

Il ruolo degli studi legali si sta evolvendo fino alla governance integrata del rischio cyber

Cybersecurity e pmi, nuova frontiera della consulenza

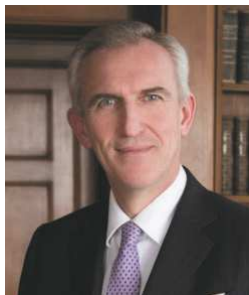
Pagine a cura

DI LUCA SETTEBRINI

Il rischio Cybersecurity è sempre più diffuso e a farne le spese non sono solamente le grandi strutture o le PA, ma anche le pmi. Una recente indagine sul fenomeno, il «Cisco Cybersecurity Readiness Index 2025», evidenzia che il 33% delle pmi italiane ha subito almeno un attacco informatico nell'ultimo anno, mentre l'80% segnala una significativa carenza di specialisti in sicurezza informatica. Tuttavia, il 97% delle aziende intervistate ha dichiarato l'intenzione di aggiornare o ristrutturare le proprie soluzioni di cybersecurity entro i prossimi due anni.

Porte d'ingresso degli attacchi sono hardware e software obsoleti, la non disattivazione di funzionalità e plugin non necessari, l'impiego di antivirus, firewall e policy di dominio rivisti e aggiornati e l'utilizzo di strumenti di intelligenza artificiale. A questi vanno aggiunte competenze interne più specifiche e la collaborazione con partner specializzati in cybersecurity. In questo scenario, il ruolo degli studi legali si è ampliato significativamente, evolvendo dalla mera gestione degli incidenti alla prevenzione e alla governance integrata del rischio cyber.

«Per i CdA, il perimetro dei rischi legali si amplia rapidamente: cyberattacchi e interruzioni operative impongono piani di risposta, continuità e gestione dei fornitori; sul fronte della riservatezza dei dati, un'applicazione più severa richiede minimizzazione, basi giuridiche e controllo dei trasferimenti», dice **Alessandro De Nicola**, partner responsabile del dipartimento Legal risk & compliance di **BonelliErede**. «Le sanzioni internazionali impongono verifiche su clienti e fornitori lungo la catena del valore, clausole contrattuali e monitoraggio extraterritoriale. La responsabilità 231 esige modelli aggiornati alla luce dei pericoli ingenerati dall'IA e dell'attenzione alle sicurezza sul lavoro anche della propria supply chain, con vigilanza effettiva. La protezione dei segreti aziendali richiede misure «ragionevoli» (accessi, accordi di riservatezza, tracciamento) e difesa contro minacce interne. Serve un sistema di controllo e compliance integrato, basato sul rischio, con mappatura processi, verifiche sulle controparti, indicatori di prestazione e di rischio, verifiche continue e canali di segnalazione verso un CdA competente, formato, con propensione al rischio definita



Alessandro De Nicola



Stefano Mele



Andrea Mezzetti



Elena Bassoli



Simona Lanna



Mascia Cassella

e un chiaro piano d'azione».

«In Gianni & Origoni assistiamo le pmi sui temi di diritto applicato alla cybersecurity con un approccio che tiene insieme mercato, regole e gestione del rischio.

Per molte imprese il tema principale da gestire non nasce solo da un attacco informatico, ma dall'essere spesso fornitori di soggetti più strutturati e regolati. In questi casi le pmi devono rispettare requisiti di sicurezza cyber imposti da contratti, audit e processi di qualificazione, spesso come condizione per mantenere commesse e posizionamento nella filiera. La nostra consulenza legale serve a rendere queste richieste governabili, distinguendo ciò che è davvero vincolante da ciò che è sproporzionato e costruendo quindi risposte sostenibili con risorse spesso anche molto limitate» ricorda **Stefano Mele**, responsabile delle practice di Cybersecurity e Space Economy Law, oltre che co-responsabile della practice Data Protection dello studio **Gianni & Origoni**. Un secondo asse di supporto legale riguarda la catena dei fornitori. «Le pmi non devono solo proteggere sé stesse, ma anche gestire il rischio derivante da partner tecnologici e subfornitori, attraverso clausole contrattuali, responsabilità chiare, controlli realistici e meccanismi di verifica compatibili con la loro

struttura. Resta naturalmente centrale anche la compliance, dalla normativa europea e nazionale agli standard richiesti dal mercato, con l'obiettivo di integrare obblighi e processi nella gestione ordinaria dell'impresa e non limitarli a un mero esercizio di scrittura formale della documentazione (la c.d. «paper security»). Infine, quando si verifica un incidente informatico, affianchiamo le pmi nella gestione end to end della crisi cibernetica, dalla risposta operativa prevista dalle norme alle comunicazioni e interloquzioni con autorità e stakeholder. In sostanza, il nostro ruolo non è quello di sostituirsi ai tecnici informatici, ma di aiutare le pmi a prendere decisioni consapevoli in un contesto complesso. L'esperienza del nostro Studio anche nella gestione diretta dei propri rischi informatici, attestata dall'essere stato il primo studio legale in Italia ad ottenere e mantenere nel tempo anche la certificazione ISO 27001, ci consente di avvicinarci a questi temi con un taglio molto pragmatico, orientato soprattutto alle decisioni e al business, anche grazie ai nostri team multidisciplinari dedicati e costruiti per far fronte ad ognuno dei singoli scenari finora richiamati».

«In questo contesto, abbiamo compreso che l'attenzione del legale si concentra sempre più sui profili di governance e

di responsabilità, soprattutto alla luce dell'entrata in vigore di normative quali la NIS II e il regolamento DORA, che rafforzano gli obblighi organizzativi, di controllo e di resilienza digitale per numerosi operatori, con ricadute indirette anche sulle pmi inserite nelle relative filiere», dice **Matteo Cerretti** partner di **DWF**. «La consulenza richiesta non si limita alla gestione dell'evento patologico, ma riguarda in misura crescente la fase preventiva: analisi dei rischi, definizione di assetti organizzativi adeguati, revisione dei contratti con fornitori ICT, predisposizione di procedure interne per la gestione degli incidenti e per le notifiche alle autorità competenti, nonché coordinamento con i presidi in materia di protezione dei dati personali. I clienti insomma comprendono che in una materia così delicata la prevenzione sia fondamentale e molto più efficace di un intervento a incidente avvenuto. Un ulteriore ambito di intervento concerne la formazione del personale e del management, considerata oggi un elemento essenziale della strategia di mitigazione del rischio. Le pmi richiedono sempre più spesso momenti di aggiornamento normativo e di sensibilizzazione, al fine di integrare la cultura della sicurezza nei processi aziendali. L'avvocato non sostituisce le competenze specialistiche in ambito

ICT, ma opera in sinergia con consulenti tecnici qualificati, chiamati a valutare le vulnerabilità dei sistemi, a implementare le misure di sicurezza e a gestire operativamente gli incidenti. Solo l'integrazione tra competenze legali e tecniche consente di costruire modelli organizzativi adeguati e di affrontare eventuali crisi in modo tempestivo e conforme al quadro normativo».

«Seguiamo i nostri clienti nell'interpretazione della complessa regolamentazione in materia di cybersecurity e dei relativi requisiti previsti dall'ACN, lavorando fianco a fianco con i team tecnici e legali per assicurare un'interpretazione conforme alla legge ma al contempo legata alle esigenze ed alla realtà delle pmi», dice **Andrea Mezzetti**, partner di **Osborne Clarke Italia**. «Sul tema della cybersecurity opera il nostro team AI & Digitalisation. Lo Studio può anche contare su un team dedicato al settore Life Sciences & Healthcare, guidato dalla partner **Maria Grazia Medici**. Per tutte le questioni di cyber-sicurezza che impattano sull'ambito sanitario, **Marialaura Boni**, counsel ed esperta di Data Protection, rappresenta il punto di raccordo tra le competenze dei due team. In caso di incidenti cross-border, Osborne Clarke fornisce assistenza con team multi-giurisdizionali, costituiti di volta in volta in base ai Paesi coinvolti e alle specifiche esigenze del caso».

Altra realtà fortemente specializzata in materia è lo studio **Bird & Bird**. «Per quanto concerne i propri sistemi informativi e di network», spiega **Gian Marco Rinaldi**, Counsel del dipartimento di Proprietà Intellettuale, «lo studio adotta un approccio multilivello alla cybersecurity, che comprende controlli avanzati su rete, dispositivi e accessi, progettati per prevenire minacce e individuare tempestivamente attività anomale, la gestione proattiva degli incidenti, supportata da procedure interne che consentono di intervenire rapidamente, documentare gli eventi e ridurre al minimo l'impatto operativo, la conformità agli standard di resilienza cibernetica, che prevedono criteri stringenti su governance, processi di risposta e piani di continuità operativa. In questo contesto la sicurezza informatica è efficace solo se condivisa da tutta l'organizzazione. Per questo lo studio ha sviluppato programmi periodici di formazione e sensibilizzazione, che includono percorsi di awareness per riconoscere tentativi di phi-

Le pmi hanno capito che la prevenzione è fondamentale

shing, comportamenti rischiosi e minacce emergenti cui si aggiungono moduli e contenuti della Digital Academy, orientati allo sviluppo di competenze digitali e alla comprensione dei rischi connessi all'uso delle tecnologie e simulazioni e campagne comportamentali, utili per rinforzare le buone pratiche e migliorare la reattività degli utenti di fronte a possibili attacchi. Per quanto riguarda i servizi di consulenza offerti ai nostri clienti in relazione alla compliance NIS2, abbiamo costituito un team specializzato di tre professionisti coordinato dal sottoscritto. In questi 15 mesi di applicazione del dlgs 138/2024 («Decreto NIS2»), il nostro team ha assistito società nazionali e internazionali nelle attività di auto-valutazione, di registrazione, di aggiornamento annuale e di implementazione degli obblighi di notifica e sulle misure di sicurezza. Lavoriamo in stretta cooperazione con i dipartimenti legali ed IT delle aziende assistite confermando come l'analisi e l'interpretazione giuridica delle norme e dei regolamenti predisposti dall'ACN sia centrale per la corretta applicazione delle misure previste. Molte aziende hanno adottato un approccio corretto comprendendo come la conformità alla normativa NIS2 sia un'occasione per rafforzare la sicurezza della società a fronte di minacce sempre più evolute e pericolose».

Altra realtà molto attiva è **LCA Studio Legale**: «Per tutte le imprese, e per alcune pmi in particolare, la sicurezza informatica rappresenta una sfida di natura culturale, che richiede un cambio di approccio e una maggiore consapevolezza a tutti i livelli dell'organizzazione», spiega **Giulio Vecchi**, equity partner del Dipartimento IP, Media, Tech & Data di LCA Studio Legale. «In questo contesto, anche alla luce degli obblighi introdotti dalla direttiva NIS2, il nostro Studio affianca le pmi con una consulenza mirata e di governance in materia di cybersecurity, supportando le imprese nella comprensione del rischio cyber, nella valutazione del suo impatto sul business e nella definizione di modelli di prevenzione e gestione coerenti con la loro dimensione e con un quadro normativo di riferimento particolarmente articolato. Il valore aggiunto dell'approccio adottato risiede nella presenza di un team con una solida conoscenza della regolamentazione del digitale. La cybersecurity viene infatti affrontata all'interno di un sistema di regole che si intersecano e si sovrappongono - dal GDPR all'AI Act, dal Digital Services Act ad altre normative settoriali - con l'obiettivo di fornire un'assistenza organica e indicazioni operative concrete per le imprese. L'obiettivo è superare una logica emergenziale della sicurezza informatica, favorendo invece una pianificazione by design integrata nei processi aziendali e nei mecca-

nismi di governance. Le attività in ambito cybersecurity coinvolgono un team dedicato composto da professionisti con competenze in materia di sicurezza informatica, data protection e contrattualistica IT. Per gli aspetti strettamente tecnici, quali test di sicurezza, valutazioni infrastrutturali e gestione degli incidenti, lo Studio si avvale di partner esterni di comprovata esperienza e affidabilità. Il nostro studio opera, quindi, come punto di raccordo tra l'impresa e i fornitori tecnologici, garantendo coordinamento, e supervisione. Le principali complessità riscontrate nello svolgimento di queste attività riguardano la carenza di competenze interne alle aziende e la frammentazione delle soluzioni tecnologiche che si sono stratificate nel tempo. Sotto il profilo organizzativo, emerge inoltre la difficoltà di coordinare fornitori diversi, spesso in presenza di budget limitati, e di integrare in modo strutturato la cybersecurity nei processi decisionali. A ciò si aggiungono gli obblighi derivanti da una pluralità di normative europee e nazionali e le crescenti responsabilità attribuite agli organi di amministrazione e controllo. Per quanto riguarda LCA, la cybersecurity è considerata un tema trasversale di primaria importanza. Sono state adottate policy interne di sicurezza, programmi di formazione e procedure di controllo sui sistemi informativi e sui flussi di dati, nella consapevolezza che la protezione delle informazioni costituisce parte integrante della responsabilità professionale e della fiducia riposta dai clienti. Non a caso, lo Studio è sempre più frequentemente sottoposto ad assessment e audit da parte dei clienti più strutturati» aggiunge Vecchi.

«Sul piano interno, gestiamo la superficie di rischio con un approccio «security-by-design»: MFA ovunque, gestione password e privilegi minimi, cifratura dei dispositivi, backup segregati, protezione endpoint/anti-phishing, procedure di gestione incidenti e data breach, oltre a formazione periodica e regole di condivisione sicura dei documenti», dice **Elena Bassoli**, avvocato e docente universitario in diritto dell'informatica e informatica giuridica. «L'obiettivo è ridurre soprattutto rischio «human factor» e compromissioni via e-mail e credenziali. Per i clienti (in prevalenza pmi) la domanda è sempre più «ibrida»: non solo GDPR e data breach, ma anche valutazioni di rischio, governance e responsabilità, contrattualistica (fornitori IT/cloud, log, SLA, audit, penali), policy interne (accessi, smart working, BYOD), piani di risposta e simulazioni tabletop. In caso di incidente, affianchiamo l'azienda nella triage legale/tecnico, nelle notifiche (Garante/Interessati quando dovute), nella gestione dei rapporti con assicurazione cyber e

nella preservazione delle evidenze, con supporto di partner tecnici quando necessario. Le complessità tipiche sono budget limitati, filiera di fornitori frammentata, carenza di competenze interne e aumento di minacce abilitate da Intelligenza artificiale». Lo Studio opera come boutique con 3 professionisti legali (ognuno nel proprio studio, coordinati come team) e ricorriamo, quando utile, a consulenti tecnici esterni (incident response/forensics) per le attività specialistiche.

Gli incidenti e le minacce informatiche (data breach, frodi su IBAN, malware, solo per citarne alcuni) producono danni rilevanti e, quando emergono, è già troppo tardi», dice **Luca Marasco**, senior associate di **Eptalex - Garzia Gasperi Iannaccone & Partners**. «La tutela legale ex post è marginale: serve prevenzione. Nelle pmi, però, sicurezza e compliance sono spesso percepite come costi, non come strumenti di protezione del patrimonio aziendale. La prevenzione efficace richiede invece un doppio canale integrato: giuridico (procedure, policy, governance, contratti) e tecnico (misure di sicurezza, controlli, monitoraggio). Ciò in quanto la tecnologia, da sola, non basta a prevenire: gli incidenti derivano quasi sempre da errori umani. Ma è soprattutto nel supporto alle imprese clienti che lo studio legale riveste un ruolo decisivo. In primo luogo, lo studio legale svolge nei confronti del cliente una valutazione preliminare sull'applicabilità di DORA o NIS2 e sul livello di esposizione al rischio, in coordinamento con i professionisti IT (interni alla società cliente, o esterni individuati, se del caso, tra quelli con cui lo studio legale collabora abitualmente), distinguendo tra soggetti obbligati e società che, pur esterne al perimetro normativo, devono adeguarsi alle richieste contrattuali dei clienti, quali due diligence, audit, obblighi di notifica, SLA, garanzie di sicurezza. Fondamentale è poi il supporto dello studio legale nel raccordo tra IT e management per tradurre requisiti tecnici in obblighi giuridici sostenibili e rendere consapevole il board dei rischi legali e reputazionali. L'adeguamento richiede invero un approccio risk-based e proporzionato: la customizzazione della documentazione richiesta (policies, clausole contrattuali, questionario di due diligence, ecc.) non è opzionale, ma imposta dalla normativa, soprattutto per le pmi, che altrimenti rischiano di adottare obblighi (e costi) sproporzionati rispetto alla propria effettiva esposizione al rischio informatico. Lo studio legale deve svolgere pertanto il ruolo di alleato strategico nella definizione in concreto delle misure organizzative di prevenzione degli incidenti e minacce informatiche, nel rispetto delle reali esigenze del cliente».

«Con l'avvento delle diretti-

ve e dei regolamenti DORA, NIS, CRA e AI Act, il tema della sicurezza e resilienza dei sistemi informativi e di rete è diventato di primaria importanza per le imprese e per le altre entità che forniscono servizi critici ed essenziali per il funzionamento della società civile», dice **Luca Tufarelli**, co-founding partner di **Ristuccia Tufarelli & Partners**. «Il tema non riguarda solo i soggetti individuati dalle disposizioni comunitarie e nazionali, ma anche i loro fornitori, poiché uno dei punti centrali della disciplina è il controllo dell'intera catena di fornitura, soprattutto quando coinvolge «funzioni essenziali o importanti» (cfr. definizioni di DORA). Anche pmi e studi legali, quindi, sono chiamati a garantire il rispetto di tali obblighi quando collaborano con questi soggetti. Non soltanto sotto il profilo della cybersecurity in senso stretto, ma anche in termini di resilienza, ossia nella capacità di reagire a eventuali blocchi dei sistemi e di ripristinare rapidamente la piena operatività. In questo contesto, il ricorso al cloud e alle protezioni fisiche offerte dalle reti consente di adottare soluzioni scalabili ed economicamente sostenibili anche per gli operatori di dimensioni più contenute. Il nostro studio ha ricevuto una forte e crescente richiesta dalle pmi per effettuare audit integrati che coinvolgessero sia il lato legale che quello squisitamente tecnologico. In tale scenario abbiamo stipulato degli accordi di partnership con primari operatori del mercato della cybersecurity per poter rispondere alla richiesta che non si limiti all'analisi del problema ma che offra anche una soluzione con un approccio integrato che guarda sia alla compliance che all'implementazione operativa».

«Per molte pmi il rischio di un attacco informatico non è, da solo, il principale driver che le spinge ad aumentare i livelli di protezione: l'attivazione di presidi di sicurezza informatica avviene soprattutto per esigenze di compliance, dettate da una normativa sempre più specifica e tecnica», dicono **Simona Lanna**, Dipartimento compliance, media e tecnologia dello **Studio Previti Associazione Professionale** e **Lorenzo Foti**, amministratore delegato di **SP Tech**. «In particolare, in questo momento storico, veniamo coinvolti con frequenza su questioni legate all'adeguamento alla direttiva NIS2 e al regolamento DORA, che richiedono lo sviluppo di un percorso integrato che unisca governance, processi e misure tecniche, evitando un approccio meramente documentale. La soluzione che, dal nostro punto di vista, riesce a semplificare il lavoro di adeguamento per le pmi è ragionare in un'ottica di compliance integrata: tutti i processi devono essere integrati per consentire al cliente di comprendere concretamente le interconnessioni tra le diverse

normative che lo interessano e sviluppare processi agevoli e completi. Il rischio, altrimenti, è quello di produrre tanti documenti che non dialogano tra loro, ingenerando confusione all'interno delle compagini aziendali (soprattutto se meno strutturate) e, di conseguenza, producendo output ad alto effort ma non apprezzati dai clienti. Per questo motivo offriamo ai nostri clienti una consulenza tecnico-legale integrata: partiamo dall'impianto normativo e lo traduciamo in requisiti organizzativi e controlli attuabili, affiancando i referenti aziendali, l'ufficio legale e il personale IT interno con specialisti tecnici coordinati dallo studio. Questo modello crea valore perché trasforma la compliance in misure e azioni concrete e sostenibili (es: risk assessment, interventi sulla contrattualistica, piani e procedure di incident response, audit), riducendo disallineamenti tra ciò che è riportato nella documentazione e l'operatività aziendale. In questo contesto, il ruolo ricoperto dagli studi legali assume una rilevanza determinante anche nel far acquisire ai propri clienti una giusta consapevolezza sui temi legati alla sicurezza informatica, primo passaggio imprescindibile per avviare un progetto di compliance coerente e aderente al contesto e alla realtà aziendale. Questo step preliminare spesso si traduce in un consolidamento anche attraverso l'attività di formazione interna e sensibilizzazione, che sempre più spesso ci viene richiesta dai clienti».

Secondo **Mascia Cassella**, partner dello studio **Masotti Cassella** «il problema è strutturale: se il GDPR era l'unico pilastro della compliance digitale, oggi le normative si stratificano. Sicurezza delle reti, protezione dati, governance dell'AI: ogni adempimento rischia di generare ridondanza documentale. Da qui la necessità di un approccio integrato che permetta di mappare una volta sola controlli e procedure, semplificando la compliance e garantendo coerenza organizzativa. Da sempre noi affianchiamo le imprese nei principali percorsi di compliance normativa e organizzativa oggi con la nuova partnership con Giovanni Ciano, ci siamo specializzati nelle nuove aree di rischio come l'identificazione delle vulnerabilità e la strutturazione di presidi organizzativi e contrattuali. Per le pmi si tratta di integrare competenza tecnica e governance. Il ruolo dell'avvocato evolve: non solo interpretare norme, ma progettare sistemi di compliance che resistano agli attacchi e dimostrino l'adeguatezza delle misure adottate».

— © Riproduzione riservata —

Supplemento a cura
di Roberto Miliacca
rmiliacca@italioggi.it
e Gianni Macheda
gmacheda@italioggi.it