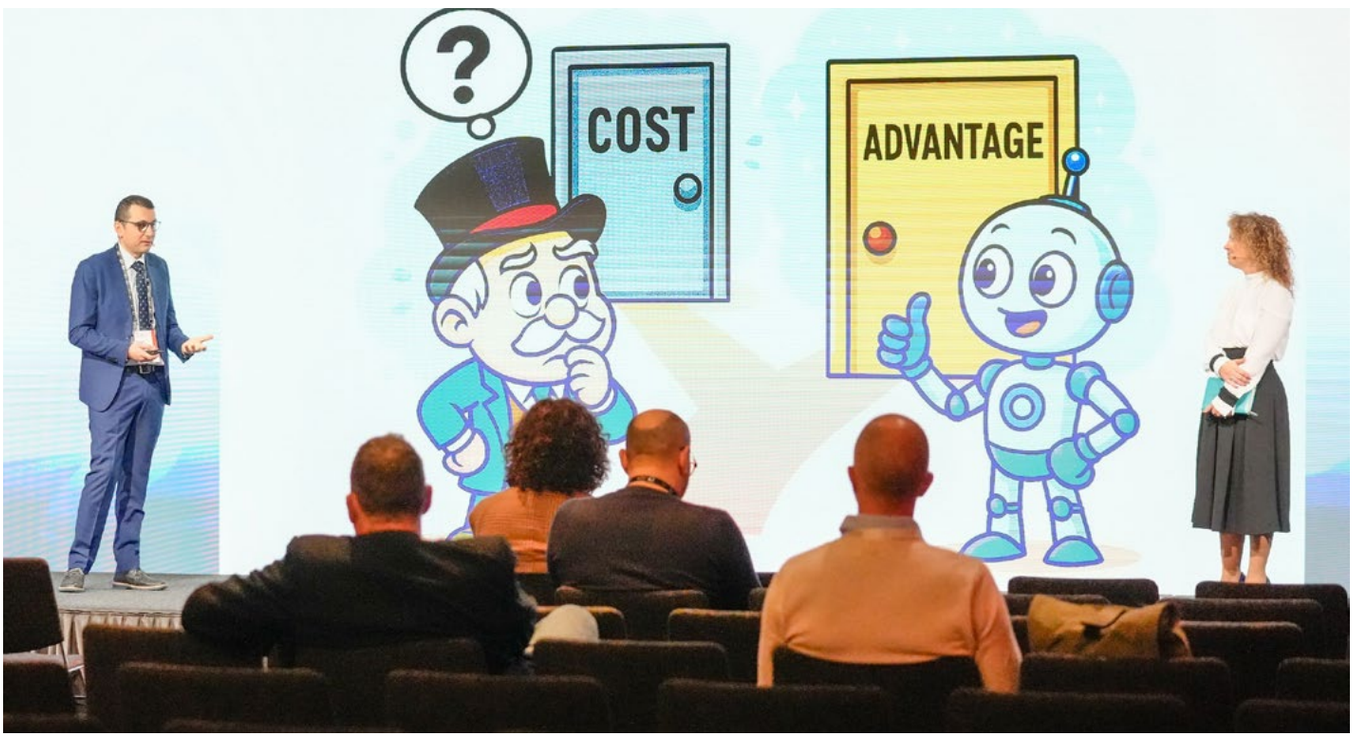
Come può la cybersecurity parlare la lingua dei soldi?

Migliorare la comunicazione tra i diversi reparti aziendali e valorizzare la cybersecurity agli occhi del cliente e dei dipendenti, lavorando in sinergia: due sfide del futuro su cui si confrontano Lilia Cucchiaro, Head of Customer Care & Digital Transformation Controlling di SCM Group e Pierpaolo Romano, Chief Information Security Officer di Italo.

di Riccardo Russo



Far crescere il proprio valore è uno dei principali obiettivi di un'azienda. La sicurezza informatica, però, non crea nuovo valore, protegge quello esistente. Genera un ROI inverso: non produce denaro, ma impedisce che venga perso. Il denaro risparmiato, però, non sempre brilla come quello guadagnato. Ciò che non accade – multe, violazioni o fughe di clienti – è difficile da visualizzare o da celebrare. Una via per farlo emergere può essere quella di convertirlo in cifre. Nel linguaggio della finanza, il rischio non è più una vaga possibilità, ma una perdita concreta sul fatturato in caso di violazioni, di multe previste dal GDPR e costi per la ricostruzione della reputazione. Una volta che questi dati sono sul tavolo, fingere di non vedere non è essere cauti: è una scelta consapevole di restare scoperti.

La cybersecurity non è un ostacolo che frena l'innovazione, ma un modo per evitare di bruciare soldi domani. È su questo piano che Pierpaolo Romano – Chief Information Security Officer di Italo – riesce effettivamente a farsi capire dal suo CFO. Lilia Cucchiaro – Head of Customer Care & Digital Transformation Controlling di SCM Group – dal canto suo, batte il tasto della comunicazione: *«CISO e CFO devono saper parlare la stessa lingua, perché, al netto di ruoli diversi,* siamo professionisti. Quando il CISO mi parla, devo capire cosa mi dice. Allo stesso modo, quando dico al CISO che il ritorno d'investimento non c'è, deve capire di cosa sto parlando».

Come vendere la cybersecurity

La cybersecurity è un servizio difficile da vendere al cliente, perché non è percepibile: non suona, non lampeggia, non accelera il lavoro delle macchine, semplicemente evita che si fermino. Per renderla rilevante, e vendibile, bisogna spostarla dal piano dell'oggetto a quello della percezione. Cucchiaro spiega come la sua azienda lavori in questo senso: *«I nostri macchinari industriali sono connessi al database del cliente, il che ci permette di effettuare manutenzioni preventive e di segnalare eventuali problemi. Tuttavia il cliente potrebbe domandarsi: "mi fido a lasciar entrare qualcuno nella mia rete"? Noi dunque, oltre a garantire il corretto funzionamento della macchina, assicuriamo la sicurezza della rete a cui si connette e la protezione del suo dato fino all'ultimo miglio, ovvero fino all'utente finale».* In questo modo la cybersecurity aumenta la percezione di affidabilità dell'azienda agli occhi del cliente e non appare più come un mero costo.

Per un CISO, la cybersecurity non è solo un servizio da rendere percepibile agli occhi del cliente, ma anche una cultura da instaurare nell'ambiente di lavoro attraverso specifiche linee guida e comportamenti: *«Insieme ai corsi di e-learning che eroghiamo* – sottolinea Romano – *stiamo proponendo anche formazioni in presenza con un professore stimato del settore. Oltre a questo tipo di formazione, però, eroghiamo periodicamente delle infografiche, ossia delle pillole-guida: come formulare una password efficace, come interagire con la mail…».* Il corso di e-learning, da solo, non basta. La vera consapevolezza del rischio digitale nasce dalla relazione con le altre persone, da storie che colpiscono l'immaginazione. È di questa opinione anche Cucchiaro: *«Seguo i miei corsi in e-learning, poi incontro molti colleghi che mi dicono: "Ah, che noia!". Allora ho iniziato a parlarne anche in altri contesti, magari davanti alla macchinetta del caffè o a pranzo: hai letto di quel ragazzo che è stato hackerato?».*

Questa condotta parte direttamente dagli impiegati. Per chi lavora in azienda la cybersecurity deve essere interiorizzata e occupare uno spazio piccolo ma importante, non essere relegata a un semplice click su "modulo completato". Il lato umano resta fondamentale nella condivisione delle esperienze formative.

Wellbeing come infrastruttura invisibile

Il fattore umano è anche un elemento intangibile che alleggerisce la pressione negli uffici. Le persone devono essere aggiornate e attente, ma se lavorano in apnea, l'errore diventa più probabile. Per Romano, il benessere dei colleghi è un fattore cruciale: *«Il wellbeing è sempre stata una mia missione, perché sono convinto che un collaboratore che sta bene e lavora in un contesto rilassato possa dare il meglio di sé. Per creare benessere nel team non basta distribuire compiti: bisogna affiancare le persone, farle sentire tutelate, capire in quale perimetro possono esprimersi al meglio».*

La palla passa dunque al team: chi lavora non è solo destinatario del benessere, ma ne è anche corresponsabile. Ciò significa non lasciare che le difficoltà sedimentino in silenzio, ma provare, per quanto possibile, a mantenere un clima leggero e affrontare i problemi insieme: sedersi in gruppo, con un foglio di carta, una matita e dei dubbi da esternare può far crollare in pochi minuti il castello di pensieri che ci si era costruito in testa. Conclude Cucchiaro: *«Nel mio ufficio capita che gli altri siano tutti, come dico io, con la testa china sul fatturato. Cerco sempre di essere simpatica, anche perché passiamo dalle otto alle dieci ore insieme. Il mio team è cambiato da pochissimo: ora lavoro con ragazzi tutti molto giovani. Sono andata a comprare delle agendine e le abbiamo ricamate insieme: abbiamo inciso davanti Welcome, con nome e cognome. È una cosa da poco, ma è un tentativo di portare serenità e leggerezza».*

Se proteggersi dai rischi informatici può essere più importante che risparmiare denaro, il benessere delle persone è ciò su cui tutto si regge, ed è la cosa che conta di più.