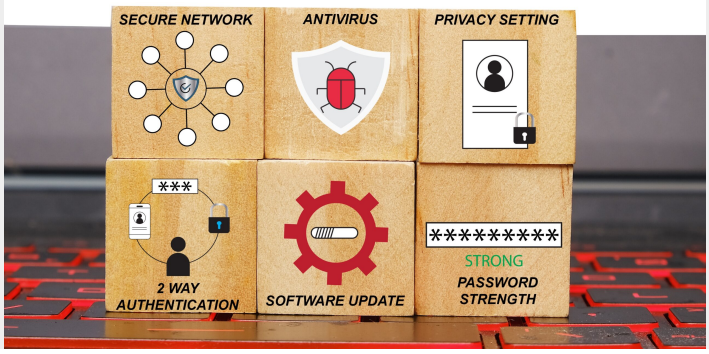
prospettiveinORGANIZZAZIONE
Rivista trimestrale di Organizzazione Aziendale
ISSN: 2465-1753

# SMART-WORKING E BYOD: QUALI RISCHI? IL RUOLO DI CYBER-AWARENESS E CYBER ORGANIZATIONAL CULTURE

*Posted on 24 Gennaio 2024 by Neri Martina e Dini Gianluca*




**Category:** Smart (Remote) Working

## Abstract

*Lo Smart-Working, soprattutto dopo la pandemia causata da Covid-19, è diventato una modalità lavorativa molto diffusa. A fronte degli innegabili vantaggi, esistono anche formidabili sfide da affrontare, tra cui la cybersecurity. Oltre alle soluzioni tecnologiche, la cyber awareness e la cyber organizational culture si attestano come approccio integrato per fronteggiare gli attacchi informatici.*

## INTRODUZIONE

Lo smart working è una modalità lavorativa che ha ricevuto recentemente un forte impulso in virtù sia dei progressi delle tecnologie ICT sia dalle politiche di gestione della pandemia da Covid-19. Una delle caratteristiche principali dello smart working è che consente di svolgere i propri compiti lavorativi da remoto, cioè da un luogo diverso dalla propria sede lavorativa.

Tuttavia, lo smart-working ha fatto emergere criticità notevoli in relazione alla cybersecurity in quanto l'impiego degli strumenti informatici è, per definizione, diffuso e lontano dalla sorveglianza del responsabile dell'organizzazione. Ad esacerbare questa situazione già di per sé critica si aggiunge la pratica del Bring Your Own Device (BYOD), che consente l'utilizzo dei propri dispositivi personali per svolgere le attività lavorative. Tutto ciò va messo in relazione con il fatto che la quasi totalità degli attacchi informatici, ad oggi, sfrutta vulnerabilità che appartengono alla sfera umana. In questo caso la tecnologia non può essere considerata il solo ed unico strumento di difesa. Infatti, la maggior parte degli attacchi informatici sono favoriti, o addirittura causati, da comportamenti umani scorretti, da cui discendono delle vulnerabilità umane che mettono a rischio tutta l'organizzazione. In questo contesto si fa riferimento al fattore umano, cioè comportamenti scorretti (causati, ad esempio, da mancanza di consapevolezza) che si traducono in un incidente informatico.

A supporto di quanto detto, i più recenti report nazionali ed internazionali evidenziano come la maggior parte degli attacchi informatici sia legata a malware di tipo generico e al phishing (Clusit Report 2023; Verizon Report 2023). I malware, cioè software malevoli, agiscono in generale contro l'utente, andando a danneggiare non solo il dispositivo interessato ma anche tutti quelli con cui l'utente comunica. Il phishing poi, appartenendo alla categoria dell'ingegneria sociale, si ricollega ad e-mail fraudolente attraverso le quali, ad esempio, si induce l'utente a rilasciare dati confidenziali come le credenziali di accesso. In entrambi i casi, sono i comportamenti errati da parte dell'utente a rendere possibile l'attacco informatico e le sue conseguenze.

In Italia il quadro complessivo non risulta essere differente. In accordo con recenti notizie diffuse dall'Agenzia Nazionale Stampa Associata (più comunemente nota come ANSA), in Italia nel 2022 e rispetto all'anno precedente, gli attacchi informatici sono aumentati del 169%. Inoltre, tra le organizzazioni che hanno subito un attacco informatico, il 79% afferma di averne subito almeno uno veicolato da e-mail di phishing. Le criticità evidenziate nell'ambito dello smart-working unite al costante aumento nel tempo degli attacchi informatici, ed insieme ad altre motivazioni, ha reso necessario l'aggiornamento normativo noto sotto il nome della NIS 2 (direttiva europea n.2555/22 approvata nel gennaio 2023). La Direttiva include misure tecniche, organizzative ed operative tra le quali è bene richiamare la cybersecurity policy, la formazione e misure sulla sicurezza delle risorse umane. In linea con tali premesse, l'obiettivo del presente lavoro è quello di analizzare dapprima il fenomeno del BYOD e come questo si configuri come profilo di rischio nel contesto specifico dello smart-working. Successivamente, dal punto di vista organizzativo, si propone una soluzione e delle prassi manageriali attraverso un approccio integrato orientato alla *cyber-awareness* e alla *cyber organizational culture*. Tali leve organizzative sono dei driver cruciali affinché l'utilizzo di dispositivi personali, in particolare quelli mobili, non si configuri come un potenziale rischio di perdita di confidenzialità, integrità e disponibilità dei dati per l'organizzazione. La cyber-awareness e la cyber organizational culture sono infatti due elementi fondamentali, e complementari alle soluzioni tecnologiche, per instaurare un utilizzo consapevole e sicuro dei dispositivi personali. La cyber-awareness si configura come veicolo privilegiato attraverso il quale l'organizzazione forma ed informa i dipendenti rispetto alle pratiche più sicure per preservare i dati (Corallo et al., 2022). La cyber organizational culture, d'altro canto, ne diventa una estensione naturale che identifica i comportamenti in linea con le linea guida in tema di sicurezza dei dati (Da Veiga et al., 2020). Se correttamente sfruttate, queste due leve organizzative contribuiscono in modo complementare alle tecnologie all'utilizzo dei dispositivi in modo sicuro nel tempo.

prospettiveinORGANIZZAZIONE
Rivista trimestrale di Organizzazione Aziendale
ISSN: 2465-1753

# SMART-WORKING E BYOD: QUALI RISCHI?

Nonostante non sia stato ancora raggiunto un pieno consenso in merito alla definizione e ai temi dello smart-working, in generale, è possibile affermare che esso si configuri come una modalità lavorativa in cui, tra le altre caratteristiche, è possibile svolgere i propri compiti al di fuori dei confini dell'organizzazione, ad esempio da casa, attraverso le tecnologie dell'informazione e della comunicazione (meglio note come ICT, cioè Information and Communication Technologies) (Kim and Oh, 2015). Tra queste, particolare rilevanza assumo i dispositivi mobili, come ad esempio gli smartphone. Lo smart-working, indubbiamente, rappresenta ad oggi una modalità lavorativa che, se pur avendo origini non recenti (quando considerato come una estensione del telelavoro), ha guadagnato ampio spazio soprattutto a seguito della pandemia da Covid-19. Infatti, proprio durante la pandemia, il numero di organizzazioni che ha adottato questa modalità lavorativa è cresciuto notevolmente. Solo in Italia, secondo i dati rilasciati recentemente dall'Osservatorio smart-working del Politecnico di Milano, nel 2020 ben 6,58 milioni di italiani lavoravano in smart-working, contro i 570.000 del 2019.

Inoltre, sebbene nel post-pandemia si sia verificato un decremento nell'applicazione dello smart-working, l'Osservatorio smart working del Politecnico di Milano prevede comunque per il futuro un aumento delle aziende che adotteranno questa modalità lavorativa.

Infatti, lo smart-working, presenta numerosi vantaggi slegati da quelli specifici del contesto pandemico. Tra questi è possibile menzionare un aumento della soddisfazione nel lavoro, una migliore percezione di benessere rispetto al contesto lavorativo, nonché una maggior bilanciamento tra vita privata e lavorativa. È vero anche però che lo smart-working porta con sé una serie di problematiche, come ad esempio le interazioni sociali ridotte o, addirittura, del tutto assenti.

Ci concentriamo qui però su uno specifico profilo di rischio associato allo smart-working con particolare riferimento alle tecnologie ICT.

Infatti, proprio i dispositivi personali e l'uso ad essi associato, configura uno specifico profilo di rischio attraverso il fenomeno del BYOD, cioè l'utilizzo di dispostivi personali, tra cui computer, tablet e smartphone per accedere a dati aziendali o, più in generale, svolgere i propri compiti lavorativi (Baillette and Barlette, 2017).

Il BYOD può essere quindi definito come una policy implementata nelle organizzazioni con un intento duale. Da un lato è possibile, infatti, accedere ai dati dell'organizzazione attraverso l'infrastruttura informatica dell'organizzazione, ma con i propri dispostivi personali. D'altra parte, il senso del BYOD risiede anche nella possibilità di accedere ai dati, per svolgere i propri compiti, quando si è all'esterno dell'organizzazione, come ad esempio in condizioni di smart-working.

Già nel 2019 su Forbes, riassumendo diversi dati in tema di BYOD, si evidenziava come il mercato per questo fenomeno avrebbe raggiunto i 367 miliardi di dollari nel 2022.

Da un lato l'utilizzo di tali dispositivi consente una maggiore flessibilità nelle ore di lavoro, nonché una maggiore efficienza legata all'utilizzo di dispositivi familiari all'utilizzatore. Inoltre, proprio l'applicazione del BYOD influenza e aumenta i comportamenti innovativi, oltre che avviare trasformazioni *it-driven* che fanno progredire i processi organizzativi. In generale, il BYOD comporta anche un risparmio non indifferente per l'organizzazione, che non deve quindi preoccuparsi di acquistare la dotazione di dispositivi, come smartphone, da conferire ai dipendenti

È vero anche che una serie di rischi in termini di cybersecurity è associata a questa pratica. Il dibattito sui rischi del BYOD è ancora aperto e oggetto di discussione e ricerca, sia scientifica sia divulgativa (Mellone, 2023; Ratchford et al., 2022). In generale, proprio questi dispositivi potrebbero essere obiettivo o veicolo privilegiato di attacchi informatici, compromettendo la sicurezza dei dati dell'organizzazione. Ampliando la platea di dispositivi utilizzati, nello specifico quelli ad uso promiscuo, è possibile che questi non abbiano le adeguate misure (tecnologiche e organizzative) di sicurezza necessarie a proteggere le informazioni.

In senso tecnico, tali dispositivi, infatti, escono dal controllo completo del reparto IT, che per ripristinare le funzioni in caso di attacco informatico potrebbe doversi trovare a gestire dispostivi diversi, con diversi software installati. Di conseguenza, senza l'infrastruttura adatta, i benefici sopra citati possono trasformarsi molto rapidamente in un incremento di tempi di gestione e controllo dei dispositivi stessi. I dispositivi potrebbero poi essere connessi a reti domestiche o pubbliche più facilmente accessibili dai criminali informatici, esponendo così a un rischio maggiore i dati dell'organizzazione. Inoltre, banalmente, i dispositivi potrebbero essere rubati, rendendo molto difficoltosa sia la protezione dei dati memorizzati su tali dispositivi sia il recupero degli stessi se non sono state definite e realizzate specifiche strategie di protezione e recupero. I dispositivi propri dell'organizzazione beneficiano di sistemi e servizi di sicurezza più avanzati, come ad esempio un servizio di filtraggio anti-spam fornito dall'organizzazione stessa che costituisce una valida, sebbene non risolutiva, barriera contro le email di phishing. I dispositivi personali, in quanto tali, potrebbero non beneficiare affatto o comunque non pienamente di questo tipo di protezione. Per esempio, un dispositivo personale potrebbe scaricare e-mail anche da domini diversi da quello dell'organizzazione di appartenenza che non eseguono un adeguato filtraggio anti-spam. È più facile quindi che i criminali informatici, puntando sempre all'anello debole dall'organizzazione, possano trovare più facile intervenire su questi dispositivi probabilmente meno protetti. Gli attacchi informatici, infatti, potrebbero essere mirati verso account personali con l'obiettivo di compromettere l'intero dispositivo.

Possiamo affermare che un primo punto chiave su cui si dovrebbe basare la decisione di optare per l'utilizzo di dispositivi digitali, e in particolare per il BYOD, è l'esistenza di tecnologie di sicurezza adeguate che permettano di gestire, almeno in parte, dispositivi che non rientrano sotto il pieno controllo dell'organizzazione. Tuttavia, le misure tecnologiche, per quanto necessarie, da sole non sono sufficienti a garantire la sicurezza informatica dell'organizzazione.

Infatti, tra gli altri rischi legati a questa pratica ne esistono alcuni che si configurano come più strettamente attenenti al profilo organizzativo della cybersecurity. Infatti, seppur generalmente ricondotta alla sfera tecnologica, una nuova area di ricerca è sempre più orientata ad analizzare la cybersecurity unitamente alla dimensione organizzativa e manageriale (Dalal et. al., 2022). In questo caso, come già detto prima in tema di fattore umano, la tecnologia da sola non può essere considerata lo strumento unico per fronteggiare i rischi associati al BYOD. Infatti, molti dei rischi a cui l'organizzazione viene esposta si legano a comportamenti scorretti da parte dei dipendenti nell'utilizzo di tali dispositivi.

L'implementazione di una BYOD policy rappresenta già di per sé una grande sfida per le organizzazioni, che non sempre riescono a formalizzare questo tipo di documentazione, affidandosi in genere a una serie di buone pratiche informali. Questo accade soprattutto per organizzazioni piccole e molto piccole le quali, se pur affrontando le stesse minacce informatiche di quelle di più grande dimensione, non hanno a disposizione le stesse risorse e, spesso, neanche la stessa consapevolezza. Anche quando definita, bisognerebbe assicurarsi che i dipendenti siano in grado di comprendere e seguire la cybersecurity policy a tutto tondo, proteggendo i dati dell'organizzazione.

## UN APPROCCIO INTEGRATO: CYBER AWARENESS E CYBER ORGANIZATIONAL CULTURE

Alla luce di quanto detto fino ad ora, appare chiaro che le protezioni di natura tecnologica, sono indubbiamente un fattore importante da tenere in considerazione quando si decide di adottare una strategia di BYOD. Tuttavia, le soluzioni tecnologiche non possono ad oggi rappresentate l'unico strumento di difesa contro gli attacchi informatici.

In linea con quanto detto, si propone quindi un approccio integrato orientato alla cyber awareness e alla cyber organizational culture. Tali fattori, sono qui intesi come complementari alle soluzioni tecnologiche. Infatti, rappresentano un importante strumento di difesa per arginare l'esposizione al rischio informatico causato dalle vulnerabilità legate al fattore umano. Cyber awareness e cyber organizational culture possono essere poi visti come due elementi fortemente correlati.

Partendo dalla cyber awareness, questa presuppone due elementi fondamentali. Il primo elemento costitutivo risiede nella conoscenza generale che chi opera all'interno dell'organizzazione, più nello specifico i dipendenti, hanno in merito agli obiettivi di sicurezza dell'organizzazione e alla sua Information Security Policy (ISP) (Bulgurcu et al., 2010). Altro elemento fondante è il comportamento. Infatti, una volta compresi gli obiettivi di cui sopra, il comportamento dei dipendenti si conformerà agli stessi, orientandosi quindi verso la protezione dei dati dell'organizzazione (Parsons, 2017). Viene da sé, quindi, che ciò si traduce in un duplice impegno. Da un lato quello dell'organizzazione di fornire gli strumenti utili a diffondere la conoscenza sui temi di cybersecurity all'interno dell'organizzazione. Dall'altro, quello dei dipendenti nell'allineare i propri comportamenti agli

obiettivi di sicurezza. Quando questo obiettivo viene raggiunto, creando così un allineamento, la cyber awareness contribuisce alla protezione dell'organizzazione attraverso i comportamenti. van Niekerk and von Solms (2006), a tal proposito, sostengono che la cybersecurity awareness esiste solo quando esiste la conoscenza.

La cyber awareness e i suoi elementi fondanti, rappresentano la base attraverso cui costruire la cyber organizational culture. Questa è considerata come uno dei migliori approcci al fattore umano e alle problematiche di cybersecurity ad esso legate (van Niekerk e von Solms, 2010). Riprendendo la più che celebre definizione di cultura organizzativa di Edgar Schein (2010), anche con riferimento specifico alla cybersecurity, questa può essere definita come le credenze, i valori e gli atteggiamenti che guidano i comportamenti dei dipendenti per proteggere e difendere l'organizzazione dagli attacchi informatici. Anche la cyber organizational culture viene definita come legata al comportamento umano all'interno del contesto organizzativo, ed è volta a proteggere l'organizzazione stessa.

È possibile notare quindi come il fine ultimo della cyber awareness e della cyber organizational culture siano strettamente correlati. Se è vero che la stessa cyber awareness è un elemento chiave su cui si fonda la cyber organizational culture, è però solo attraverso quest'ultima che la cybersecurity entra a far parte in modo naturale delle attività svolte quotidianamente da e per l'organizzazione.

Di seguito si da evidenza delle prassi manageriali a supporto di una corretta implementazione dell'approccio integrato qui proposto.

# PRASSI MANAGERIALI A SUPPORTO

Partendo dalla cyber awareness, le prassi manageriali a supporto su cui le organizzazioni possono far leva sono diverse. Al fine di stimolare la conoscenza due fattori fondamentali sono rappresentati dalla formazione e dall'implementazione di una cybersecurity policy. La cybersecurity policy è costituita da un insieme di regole, linee guida, pratiche e procedure che stabiliscono le modalità con cui l'organizzazione affronta e gestisce la sicurezza informatica. Attraverso la cybersecurity policy vengono definite le strategie e gli obiettivi di sicurezza dell'organizzazione, insieme a tutte le misure necessaria per proteggere le risorse informatiche da minacce (siano esse interne o esterne) o accessi non autorizzati. Ancora, attraverso questa vengono definite le misure volte a prevenire la perdita, la divulgazione o la corruzione delle informazioni dell'organizzazione. Questa deve essere diffusa a tutti i livelli dell'organizzazione, nonché aggiornata con cadenza regolare. In generale, una cybersecurity policy può riguardare aspetti più o meno tecnici legati alla cybersecurity. Tuttavia, in questo contesto, elementi chiave sono l'utilizzo dei dispositivi personali e/o mobili. Ad esempio, quali siano i comportamenti sicuri e adeguati da adottare quando si scaricano applicazioni o si visitano siti web. In questo caso, indicazioni utili da contenere nella policy o da veicolare tramite la formazione sono come riconoscere siti web ufficiali da quelli fraudolenti, o ancora come riconoscere una applicazione certificata da una che potrebbe

contenere un malware. Inoltre, questa potrebbe riguardare la gestione delle password (frequenza di aggiornamento o come impostare una password sicura) o la corretta conservazione di dati aziendali all'interno del dispositivo. La formazione poi deve essere svolta con cadenza regolare, fungendo quindi non solo come strumento attraverso cui porre le basi della conoscenza, ma come strumento per alimentarla continuamente nel tempo. La formazione dovrebbe essere orientata al dipendente tenendo conto di diverse modalità attraverso cui svolgerla. Ad esempio, potrebbe essere più efficace utilizzare delle simulazioni e non solo delle lezioni frontali. Inoltre, la formazione presuppone una pianificazione di lungo termine, predisponendo così degli incontri cadenzati e regolari durante l'anno. Questo permetterebbe di essere costantemente aggiornati. La formazione dovrebbe essere demandata ad esperti di cybersecurity che possano predisporre la strategia di apprendimento più adatta alle necessità dell'organizzazione e dei dipendenti.

Continuando la discussione con la cyber organizational culture, sappiamo che questa viene stimolata attraverso la comunicazione, la sensibilizzazione e la formazione, nonché veicolata anch'essa tramite la cybersecurity policy. Infatti, quando la cultura della cybersecurity esiste all'interno dell'organizzazione, questa stimola il rispetto della cybersecurity policy. Tra le prassi manageriali più importanti ritroviamo la guida e il coinvolgimento del management, la stessa cyber awareness e la formazione. Soffermandoci sulle prassi fin qui non discusse, possiamo dire che per quanto riguarda la figura del management e il suo coinvolgimento, questo rappresenta un elemento molto importante affinché non solo vengano stabilite le priorità in termini di cybersecurity, ma anche che misure contenute nella cybersecurity policy vengano diffuse in tutta l'organizzazione. Il management ha poi il compito di partecipare attivamente alle attività sul tema, come ad esempio la formazione. I canali di comunicazione sono poi essenziali affinché si veicolino le informazioni e le buone pratiche. Questi devono essere stabiliti dal management e possono avere carattere formale o informale. La loro funzione principale risiede nel segnalare tempestivamente attacchi informatici, condividere informazioni sulle emergenti dinamiche cyber, o ancora identificare potenziali vulnerabilità. Un esempio potrebbe essere dedicare alcuni minuti di ogni riunione a condividere delle notizie o informazioni circa la cybersecurity, o ancora istituire delle riunioni ad hoc con tutto il personale. Questo farà sì che l'importanza della cybersecurity e della protezione delle informazioni sia percepito come un elemento di estremo rilievo all'interno dell'organizzazione. Sono diverse poi le figure che possono essere inserite nel contesto organizzativo come esperti di cybersecurity. Tra questi ricordiamo ad esempio il Chief Information Security Officer (CISO), cioè il manager responsabile nel definire la strategia di cybersecurity dell'organizzazione. L'insediamento di una figura esperta e dedita solo alla gestione della cybersecurity fungerà da facilitatore nella diffusione della conoscenza, di monitoraggio dell'efficacia delle pratiche di cybersecurity nonché punto di riferimento e coordinamento durante un attacco informatico.

# CONCLUSIONI

Gli attacchi informatici ad oggi si diffondono ad ampio spettro verso qualsiasi tipo di organizzazione, con numeri che mostrano tutt'altro che un possibile decremento.

L'evolvere delle metodologie lavorative, soprattutto a causa della pandemia causata da Covid-19, ha fatto sì che vi fosse un aumento considerevole dell'utilizzo dei dispositivi personali a supporto dello svolgimento dei propri compiti durante lo smart-working. Proprio questi dispositivi, quando utilizzati senza la corretta conoscenza, possono diventare veicolo di attacchi informatici che mettono a rischio i dati delle organizzazioni. Ad oggi, la maggioranza degli attacchi informatici sfrutta però vulnerabilità che non possono essere risolte solo tramite strumenti tecnologici, poiché puntano a far leva sul fattore umano. Come qui proposto, sono diverse le azioni che le organizzazioni possono intraprendere al fine di operare in condizioni di cyber awareness e cyber organizational culture. Tra queste, implementare una cybersecurity policy volta a identificare le misure necessarie a proteggere l'organizzazione dall'utilizzo non corretto dei dispositivi personali. Ancora, assicurare a tutti coloro che operano all'interno dell'organizzazione adeguata formazione sulle tematiche di cybersecurity.

L'approccio integrato qui discusso si configura come un valido strumento a supporto della tecnologia, quando inserito in modo coerente in una strategia di cybersecurity. Dunque, un approccio integrato volto alla cyber awareness e alla cyber organizational culture può far sì che l'elemento umano si evolva da veicolo principale di vulnerabilità a strumento di difesa.

## Ringraziamenti

Il presente lavoro è stato finanziato dall'Università di Pisa per mezzo dei fondi "PRA-Progetti di Ricerca di Ateneo"-n.progetto PRA_2022_2023 "Valutazione della consapevolezza e della preparazione alla cybersecurity nel settore sanitario" (PRA_2022_87).

## Bibliografia

Baillette, P., & Barlette, Y. (2018). BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs: The identification of a twofold security paradox. Journal of Organizational Change Management, 31(4), 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548. https://doi.org/10.2307/25750690

Clusit (2022). Rapporto Clusit 2023 sulla sicurezza ICT in Italia. Consultato l'11 maggio 2023 da https://clusit.it/rapporto-clusit/

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial

Internet of Things: A systematic literature review. Computers in Industry, 137, 103614. https://doi.org/10.1016/j.compind.2022.103614

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. Journal of Business and Psychology, 37(1), 1-29. https://doi.org/10.1007/s10869-021-09732-9

Kim Yong-Young & Oh Sangjo (2015). What makes smart work successful? Overcoming the constraints of time geography, Proceedings 48th Hawaii International Conference on System Sciences, January 5(8), 1038-1047.

Mellone, M., (2023, 30 Maggio). BYOD in azienda, consigli per farlo bene. Agenda Digitale. https://www.agendadigitale.eu/sicurezza/byod-in-azienda-rischi-e-opportunita/

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. Information Security Journal: A Global Perspective, 31(3), 253–273. https://doi.org/10.1080/19393555.2021.1923873

Schein, E. H. (2010). Organizational culture and leadership (Vol. 2). John Wiley & Sons.

Van Niekerk, J., & Von Solms, R. (2006, July). Understanding Information Security Culture: A Conceptual Framework. In ISSA (pp. 1-10)

Van Niekerk, J.F., Von Solms, R. (2010). Information security culture: a management perspective. Computers & Security, 29, 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Verizon (2023). Data breach investigations report. Consultato il 24 aprile 2023 da https://www.verizon.com/business/resources/reports/dbir/

# Sitografia

ANSA (2023, 28 febbraio). In Italia 79% aziende ha subito almeno un attacco via email. ANSA. https://www.ansa.it/sito/notizie/tecnologia/hitech/2023/02/28/in-italia-79-aziende-ha-subito-almeno-un-attacco-via-email_e7b2c8f9-136a-43f9-b66c-aa2f47d49c26.html

Bullock, L., (2019, 21 Gennaio). The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future. Forbes. https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/?sh=468155731f30

Crespi, F., (2023, 23 gennaio). Smart Worker: chi sono e quanti sono i lavoratori agili in Italia. Osservatori digital innovation. https://blog.osservatori.net/it_it/smart-worker-in-italia#:~:text=Secondo%20i%20numeri%20dell%27Osservatorio,3%20dei%20lavoratori%20dipendenti%20italiani).

Santamato (2023, 23 Marzo). Italia nel mirino hacker, +169% attacchi nel 2022. ANSA. https://www.ansa.it/sito/notizie/tecnologia/hitech/2023/03/07/italia-nel-mirino-hacker-169-attacchi-nel-2022_487da952-05a3-40b8-b746-6b5f5a2388df.html