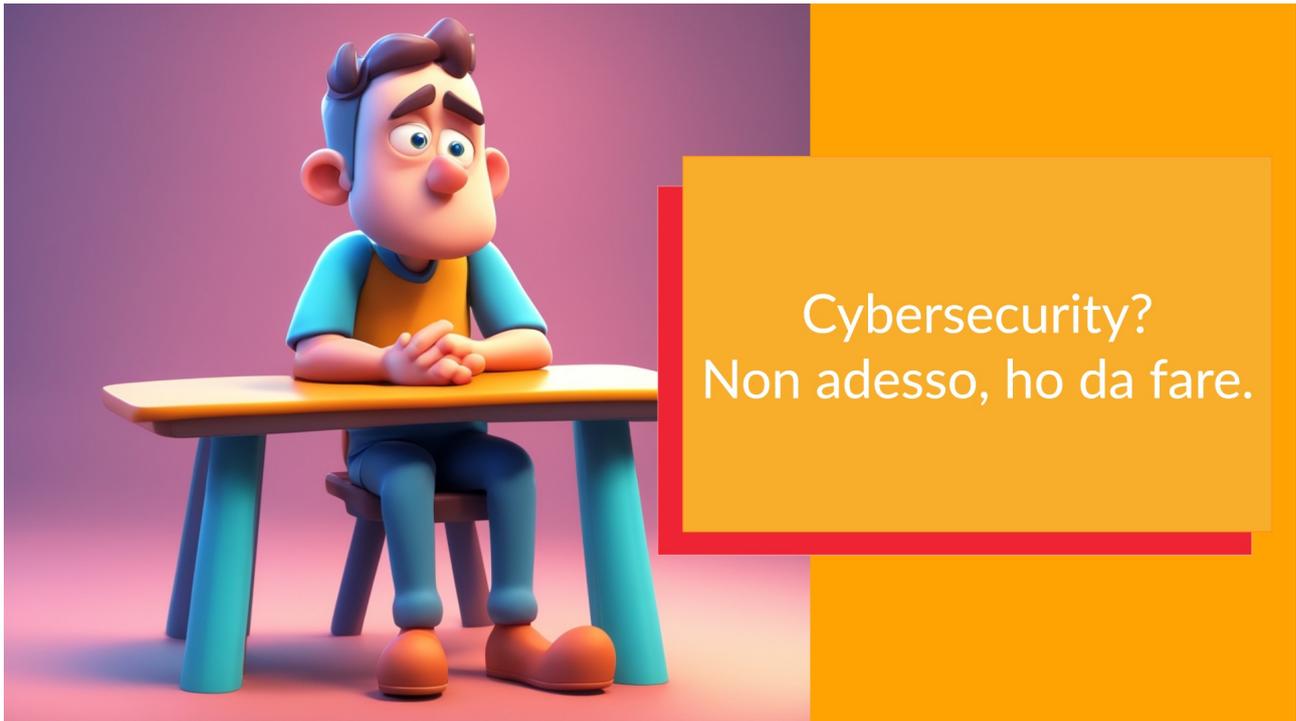




**Nessun problema può essere risolto congelandolo.  
(W. Churchill)**



La frase nell'immagine è una di quelle che spesso si ricevono parlando della sicurezza informatica.

Così come altre frasi molto simili:

“Non ne ho bisogno. Grazie.”

“Sono già a posto. Grazie.”

“È troppo costoso. Grazie.”

A volte al “grazie” viene aggiunto un:

“Me ne hanno parlato in molti, ma per ora ho altre priorità.”

Ognuna di queste risposte si basa su alcuni presupposti:

- che le aziende siano immuni agli attacchi informatici.  
**In realtà**, nessuna azienda è completamente al sicuro e anche le aziende più grandi e strutturate, sono state vittime di attacchi informatici.
- che le aziende siano già sufficientemente protette da altre misure di sicurezza, come l'aggiornamento dei sistemi operativi o l'utilizzo di firewall.  
**In realtà**, queste misure di sicurezza non sono sufficienti a proteggere le aziende da attacchi informatici sofisticati.
- che l'implementazione di soluzioni di sicurezza informatica sia troppo costosa per le aziende.  
**In realtà**, i costi in sicurezza informatica sono un investimento necessario per proteggere l'attività aziendale e i dati sensibili.

Argomentare in questi modi, da parte degli addetti alla sicurezza, è un rischio, che oltretutto non dipende dalle dimensioni aziendali; infatti gli attacchi informatici sono una minaccia sempre più frequente e pericolosa per le aziende di qualsiasi dimensione.

I rischi associati alla mancata implementazione di soluzioni di sicurezza informatica sono molteplici e possono avere un impatto significativo:

- Rischi economici;
- Interruzioni delle attività aziendali;
- Perdita di dati sensibili con conseguenti effetti legali;
- Conseguenze sulla reputazione dell'azienda.



*Questo documento contiene informazioni che IPnext s.r.l. considera confidenziali, proprietarie e significative per la tutela della propria attività. E' vietata la copia, la riproduzione, la distribuzione dei contenuti. - © Tutti i diritti sono riservati*



Questi motivi devono spingere i responsabili aziendali a domandarsi:

- “**Veramente** non ne ho bisogno? Ho calcolato quanto potrebbe costarmi un’interruzione della attività lavorativa per queste cause?”
- “**Sono assolutamente certo** che le soluzioni che adotto siano efficaci e soprattutto in grado di proteggere, anche rispetto alle rapide evoluzioni dei cyber attacchi?”
- “Ma davvero è troppo costoso? **Ho valutato** che non si tratta di costi, ma di investimenti che oltre alla sicurezza portano benefici alla mia azienda?”

L’infrastruttura informatica è senza dubbio sempre più centrale in un’azienda, ma è anche molto sensibile ed esposta all’esterno.

Valutarne la difesa, o verificare l’effettiva efficienza di quella presente, sono argomenti di cui ogni responsabile aziendale della stessa, deve farsi carico.

**IPnext** può collaborare con il personale tecnico, interno od esterno, delle aziende, per valutare le specifiche esigenze; analizzare l’eventuale infrastruttura esistente, e consigliare le soluzioni più adatte e che soprattutto possano adeguarsi al sempre più rapido evolversi del “**cyber-bad-world**”.

---

## **IPnext**

*Siamo partner tecnologici di molte imprese italiane.*

*Insieme a loro progettiamo e gestiamo le soluzioni ICT più evolute, per continuare a crescere insieme.*

- [IPnext](#) sito Web
- [IPnext](#) documentazione & soluzioni
- [IPnext LinkedIn](#)
- [IPnext Newsletter](#) “Verba Volant”

---

#CyberSecurity #IPnext #PaloAlto #AristaNetworks

Questo documento contiene informazioni che IPnext s.r.l. considera confidenziali, proprietarie e significative per la tutela della propria attività. E' vietata la copia, la riproduzione, la distribuzione dei contenuti. - © Tutti i diritti sono riservati

---

IPnext s.r.l. Viale Lucania 3 20139 Milano | +39.02.2563154 | <http://www.ipnext.it> | [info@ipnext.it](mailto:info@ipnext.it)