DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

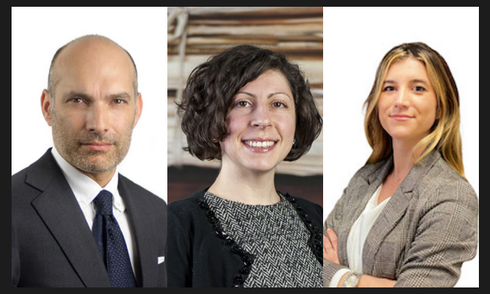
Incidenti di sicurezza e data breach in ambito bancario. Le polizze cyber.

Luglio 2022

Paolo Gallarati, Partner, ADVANT Nctm

Virginia Paparozzi, Managing Associate, ADVANT Nctm

Cecilia Moioli, Associate, ADVANT Nctm



Paolo Gallarati, Partner, ADVANT Nctm

Virginia Paparozzi, Managing Associate, ADVANT Nctm

Cecilia Moioli, Associate, ADVANT Nctm

Paolo Gallarati

Paolo Gallarati è specializzato in Diritto Commerciale e Societario e Fusioni e Acquisizioni e ha maturato una significativa esperienza in complesse operazioni sia italiane che internazionali aventi per oggetto fusioni, acquisizioni, investimenti in Italia e all'estero. Assiste multinazionali e imprese italiane con un focus sui settori TMT, farmaceutico e oil & gas.

1. Incidenti di sicurezza e violazioni di dati personali. Peculiarità del settore bancario

1.1 Premessa

La materia della *cybersecurity*, prima relegata in normative settoriali, dal 2018 circa è al centro dell'intervento del legislatore europeo e italiano.

L'aumento esponenziale degli attacchi informatici e l'acquisita consapevolezza della gravità delle loro conseguenze ai danni dello Stato, delle imprese e delle persone fisiche hanno impresso un'evidente accelerazione alla produzione normativa. Dal GDPR (Regolamento UE 2016/679) al codice europeo delle comunicazioni elettroniche (d.lgs. 259/2003, come da ultimo modificato dal d.lgs. 207/2021), dall'attuazione della Direttiva NIS (con il d.lgs. 65/2018) al perimetro di sicurezza nazionale cibernetica (D.L. 105/2019), gli obblighi in materia di *cybersecurity* riguardano ormai una platea sempre più ampia di soggetti.

In ambito bancario, la gestione degli incidenti di sicurezza informatica è regolata altresì da una disciplina di settore e dagli Orientamenti della Banca d'Italia e dell'Autorità Bancaria Europea.

1.2 Gli incidenti di sicurezza

Un incidente di sicurezza è, in termini generali, un evento che compromette l'integrità, la disponibilità o la riservatezza di sistemi informativi o delle informazioni che detti sistemi elaborano, conservano o trasmettono.

Non vi è né una definizione né una disciplina unitaria di incidente di sicurezza, che sono invece contenute in normative di settore, nazionali ed europee, come, per quanto rileva ai fini del presente contributo, la Direttiva UE 2016/1148 (c.d. Direttiva NIS), recepita in Italia ad opera del d.lgs. n. 65/2018; il D.L. 105/2019, che istituisce il perimetro di sicurezza nazionale cibernetica; e la Direttiva UE 2015/2366 (c.d. Direttiva PSD2), recepita nell'ordinamento nazionale con il d.lgs. 218/2017, relativa ai servizi di pagamento nel mercato interno e applicabile a tutti i fornitori di servizi di pagamento, incluse le banche.

Nello specifico, il decreto attuativo della Direttiva NIS e il decreto istitutivo del perimetro di sicurezza cibernetica impongono l'adozione di misure di sicurezza stringenti a carico di soggetti, pubblici e pri-

vati, che, rispettivamente, svolgono un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali o offrono servizi digitali, ed esercitano una funzione essenziale dello Stato o assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

I soggetti riconducibili a tali categorie, dunque, dovranno garantire *standard* di sicurezza e procedurali più rigorosi rispetto a chi non vi rientra: ciò principalmente in ragione del considerevole impatto che eventuali incidenti informatici potrebbero avere nei settori interessati.

Si segnala, a questo proposito, che tali enti sono individuati, con propri provvedimenti, dalle autorità pubbliche competenti, e che i settori di rilievo includono il settore bancario e delle infrastrutture dei mercati finanziari oltre che, più in generale, quello economico e finanziario.

Venendo alla definizione di incidente di sicurezza in ambito bancario, la Circolare n. 285 del 17 dicembre 2013 della Banca d'Italia (cfr. Parte Prima, titolo IV, Cap. 4, sez. 1, par. 3) definisce l'"*incidente operativo o di sicurezza*" come un "*evento, o serie di eventi collegati, non pianificati dalla banca, che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull'integrità, la disponibilità, la riservatezza e/o l'autenticità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad esempio, frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi)*".

La Banca d'Italia, inoltre, classifica gli incidenti di sicurezza in due categorie: (i) *incidenti cyber*, intesi come incidenti causati da attività volontaria e malevola riguardanti l'accesso, l'uso, la divulgazione, l'interruzione, la modifica o la distruzione non autorizzati delle risorse della banca o incidenti che producono, anche involontariamente, diffusione e/o alterazione di dati riservati della clientela e/o dell'intermediario; oppure (ii) *incidenti operativi,* ossia incidenti derivanti da processi inadeguati o malfunzionanti, persone e sistemi o eventi di forza maggiore. Tale classificazione è contenuta all'interno delle "Istruzioni per la segnalazione di gravi incidenti operativi o di sicurezza", pubblicate dalla Banca d'Italia in data 10 dicembre 2021.

1.3 Le violazioni di dati personali: violazione di riservatezza, disponibilità o integrità

Una violazione di dati personali, o *data breach*, è una particolare tipologia di incidente di sicurezza che coinvolge dati personali, ossia quelle informazioni che identificano, direttamente o indirettamente, una persona fisica (c.d. interessato).

L'art. 4, n. 12, del GDPR definisce "violazione dei dati personali" come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Le violazioni dei dati personali, quindi, possono essere classificate in:

- violazioni della riservatezza, che comportano una divulgazione o un accesso non autorizzato o accidentale ai dati personali;
- violazioni della disponibilità, che comportano la perdita di accesso o la distruzione accidentali o non autorizzate dei dati personali; e
- violazioni dell'integrità, che comportano una modifica non autorizzata o accidentale dei dati personali.

Un esempio di *data breach*, che può comportare una violazione sia della riservatezza che della disponibilità, è dato dal *ransomware*, il cui schema è quello dell'estorsione: gli *hacker* criptano i dati di un'organizzazione e richiedono il pagamento di una somma di denaro (in genere in criptovaluta) per ripristinare l'accesso agli stessi. Spesso l'attacco non si limita alla criptazione dei dati ma consiste anche nella loro esfiltrazione, a cui segue la minaccia di renderli pubblici online in caso di mancato pagamento del riscatto.

Un ulteriore esempio di *data breach*, che comporta di regola una violazione della riservatezza, è dato dal *phishing*. Nella sua versione più semplice, l'*hacker*, spacciandosi per un'altra persona, invia un'email alla vittima chiedendo di fornire informazioni quali numeri di carte di credito o password. La tecnica di *phishing* più sofisticata e che sta prendendo sempre più piede, almeno in Italia, è denominata BEC (*Business Email Compromise*). In genere, in questo caso l'*hacker* sottrae le credenziali di accesso all'ac-

vedi l'articolo online

count email di un dipendente o di un dirigente di un'organizzazione (mediante una normale azione di *phishing* o introducendosi nei relativi sistemi in altro modo); dopodiché, spacciandosi per un apicale chiede a un proprio dipendente di effettuare un pagamento su un certo conto corrente bancario o, spacciandosi per un fornitore, chiede al committente il pagamento dei corrispettivi dovuti su coordinate bancarie diverse da quelle originariamente comunicate dal reale fornitore.

Infine, un esempio di *data breach* che potrebbe comportare la violazione integrità del dato riguarda la perdita di documenti o di dispositivi portatili, nel caso in cui non sia disponibile una copia di *backup*.

1.4 Statistiche sull'incidenza di violazioni di dati personali nel triennio 2019 – 2021

Negli ultimi anni si è registrato un considerevole aumento delle violazioni dei dati personali a danno di imprese italiane ed europee. Secondo l'"*Enisa Threat Landscape 2021*", pubblicato, appunto, dalla European Union Agency for Cybersecurity (ENISA), delle nove categorie di minacce alla sicurezza informatica, nel 2021 è il *ransomware* ad averla fatta da padrone con, a seguire, il *phishing*. In calo, rispetto al 2020, gli incidenti connessi al *malware*.

Come sottolineato dall'ENISA, tra aprile 2020 e luglio 2021 i settori più colpiti da attacchi informatici sono stati la pubblica amministrazione (198 incidenti), i fornitori di servizi digitali (152 incidenti), il settore pubblico in generale (151 incidenti), la sanità (143 incidenti) e il settore finanziario/bancario (97 incidenti).

Per quanto riguarda, nello specifico, le violazioni notificate al Garante per la protezione dei dati personali (di seguito, anche, il "Garante"), l'autorità ha registrato 1.443 casi nel 2019, 1.387 nel 2020, e 2.071 casi nel 2021; nel 2018, invece, i casi erano solo 650 (come emerge, rispettivamente, dalle rispettive relazioni annuali).

Dei provvedimenti pubblicati dall'autorità su questi temi nell'ultimo anno, la quasi totalità ha riguardato azioni accidentali interne (come episodi di erronea trasmissione/condivisione di dati a soggetti non autorizzati); i rimanenti casi, relativi ad azioni intenzionali esterne, hanno riguardato attacchi *ransomware*. Quanto alla tipologia di sanzioni applicate, l'autorità ha principalmente rivolto ai soggetti coinvolti ammonimenti o comminato sanzioni amministrative pecuniarie.

Tra le sanzioni più alte, il Garante ha sanzionato un istituto di credito per l'importo di euro 1.650.000, non per violazioni specifiche degli artt. 33 e 34 del GDPR, ma per non aver adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, circostanza emersa, appunto, nel corso dell'attività istruttoria svolta dall'autorità in relazione a un *data breach*.

1.5 Conseguenze legali derivanti da incidenti di sicurezza o violazioni di dati personali: notifiche, comunicazioni e misure di sicurezza tecniche e organizzative

Nel caso si verifichino incidenti di sicurezza o violazioni di dati personali, il soggetto che li abbia subiti dovrà attivarsi prontamente per adempiere agli obblighi previsti dalla normativa applicabile che, in termini generali, includono la notifica di tali eventi alle autorità competenti e, nei casi più gravi, agli interessati. È inoltre richiesto di adottare prontamente misure di sicurezza tecniche e organizzative adeguate per mitigare gli effetti dell'incidente e prevenire futuri episodi.

Talune imprese, come accade in ambito bancario, possono ricadere nell'ambito applicativo di diverse normative e, pertanto, sono astrattamente soggette a diversi obblighi in materia di sicurezza informatica.

1.5.1 Gli obblighi previsti dal GDPR

In primo luogo, qualora l'incidente di sicurezza abbia ad oggetto dati personali e sia quindi qualificato come violazione di dati ai sensi del GDPR, il titolare del trattamento – ovvero l'ente che determina le finalità e i mezzi del trattamento (per esempio, l'istituto di credito in relazione ai dati personali della propria clientela) – che lo abbia subito è tenuto a conformarsi a due obblighi principali.

Il primo, previsto dall'art. 33 (1) GDPR, è quello di notificare la violazione all'autorità di controllo competente (in Italia, il Garante) entro 72 ore dal momento in cui ne è venuto a conoscenza, salvi i casi in cui sia ammesso procedere attraverso una notifica ritardata, ovvero una notifica a due stadi, preliminare e definitiva; il secondo, previsto dal successivo art. 34 (1) GDPR, è quello di darne comunicazione agli interessati. La notifica all'autorità di controllo è sempre obbligatoria tranne nel caso in cui "sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche". La comunicazione agli interessati è obbligatoria, invece, quando la violazione dei dati personali è

vedi l'articolo online

suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Alla luce di quanto sopra, è evidente che la valutazione dell'esistenza di un rischio (o di un rischio elevato), non appena si viene a conoscenza di una violazione, è fondamentale per comprendere se procedere con la notifica al Garante e con la comunicazione agli interessati oltre che, naturalmente, per adottare misure efficaci per contenere e risolvere la violazione.

A questo riguardo, il Gruppo di lavoro "Articolo 29" (WP29) – i.e. il gruppo di lavoro europeo indipendente che, fino all'entrata in vigore del GDPR, si occupava di questioni relative alla gestione dei dati personali – con le sue "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 (WP250)", successivamente fatte proprie dallo European Data Protection Board (EDPB), elenca e descrive sette fattori di rischio da considerare. In questo contesto, il WP29 richiama, in particolare, il documento di dicembre 2013 "*Recommendations for a methodology of the assessment of severity of personal data breaches*" adottato dall'ENISA, contenente una metodologia per la valutazione della gravità della violazione, quale utile strumento per la predisposizione da parte dei titolari del piano di intervento ai fini della gestione dei *data breach*. Questi fattori includono:

- tipo di violazione;
- natura, carattere "sensibile" e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato;
- caratteristiche particolari del titolare del trattamento;
- numero di persone fisiche interessate.

1.5.2 Gli obblighi previsti dal decreto che recepisce la Direttiva NIS

Il decreto che recepisce la Direttiva NIS, invece, prevede che gli operatori di servizi essenziali e i fornitori di servizi digitali debbano notificare gli incidenti aventi un impatto rilevante sui servizi essenziali al *Computer Security Incident Response Team* (CSIRT), istituito presso l'Agenzia per la Cybersicurezza Nazionale, la quale è designata quale autorità nazionale competente NIS, vigila sull'applicazione della Direttiva NIS e ha poteri ispettivi e sanzionatori in materia.

Le notifiche di tali incidenti devono essere effettuate "senza ingiustificato ritardo", secondo le modalità definite dal CSIRT ed eventualmente da ciascuna autorità NIS di settore con proprie linee guida.

1.5.3 Gli obblighi previsti dalla normativa in materia di perimetro di sicurezza nazionale cibernetica

Analogamente, il DPCM 14 aprile 2021, n. 81, definisce le modalità per la notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici afferenti al perimetro nazionale di sicurezza cibernetica. Esso prevede l'obbligo, per i soggetti inclusi nel perimetro, di notificare al CSIRT gli incidenti di sicurezza aventi impatto sui beni ICT di rispettiva pertinenza, entro 6 ore ovvero entro 1 ora, a seconda della gravità, dal momento in cui i soggetti medesimi ne siano venuti a conoscenza (anche mediante attività di monitoraggio, test e controllo).

1.5.4 Gli obblighi previsti in ambito bancario dalla Direttiva PSD2, dall'Autorità Bancaria Europea e dalla Banca d'Italia

La Direttiva PSD2, infine, prevede che, in caso di grave incidente operativo o relativo alla sicurezza, i prestatori di servizi di pagamento, ivi incluse le banche, debbano notificarlo senza indugio all'autorità competente dello Stato membro di origine del prestatore di servizi di pagamento. Al ricevimento della notifica, l'autorità competente fornisce i dettagli dell'incidente all'Autorità Bancaria Europea (European Banking Authority o EBA) e alla BCE. In attuazione di detta Direttiva, gli obblighi in questione sono contenuti a livello nazionale in all'articolo 6 ter del d.lgs. n. 11 del 27 gennaio 2010, introdotto ad opera dell'art. 2, comma 8 del d.lgs. n. 218 del 15 dicembre 2017, laddove è previsto che "*i prestatori di servizi di pagamento trasmettono alla Banca d'Italia dati statistici sulle frodi connesse agli strumenti e ai servizi di pagamento. La Banca d'Italia definisce le modalità e i termini per l'invio dei dati, tenendo anche conto degli orientamenti dell'ABE. I dati vengono poi trasmessi a ABE e BCE in forma aggregata*". Inoltre, obblighi puntuali di notifica dei "gravi incidenti" ai sensi della Direttiva PSD2 sono contenuti all'interno della già citata Circolare della Banca d'Italia n. 285, aggiornata in seguito all'emanazione della Direttiva PSD2,

nonché delle "Istruzioni per la segnalazione di incidenti operativi e di sicurezza", pubblicate da Banca d'Italia in data 10 dicembre 2021 e della Comunicazione della Banca d'Italia del 29 ottobre 2021, che a sua volta recepisce gli Orientamenti dell'EBA, avente natura di atto normativo di carattere generale vincolante per i destinatari.

In data 10 giugno 2021, infatti, l'EBA ha emanato gli Orientamenti aggiornati in materia di segnalazione dei gravi incidenti ai sensi dell'art. 96 della Direttiva PSD2, che abrogano e sostituiscono i precedenti Orientamenti del 2017. La Banca d'Italia si è conformata a detti Orientamenti dell'EBA con Comunicazione del 29 ottobre 2021.

In particolare, gli Orientamenti dell'EBA stabiliscono criteri per la classificazione degli incidenti operativi o di sicurezza gravi, nonché il contenuto, il formato e le procedure per la comunicazione di questi incidenti alle autorità nazionali. Ai sensi della normativa sopra citata, al fine di verificare la rilevanza e gravità dell'incidente devono essere prese in considerazione soglie qualitative e quantitative, come di seguito evidenziato:

- l'incidente operativo o di sicurezza è reso pubblico e/o può comportare importanti danni reputazionali;
- l'impatto finanziario stimato supera i cinque milioni di euro o il massimo tra lo 0.1 per cento del capitale primario di classe 1 dell'intermediario e 200.000 euro;
- la gestione dell'incidente è soggetta ad un alto livello di *escalation* interna (es. CIO o equivalente);
- l'incidente comporta verosimilmente la violazione di obblighi legali o regolamentari;
- l'incidente operativo o di sicurezza innesca o potrebbe innescare procedure di gestione della continuità operativa o di gestione delle crisi;
- alto impatto delle transazioni interessate;
- il numero degli utenti interessati è maggiore di 50.000 o del 25% del numero totale di utenti del servizio;
- concomitanza di impatti c.d. "minori";
- l'incidente ha un impatto sistemico e può interessare altre istituzioni/organizzazioni;
- l'incidente è comunicato al CERT/CSIRT.

Quanto alle tempistiche per comunicare i "gravi incidenti" alla Banca d'Italia, le già citate "Istruzioni per la segnalazione di incidenti operativi e di sicurezza", pubblicate da Banca d'Italia in data 10 dicembre 2021 prevedono obblighi di segnalazione aventi tempistiche stringenti e differenziate a seconda che l'istituto bancario sia classificato come "banca significativa" ovvero "banca meno significativa", mediante tre tipologie di rapporti: i) un primo report relativo all'incidente, atteso entro due ore (ovvero quattro ore per le "banche meno significative") dal momento in cui esso è stato classificato come "grave"; ii) un secondo report, denominato "report ad interim", inviato quando le regolari operazioni sono state ripristinate e l'attività è tornata alla normalità; iii) un terzo e ultimo report, atteso entro 20 giorni lavorativi dalla chiusura dell'incidente.

Tutte le normative sopra brevemente descritte, inoltre, prevedono l'obbligo a carico delle imprese di adottare misure di sicurezza e organizzative adeguate, determinate, tra l'altro, in funzione della natura delle attività esercitate e dei servizi prestati, della gravità delle conseguenze di eventuali incidenti, nonché, nel caso in cui siano coinvolti dati personali, della natura, oggetto, contesto e finalità del trattamento, dello stato dell'arte e dei costi di attuazione.

Tali misure devono essere identificate e adottate in via generale e preventiva, al fine di garantire la sicurezza dei sistemi informatici utilizzati, nonché prevenire e minimizzare l'impatto di eventuali incidenti di sicurezza; ma misure di sicurezza tecniche e organizzative devono essere identificate e adottate, prontamente, anche al verificarsi degli incidenti in questione, al fine di mitigarne gli effetti negativi e mettere nuovamente in sicurezza i sistemi coinvolti.

Tra le misure di sicurezza segnalate dall'ENISA e dall'EDPB si segnalano, a titolo esemplificativo, l'adozione di meccanismi di crittografia, di autenticazione a fattori multipli e di sistemi *firewall*.

Infine, si riporta l'orientamento del WP29 che ha espressamente affermato che, in via generale, non dovrebbe sussistere un obbligo di notifica nel caso in cui si verifichino le seguenti condizioni (Opinion n. 3/2014): i) la chiave di cifratura non è stata compromessa; ii) sussistenza di una copia di *backup* dei dati; iii) adozione di meccanismi di criptazione dei dati. In aggiunta, è opportuno tenere conto della sussistenza dell'ulteriore condizione consistente nella possibilità di immediato blocco di qualsiasi dispositivo oggetto della violazione, mediante cancellazione irreversibile della memoria del dispositivo non appena questo si colleghi ad una rete, in combinazione con una password OPT fornita all'utente su dispositivi diversi da inserire nel dispositivo violato.

2. Polizze *cyber* e servizi accessori di *data breach management*

2.1 Introduzione

Preliminarmente si evidenzia che il presente contributo non si sofferma sui profili regolatori delle polizze *cyber*, per i quali si rinvia ad un successivo intervento; in questa sede ci si concentrerà, invece, sull'aspetto dei servizi accessori a tali polizze, consistenti nella gestione della violazione del dato, come meglio evidenziato nei successivi paragrafi.

2.2 Servizi di gestione della violazione

L'inosservanza degli obblighi descritti ai paragrafi che precedono può comportare l'applicazione di sanzioni estremamente significative. Solo con riferimento alla violazione degli articoli 33 e 34 del GDPR, le imprese possono andare incontro a sanzioni amministrative pecuniarie fino a 10 milioni di euro o al 2% del fatturato annuo globale dell'azienda, se superiore.

Più in generale, gli incidenti possono esporre i soggetti che li abbiano subiti a danni e costi per la difesa derivanti da reclami o azioni di terzi e in particolare gli interessati dal trattamento dei dati personali, contro tali soggetti e i *service provider* (con cui tali soggetti sono solidalmente responsabili nei confronti degli interessati); danni alla reputazione; costi per le investigazioni di *cybersecurity*, la consulenza e l'attuazione di misure tecniche adeguate per contenere o rimediare alla violazione.

In questo contesto, le polizze assicurative di tipo "*cyber*" (che operano di regola come assicurazioni per la responsabilità civile, nonché come assicurazioni contro i danni), con *focus* specifico sulle violazioni dei dati personali e in materia di *cybersecurity*, rappresentano uno strumento utile per proteggere la propria organizzazione da minacce informatiche offrendo coperture per i danni da interruzione dell'attività, danni reputazionali nonché per i costi sostenuti per le attività di assistenza in sede di rimedio o adempimento agli obblighi conseguenti alle violazioni.

A maggior ragione, possono essere ancora più interessanti per l'assicurato le polizze che includono, oltre alle tradizionali coperture assicurative, anche il servizio accessorio di gestione e assistenza della violazione del dato personale o in generale dell'incidente di sicurezza.

Tali polizze *cyber*, infatti, hanno un approccio esaustivo, prendendo in considerazione la necessità per i soggetti colpiti da incidenti di sicurezza di agire prontamente, al fine di valutare e contenere la violazione, tramite il coinvolgimento e il coordinamento di diversi professionisti.

Il vantaggio di tali polizze per l'assicurato consiste nella possibilità di usufruire del servizio di gestione per effetto della mera vigenza della polizza e quindi anche prima della verifica e della conferma dell'operatività della copertura assicurativa, senza costi ulteriori rispetto al premio già pagato.

Il servizio di gestione si articola nella raccolta delle informazioni relative al sinistro, nell'assistenza all'assicurato in sede di valutazione delle iniziative da porre in essere e nella selezione dei fornitori (*vendors*) i cui servizi siano necessari per porre rimedio alla violazione o adempiere agli obblighi ad essa conseguenti. Il costo dei fornitori non è incluso nel servizio di gestione ma è suscettibile di rimborso ai termini e condizioni della polizza.

2.3 *Vendor services*: legali, negoziali, informativi, comunicativi

La gestione dell'incidente richiede, in generale, l'intervento coordinato di diversi professionisti specializzati. Anzitutto, al fine di valutare la natura dell'incidente e il relativo livello di rischio, nonché per comprendere gli obblighi legali applicabili e svolgere i relativi adempimenti (come la notifica della violazione al Garante e la comunicazione agli interessati), l'intervento di consulenti legali assume carattere di priorità. Contestualmente, è senz'altro necessario coinvolgere risorse specializzate in ambito informatico e in materia di *cybersecurity*. Ciò al fine di investigare prontamente le caratteristiche tecniche

dell'incidente e la sua portata, e porre in essere nel più breve tempo possibile tutte le attività finalizzate, da un lato, a raccogliere gli elementi utili per comprendere la portata dell'incidente e in che misura lo stesso abbia eventualmente impattato sulla sicurezza dei sistemi aziendali in generale, e, dall'altro, a minimizzare l'impatto dell'incidente medesimo e mettere in sicurezza i sistemi in questione.

Vi sono ulteriori consulenti, tuttavia, il cui coinvolgimento può essere essenziale, soprattutto in relazione a determinate violazioni di sicurezza. Per esempio, qualora l'episodio sia stato reso pubblico o possa comunque essere reso noto, la società può valutare – con l'assistenza di agenzie di comunicazione o PR – di predisporre comunicati stampa o comunicazioni analoghe relativi all'incidente, al fine, soprattutto, di gestire il relativo impatto mediatico. Ancora, casi di *ransomware* possono rendere utile l'intervento di consulenti specializzati nella negoziazione del riscatto; si tratta di società, con elevata specializzazione tecnica, che entrano in contatto con gli *hacker* al fine di verificare se la minaccia sia reale (per esempio chiedendo evidenza della possibilità di decriptare i file aziendali oggetto di criptazione e riscatto) e negoziare, appunto, l'importo del riscatto richiesto. Ancora, nel caso in cui i dati aziendali siano stati oggetto di esfiltrazione (o vi sia il rischio che gli stessi siano stati oggetto di esfiltrazione), è possibile dare incarico a società terze di porre in essere attività di monitoraggio del web (c.d. ID o *credit monitoring*) – e in particolare del *dark web* e del *deep web* – al fine di comprendere se i dati siano effettivamente stati resi pubblici, per esempio nel caso di mancato pagamento del riscatto.

Tutti tali fornitori terzi sono di regola parte di un *panel* valutato e approvato dalla società assicurativa che offre le polizze *cyber* in esame, e che possono essere attivati dal soggetto assicurato che abbia subito l'incidente.

Nello specifico, l'assicurato che sia coinvolto in una violazione di sicurezza la notificherà prontamente tramite i canali individuati nella polizza, attivando così il c.d. *breach response management team*, che rappresenta il punto di contatto per l'assicurato e l'assicuratore, coinvolge i fornitori terzi e coordina il loro intervento per la gestione dell'incidente.

3. Conclusioni

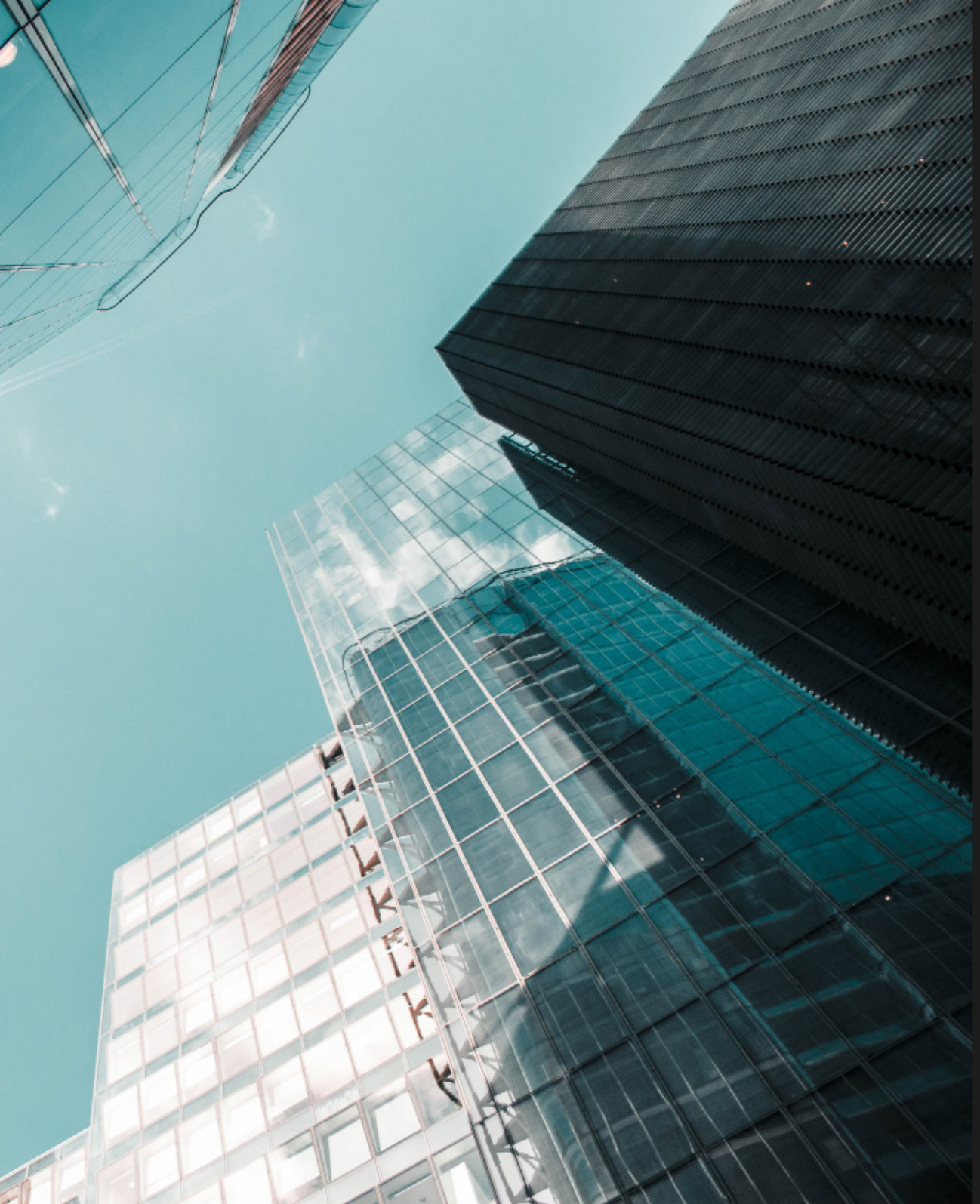
L'incidente di sicurezza è un fenomeno che colpisce tutti i settori economici ed è, come è emerso nel presente contributo, in significativa crescita.

Di fronte all'alto numero di attacchi informatici e, più in generale, incidenti di sicurezza, occorre senz'altro richiamare l'attenzione delle imprese, specialmente in settori così delicati come quello bancario, sull'importanza di proteggere la propria infrastruttura informatica con misure di sicurezza quanto più all'avanguardia, sottoponendole a verifiche e valutazioni periodiche di modo che siano mantenute sempre aggiornate.

Tali misure devono essere accompagnate anche un apparato documentale e procedurale che consenta, da una parte, di fornire evidenza alle autorità pubbliche competenti circa le valutazioni svolte – soprattutto nella misura in cui debbano essere adottate misure adeguate al rischio specifico per la singola organizzazione, dalla stessa determinato – e, dall'altra, consentano di gestire a livello operativo tutti i vari passaggi interni per la gestione dell'incidente di sicurezza. Ciò al fine di poter valutare tempestivamente la natura dell'incidente, da parte delle varie funzioni interne coinvolte per area (come l'area legale, l'area IT, l'area assicurativa), adempiere agli obblighi di legge nella tempistica stabilita e mettere in sicurezza i sistemi informatici coinvolti.

A questo proposito, le polizze *cyber* (in particolare quelle che attengono a servizi di gestione inclusi nel premio, senza essere subordinate a conferma di copertura) possono senz'altro rappresentare uno strumento utile per proteggere la propria organizzazione, grazie anche al loro approccio esaustivo che consente di avere a disposizione un *team* dedicato e specializzato per la gestione delle violazioni di sicurezza, un vero e proprio "pronto intervento" da attivare appena si è colpiti da tali eventi.

In questo contesto sarà possibile gestire in modo efficiente le conseguenze negative degli incidenti di sicurezza che, come si è visto, oltre ai profili sanzionatori possono avere anche un significativo impatto economico, in termini di costi di assistenza per porre rimedio all'incidente o adempiere agli obblighi di legge ad esso conseguenti.



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it