SOPHOS

IL COSTO UMANO DELLA VIGILANZA: AFFRONTARE IL BURNOUT DA CYBERSECURITY NEL 2025

Whitepaper Sophos. Agosto 2025

Introduzione

Il panorama della cybersecurity viene segnato sempre più pesantemente dalla pressione incessante di minacce informatiche sofisticate, tra le quali il ransomware. In un simile contensto, caratterizzato dalla presenza dilagante di minacce, i team IT e di sicurezza sono sempre più sotto pressione e questo porta a una sfida molto problematica, la cui diffusione sembra inarrestabile: lo stress e il burnout da cybersecurity.

Questo report valuta l'impatto che questa pressione ha sui team aziendali, traendo spunto dai dati emersi da nuove ricerche volte a identificare le principali cause scatenanti e le conseguenze del burnout, evidenziando in ultima analisi come questi problemi estremamente critici possano essere mitigati mediante l'uso di soluzioni strategiche.

Un sondaggio vendor-agnostic ha raccolto dati coinvolgendo 5.000 professionisti IT/di cybersecurity in 17 paesi diversi. Il sondaggio è stato realizzato nel corso del primo trimestre del 2025, chiedendo ai partecipanti di riflettere sulle loro esperienze nel corso dei 12 mesi precedenti.

Capire lo stress e il burnout da cybersecurity

Lo **stress da cybersecurity** è caratterizzato1 da uno stato di esaurimento mentale ed emotivo, spesso dovuto a una vigilanza costante, a un numero eccessivo di alert e alla responsabilità di dover difendere i sistemi da minacce informatiche in continua evoluzione. Rappresenta lo stress cognitivo ed emotivo provato dai professionisti che lavorano in questo settore estremamente esigente.

Il **burnout**, una sindrome psicologica più generalizzata, comprende esaurimento emotivo, cinismo e un inferiore senso di realizzazione personale. Si osserva spesso come conseguenza dello stress cronico sul posto di lavoro. Nell'ambito della cybersecurity, lo stress può essere considerato come una manifestazione diretta o uno dei principali fattori determinanti del burnout in senso lato.

Il **burnout da cybersecurity** è una manifestazione specifica di questa teoria più generale del burnout, esclusivamente nel contesto della cybersecurity. Comprende l'esaurimento mentale, fisico ed emotivo causato da un'eccessiva o prolungata esposizione agli stress tipici delle mansioni di cybersecurity.

I professionisti che lavorano in questo campo devono affrontare pretese cognitive ed emotive uniche nel loro genere, tra cui la necessità di gestire avvisi di sicurezza continui, l'esigenza di garantire il rispetto della conformità a normative molto rigide, nonché il dovere di coordinare una risposta tempestiva per le minacce informatiche emergenti.

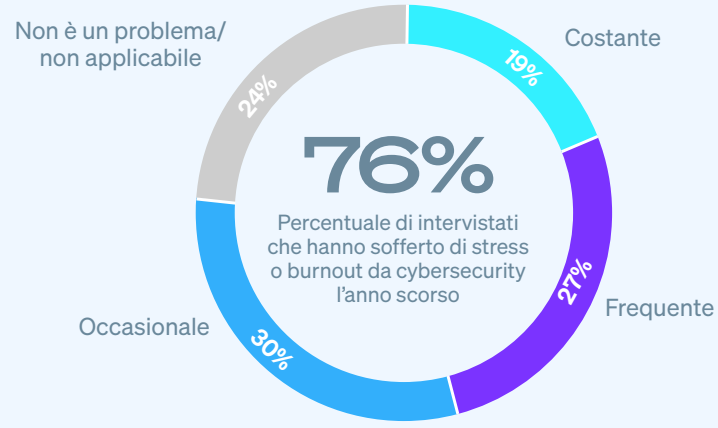
Questa esposizione continua ad attività impegnative e stressanti e la necessità di una risposta rapida e accurata agli incidenti sono fattori fondamentali che amplificano il rischio di stress e burnout tra il personale di cybersecurity.

Pressioni incessanti e ripercussioni estese

Esperienze di burnout

Le pressioni incessanti sui professionisti di cybersecurity vengono evidenziate dall'impatto sui team di IT e cybersecurity negli ultimi 12 mesi.

Alla domanda se avessero vissuto esperienze personali di stress o burnout da cybersecurity, il 76% degli intervistati ha indicato di averlo sperimentato in prima persona l'anno scorso. Analizzando i dati in maniera più approfondita, si osserva che il 19% dei partecipanti lo ha segnalato come un problema "constante", il 27% come un problema "frequente" e il 30% come un problema "occasionale".



Hai sofferto di stress o burnout da cybersecurity l'anno scorso? n=5.000

Dai dati emerge che il burnout è un problema dilagante nelle organizzazioni di tutte le dimensioni: ha sofferto di burnout il 76% degli intervistati in aziende con 100-1.000 dipendenti, il 77% in aziende con 1.001-3.000 dipendenti e il 75% in aziende con 3.001-5.000 dipendenti.

La cosa più preoccupante è che il problema non fa che peggiorare:
nel 2024 il 69% dei partecipanti al sondaggio dichiara di aver sperimentato più stress e burnout rispetto al 2023.

[1] Digital detox: l'impatto della stanchezza da cybersicurezza sulla produttività e sul benessere mentale dei dipendenti

Le conseguenze del burnout

Non sorprende affatto che il burnout abbia un impatto negativo sulle persone che lo subiscono, con quasi la metà (46%) degli intervistati che indica di aver sperimentato un'ansia accentuata a causa di attacchi informatici o violazioni; quattro partecipanti al sondaggio su dieci (39%) ammettono di aver notato un calo della produttività sul lavoro; infine un terzo (33%) sostiene di avere meno motivazione al lavoro.

Conseguenze dello stress e del burnout da cybersecurity

L'impatto del burnout	Media (n=3.803)	Livello di burnout sofferto		
		Problema costante (n=944)	Problema frequente (n=1.357)	Problema occasionale (n=1.502)
Ha sperimentato un'ansia accentuata a causa di attacchi informatici o violazioni	**46%**	47%	45%	46%
Calo della produttività sul lavoro	**39%**	36%	36%	43%
Meno motivazione al lavoro	**33%**	34%	33%	34%
Ha avuto bisogno di prendersi un periodo di pausa dal lavoro	**29%**	31%	28%	28%
Ha pensato di cambiare carriera/ruolo	**23%**	29%	25%	17%
Ha pensato di rassegnare le dimissioni dal proprio lavoro	**22%**	28%	25%	16%

Quali sono state le conseguenze personali (se presenti) dello stress o del burnout da cybersecurity? Intervistati che hanno dichiarato di aver sofferto di burnout nei 12 mesi precedenti. Base di partecipanti indicata nel grafico.

Queste statistiche mettono in evidenza una difficoltà seria e molto diffusa, che pregiudica direttamente l'efficacia e la sostenibilità delle difese di sicurezza.

Le principali cause delle pressioni

La natura estremamente impegnativa delle moderne difese informatiche, accentuata dal ritmo incessante dei cyberattacchi, contribuisce in maniera significativa al burnout. Tra tutti i partecipanti che hanno sofferto stress o burnout da cybersecurity, i cambiamenti costanti di tecnologie/soluzioni di difesa informatica sono stati il principale fattore determinante (38%). Per chi ha risposto che il burnout è un problema "costante", la natura stessa del lavoro di un professionista di cybersecurity (ovvero mansioni di routine intervallate da attività mirate) è risultata la causa più comune, indicata dal 40% degli intervistati.

I fattori che contribuiscono allo stress e al burnout da cybersecurity

Cause di burnout	Media (n=3.803)	Livello di burnout sofferto		
		Problema costante (n=944)	Problema frequente (n=1.357)	Problema occasionale (n=1.502)
Cambiamenti costanti di tecnologie/soluzioni	**38%**	36%	37%	41%
La natura stessa del lavoro di un professionista di cybersecurity (mansioni di routine intervallate da attività mirate)	**37%**	40%	36%	36%
Evoluzione continua delle minacce	**34%**	31%	31%	39%
Esigenza di copertura 24/7	**32%**	30%	32%	33%
Pressioni dovute ai continui cambiamenti delle normative e degli obblighi legali	**32%**	34%	34%	29%
Priorità che cambiano continuamente	**30%**	28%	29%	32%
Pressioni del consiglio di amministrazione e/o della direzione esecutiva	**30%**	29%	30%	30%
Carenza di personale qualificato	**27%**	24%	26%	29%
Limitazioni del budget (personale escluso)	**26%**	27%	28%	24%
Nessun accesso al supporto di esperti esterni	**26%**	30%	25%	23%
Elevato volume di avvisi	**25%**	24%	26%	25%

Quali fattori sono stati la causa dello stress o del burnout da cybersecurity che hai sofferto? Intervistati che hanno dichiarato di aver sofferto di burnout nei 12 mesi precedenti. Base di partecipanti indicata nel grafico.

In media, gli intervistati hanno indicato tre fattori diversi che hanno contribuito al loro burnout, il che evidenzia le molteplici pressioni affrontate dai team IT.

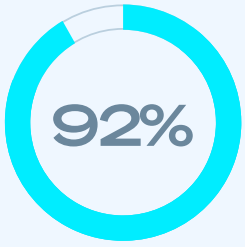
Impatto individuale e sull'organizzazione

Trascurare il burnout implica una serie di effetti negativi concatenati, che influiscono sia sul benessere individuale dei professionisti di sicurezza, che sulla resilienza complessiva dell'organizzazione.

- **Impatto individuale:** i professionisti soffrono alti livelli di stress, ansia, insoddisfazione sul lavoro ed effetti negativi sulla loro salute mentale e fisica. Anche le relazioni personali possono essere messe a dura prova e questo a sua volta può portare a un elevato turnover dei dipendenti.
- **Impatto sull'organizzazione:**
  - Maggiore vulnerabilità: quando sono allo stremo, i team sono più propensi a commettere errori e sviste che possono potenzialmente causare lacune di sicurezza critiche e un maggiore rischio di violazione dei sistemi.
  - Minore efficienza: il burnout incide negativamente sulla concentrazione, sul processo decisionale e sulla produttività, compromettendo la capacità del team di difendersi dalle minacce più avanzate.
  - Fuga di talenti: gli alti tassi di stress associati a questo lavoro contribuiscono alla perdita di professionisti qualificati, aggravando la già elevata carenza di personale di cybersecurity.
  - Disagi operativi: quando il profilo di sicurezza risulta compromesso per via del burnout, si possono verificare incidenti di sicurezza più gravi e più frequenti, attacchi ransomware inclusi, che finiscono poi per causare disagi operativi e perdite finanziarie significative.

Le misure strategiche e la loro efficacia

Le organizzazioni adottano varie strategie per mitigare lo stress da cybersecurity. Anche se esistono diverse misure che aiutano ad attenuare il problema (come promuovere una cultura solidale nell'azienda, offrire risorse per la salute mentale e investire nello sviluppo professionale), l'adozione di partnership strategiche esterne, in particolar modo nell'ambito dei servizi di Managed Detection and Response (MDR) è quella che mostra i risultati più promettenti.



Percentuale di intervistati affetti da questo problema che utilizzano l'MDR e che sostengono che il servizio ha ridotto lo stress e il burnout.

Dai dati di ricerca emerge che i servizi MDR sono un modo estremamente efficace per ridurre il burnout: il 92% degli intervistati che soffrono di questo problema e che utilizzano un servizio MDR dichiara infatti che ha contribuito a ridurre lo stress e il burnout da cybersecurity. La metà dei partecipanti per i quali il burnout costituisce un problema "costante" confessa di aver notato una riduzione "significativa" e un ulteriore 45% una riduzione "moderata" del burnout. Questo conferma che affidare le Security Operations più critiche a provider esperti di servizi MDR riduce notevolmente la pressione sui team interni.

Efficacia dei servizi MDR nel ridurre lo stress e il burnout da cybersecurity

Impatto	Media (n=3.750)	Livello di burnout sofferto		
		Problema costante (n=940)	Problema frequente (n=1.340)	Problema occasionale (n=1.470)
Riduzione significativa del burnout	**39%**	50%	35%	34%
Riduzione moderata del burnout	**53%**	45%	56%	56%
Totale	**92%**	95%	92%	90%

Se la tua organizzazione utilizza un servizio di Managed Detection and Response (MDR), questo ha contribuito a ridurre le esperienze di stress o burnout da cybersecurity? Intervistati che affermano di aver sofferto di burnout nei 12 mesi precedenti e la cui organizzazione utilizza un servizio MDR. Base di partecipanti indicata nel grafico.

Sophos MDR come uno dei pilastri di un sistema di difesa sostenibile

La lotta contro il cybercrimine è spietata. Per creare un sistema di difesa resiliente a tutti gli effetti, le organizzazioni non devono potenziare soltanto le proprie capacità tecnologiche, ma dal punto di vista umano sono anche tenute a tutelare il benessere dei loro team di sicurezza.

Sophos MDR offre una soluzione estremamente efficace per mitigare il burnout da cybersecurity, in quanto è in grado di risolvere molte delle cause principali di questo fenomeno:

- **Apprendimento costante:** il team Sophos MDR segue attentamente le innovazioni sia nell'ambito della protezione informatica che delle minacce, per garantire ai clienti di poter godere dei vantaggi degli sviluppi tecnologici al fine di ottimizzarne le difese.
- **Monitoraggio continuo e risposta immediata agli attacchi:** Gli analisti esperti di Sophos MDR hanno tutte le competenze necessarie per gestire la natura imprevedibile delle Security Operations per conto dei clienti. Possono spaziare da attività continue di monitoraggio, rilevamento e indagine che consumano una quantità elevata di larghezza di banda, fino a una risposta alle minacce a 360 gradi in caso di incidente, per evitare al team interno aziendale di dover intervenire precipitosamente, spesso fuori orario ufficio.
- **Accesso diretto ai nostri esperti di sicurezza:** i clienti Sophos MDR possono contare sull'esperienza di centinaia di analisti in ogni ambito delle Security Operations, inclusi esperti di threat hunting, rilevamento, indagine e risposta, nonché tecnici specializzati che agiscono dietro le quinte per contrastare malware e antagonisti informatici.
- **Protezione 24/7:** sette Security Operations Center globali che monitorano incessantemente i sistemi, garantendo ai clienti protezione completa a qualsiasi ora del giorno e della notte.
- **Valutazione degli alert basata sull'IA:** le enormi quantità di avvisi generati ogni giorno possono facilmente diventare opprimenti. Sophos MDR sfrutta la combinazione tra strumenti di valutazione con tecnologie di IA realizzati su misura e l'intervento esperti con anni di esperienza maturata sul campo per filtrare le informazioni non pertinenti e identificare rapidamente le attività sospette.

Una partnership con Sophos MDR permette alle organizzazioni di stabilire un profilo di sicurezza efficace e sicuro, non solo per potenziare le difese contro minacce come il ransomware, ma anche per offrire un sostegno fondamentale ai professionisti di cybersecurity, con attività che ne tutelino la salute mentale e il benessere professionale. In questo modo, le aziende potranno contare su difese umane sostenibili ed efficaci, anche di fronte a minacce informatiche in continua evoluzione.

Per scoprire come Sophos può aiutarti a ottimizzare le tue difese,
parla con un consulente o visita www.sophos.it/mdr

Scopri di più sul ransomware e su come Sophos può aiutarti a proteggere la tua organizzazione.

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle sue funzionalità next-gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di intelligenza artificiale e machine learning.

26/08/2025 WP (MP)

SOPHOS