi che sono i più vitali per l'organizzazione. Poi si analizzano i processi necessari per fornire un servizio o un prodotto. E questi processi vengono ovviamente classificati in base a quelli che sono necessari per realizzare i prodotti e i servizi vitali, anch'essi classificati in base a tale priorità. E poi si analizza ulteriormente per vedere quali sono le attività e le risorse critiche necessarie

per realizzare i processi e, in questo modo, si scopre da cosa dipendiamo. Naturalmente,

Questo viene fatto nella fase di analisi e consolidamento e alla fine presentiamo i risultati al top management per selezionare successivamente le strategie di continuità aziendale più appropriate.

Come potrebbe apparire un esempio di guida al colloquio? Sul lato sinistro, si può vedere una guida al colloquio di questo tipo, che da un lato cattura informazioni importanti sul processo e sui suoi requisiti. E dall'altro lato, in basso a sinistra, si può vedere questo danno nel tempo. Si tratta di una valutazione qualitativa con 4 diversi livelli e si può notare come i danni si manifestino nel tempo. Sul lato destro si può vedere una guida all'intervista per uno specifico sistema IT al fine di ottenere maggiori informazioni sui sistemi IT. Ci sono rischi noti, single point of failures, tempi di ripristino e così via.

È importante anche specificare la dipendenza tra i processi. Quindi, quale processo dipende da un altro processo e poi successivamente quale processo dipende da quale risorsa e quale risorsa dipende da quale risorsa. In questo modo possiamo verificare se i tempi di recupero sono validi per un determinato caso d'uso.

Continuiamo con le strategie di continuità aziendale.

Dopo aver effettuato l'analisi dell'impatto sul business e la valutazione dei rischi, siamo in grado di determinare le strategie per reagire ai disastri o alle interruzioni più gravi. Quindi, quello che stiamo cercando di fare è identificare gli obiettivi di tempo di ripristino. Naturalmente, questi obiettivi di tempo di ripristino devono essere più brevi dell'interruzione massima accettabile, ma bisogna tenere presente che gli obiettivi di tempo di ripristino più brevi sono più alti e normalmente i costi sono elevati, quindi è sempre così. Dobbiamo trovare un compromesso tra i costi e l'obiettivo di tempo di ripristino appropriato. Naturalmente si valutano anche le strategie esistenti. Quindi, se esistono strategie già esistenti che sono appropriate per i tempi di recupero analizzati, allora non dobbiamo fare nulla, ma per quelle in cui troviamo un divario, ovviamente, dobbiamo introdurre nuove strategie. Non appena vengono individuate delle strategie, queste devono essere approvate dalla direzione. E, naturalmente, devono essere previste risorse finanziarie e finanziarie per l'attuazione di tali strategie.

Ma quali potrebbero essere queste strategie? Per esempio, nel campo dei luoghi di lavoro, le strategie potrebbero essere quelle della distribuzione delle attività aziendali, per cui si distribuisce il lavoro in più sedi, oppure quelle dei luoghi di lavoro alternativi interni. Quindi, se si verifica un incidente, è possibile spostare i luoghi di lavoro in termini di personale. Potreste formare, ad esempio, dei sostituti attraverso corsi di formazione intersettoriali, in modo che imparino a sostituire personale importante. Potreste assumere o stipulare contratti per il personale tecnico da fornitori esterni. E naturalmente, una misura molto efficace è quella di avere un buon sistema di gestione delle conoscenze. Quindi, in qualche modo, catturare i compiti più importanti. Per quanto riguarda la tecnologia dell'informazione, si potrebbe procedere a licenziamenti. Oppure che si stipulino degli accordi sul lato IT, ad esempio, cold site, warm site o hot site. Oppure limitare le operazioni IT in caso di interruzione. Potrebbero esserci anche delle alternative al cloud o delle strategie cloud da adottare in caso di incidente. E, naturalmente, ci potrebbero essere anche cose a livello di componenti, ad esempio lo stoccaggio di parti di ricambio o di componenti o la stipula di accordi con i fornitori che garantiscano l'ottenimento di parti di ricambio o di componenti in un determinato periodo di tempo a seguito di un incidente.

La fase successiva è dedicata alle procedure di continuità operativa.

E una parte importante di questo sono i piani di continuità aziendale. I piani di continuità aziendale sono il vostro manuale di comportamento in caso di imprevisti e la prima cosa che i piani di continuità aziendale devono avere è un processo di attivazione. Quindi, bisogna avere un processo chiaro su quando attivare un determinato piano. Naturalmente, devono essere chiari anche i ruoli e le responsabilità e le attività di risposta e recupero devono essere descritte in ogni piano e, ovviamente, anche la strategia di comunicazione, sia interna che esterna. Nel complesso, si tratta di un piano che copre le soluzioni da adottare nel caso di un evento negativo.

Tenete presente che è destinato a essere utilizzato in situazioni di alta pressione, quindi quando le persone sono sotto stress, non vogliono leggere molto, quindi deve essere facile da usare. Dovrebbe essere abbastanza veloce da capire quali sono le parti importanti del piano, quindi dovrebbe essere dotato di liste di controllo, che sono spesso rappresentate nei piani di continuità operativa, in modo che le persone possano avere una visione d'insieme molto rapida di quale sia il prossimo compito da svolgere. Quindi, le caratteristiche di un piano di continuità di base efficace includono che il piano deve essere diretto, quindi chiaro, orientato all'azione e basato sul tempo, in modo da essere in grado di valutare rapidamente le informazioni rilevanti di cui si ha bisogno. Deve essere adattabile: quando si parla di continuità aziendale, non è possibile pianificare ogni singolo evento negativo a cui si pensa. Quindi, il piano deve essere adatto a un'ampia gamma di eventi dirompenti, compresi quelli che forse un'organizzazione non si aspetta. Pensate alla pandemia di Corona, un evento che la maggior parte delle organizzazioni non si aspettava, ma chi aveva un piano di continuità operativa è riuscito in qualche modo a farvi fronte, anche se non era esattamente previsto dal piano. Il piano deve essere anche conciso, quindi deve contenere solo le informazioni utili in caso di incidente. Ovviamente ha senso documentare molto e avere una documentazione per tutti i sistemi e così via, ma all'interno del piano dovrebbero esserci dei riferimenti cartacei, ma dovrebbero comunque esserci solo le cose necessarie in caso di incidente. E, naturalmente, deve essere pertinente, il che significa che deve essere attuale e aggiornato, il che rappresenta una sfida. I sistemi cambiano spesso e cose del genere, così come i processi e le procedure. Ma è fondamentale avere un piano di continuità aziendale aggiornato.

Quali sono gli elementi fondamentali di ogni piano di continuità aziendale? Naturalmente, all'inizio si deve avere una sorta di scopo e di portata, in modo da sapere a cosa serve il piano e qual è il suo obiettivo; inoltre, è importante dichiarare l'ipotesi in cui il piano può essere utilizzato. Ad esempio, si presuppone che un'altra filiale sia ancora operativa o qualcosa del genere. Naturalmente, se l'ipotesi non è più vera nella realtà, il piano potrebbe non essere appropriato. Naturalmente, dovrebbe esistere una struttura di gestione degli incidenti, ovvero la struttura in cui le squadre di emergenza e le squadre di gestione degli incidenti lavorano insieme. Normalmente c'è una struttura a livelli liberi che va dalla gestione superiore o struttura di primo livello a una struttura di coordinamento e poi sullo strato inferiore ci sono le squadre di recupero, le squadre operative, che di solito sono prese in prestito dai servizi di emergenza. Per ogni squadra di intervento e per i membri della squadra di intervento ci sono ovviamente delle responsabilità, che dovrebbero essere indicate nel piano anche per quanto riguarda la mobilitazione e l'allerta della squadra. Quindi, come si forma una squadra durante un incidente e in quali circostanze il piano può essere attivato? È importante concordare una sorta di punto di decisione quando le procedure di emergenza devono essere attivate e tali criteri devono essere chiariti in modo oggettivo, perché altrimenti è piuttosto difficile sapere quando attivare o meno un piano. Se ci si basa solo sulle stime, è molto difficile stabilire se attivare o meno un piano.

Naturalmente, i piani possono anche avere

l'invocazione di modalità di recupero e, naturalmente, anche i dati di contatto, che di solito sono indipendenti e vengono modificati molto spesso, dato che i dati di contatto potrebbero cambiare molto spesso.

Ogni piano è valido solo se viene testato.

I test sono quindi fondamentali quando si parla di resilienza della continuità aziendale. Da un lato, si migliora la consapevolezza. Si valuta anche l'adeguatezza delle capacità sviluppate e se l'ubicazione delle risorse funziona, se le strutture di comunicazione funzionano. Inoltre, l'esecuzione di diversi tipi di esercitazioni e test aiuta davvero a migliorare le procedure. Ad ogni esercitazione o test, scopriremo nuovi modi per migliorare la risposta. E naturalmente, più ci si esercita, più si ha fiducia nella propria reazione durante un incidente. Quindi, le prove e le esercitazioni sono davvero fondamentali.

Ci sono molti tipi diversi di esercitazioni e test che si possono fare, da quelli basati sulla discussione a quelli basati sulle operazioni, in cui si fa davvero qualcosa come il ripristino di un sistema e così via. Esempi di metodi di esercitazione basati sulla discussione sono il desk check, che consiste nell'esaminare un piano di continuità operativa, ad esempio per un servizio o un reparto, e verificare se le informazioni sono aggiornate. Un po' più complesso è un work through in cui ci si siede insieme e si discute lo scenario con diversi tipi di unità organizzative per verificare se i piani, il piano, l'interazione funzionano. I workshop e le esercitazioni su tavolo sono più che altro tentativi di risolvere realmente uno scenario in un certo lasso di tempo e i giochi basati sulla discussione vanno in una direzione simile.

Questa era una panoramica molto breve sulla gestione della continuità operativa.

Spero che abbiate imparato molto e se avete domande, non esitate a contattarci e vi auguro una buona giornata.