Come affrontare la sfida del rischio cyber

20 settembre 2016

Un rapporto a cura dei Lloyd's

LLOYD'S

Sommario

Sezione 1
Riepilogo

1.1 Riepilogo

Oggi, praticamente ogni azienda, indipendentemente dalle dimensioni o dalla sede, si affida alla tecnologia digitale. Se questo da una parte aiuta a rendere le società più efficienti, a ridurne i costi e ad aprire nuovi mercati, dall'altra le rende anche più vulnerabili agli attacchi cyber. Negli ultimi due anni si sono verificati alcuni importanti incidenti provocati da hacker che hanno spesso causato la divulgazione di informazioni sui clienti e hanno portato alla ribalta la questione della sicurezza informatica.

A rendere il problema ancora più pressante si aggiunge il fatto che, nel 2018, l'Unione Europea introdurrà il General Data Protection Regulation (GDPR), il Regolamento generale sulla protezione dei dati, che stabilirà stringenti requisiti per qualsiasi società che gestisca i dati di consumatori europei.

I Lloyd's – il centro globale per l'assicurazione cyber – ha commissionato questo sondaggio per scoprire cosa stanno facendo le aziende europee per affrontare la sicurezza informatica e come si stanno preparando per il GDPR.

Il sondaggio ha coinvolto 346 vertici aziendali presso importanti società (con fatturato superiore a 250 milioni di €) in tutta Europa. Gli intervistati occupano posizioni quali: Chief Executive Officer (CEO); Chief Financial Officer (CFO); Chief Operating Officer (COO); Chief Information Officer (CIO); Chief Technology Officer (CTO); Chief Risk Officer (CRO); e giurista d'impresa.

La maggior parte delle grandi aziende europee ha subito una violazione dei dati negli ultimi cinque anni ma non teme che tale evento possa ripetersi.

- Il 92% degli intervistati ha dichiarato che la loro azienda è stata vittima di una violazione dei dati negli ultimi cinque anni, eppure solo il 42% degli intervistati teme che l'evento si ripeta in futuro.

Il rischio cyber ha recentemente acquisito una maggiore importanza nell'ordine del giorno dei consigli di amministrazione: ora infatti è il CEO, e non il CIO, a gestire la sicurezza informatica.

- I piani per la protezione dei dati e per la gestione di un'eventuale violazione ora sono gestiti dai CEO nella maggior parte delle aziende (54%) coinvolte nel sondaggio. Per contro, i CIO gestiscono il processo decisionale solamente nel 10% delle aziende. Questa è la conseguenza di numerosi incidenti cyber importanti che hanno coinvolto aziende in tutto il mondo, molti dei quali hanno avuto un impatto significativo sul fatturato o sul valore azionario e, in alcuni casi, hanno anche portato alle dimissioni dei vertici aziendali.

La consapevolezza del Regolamento generale sulla protezione dei dati sembra essere elevata, ma la comprensione delle sue implicazioni è molto più ridotta, il che potrebbe avere delle conseguenze molto gravi.

- Il 97% degli intervistati ha sentito parlare del GDPR, ma solo il 7% ha dichiarato di conoscerlo "molto bene"; il 57% ha detto di sapere "poco" o "niente" del nuovo regolamento, nonostante le gravi conseguenze finanziarie e legali di un'eventuale mancata conformità alle sue regole.

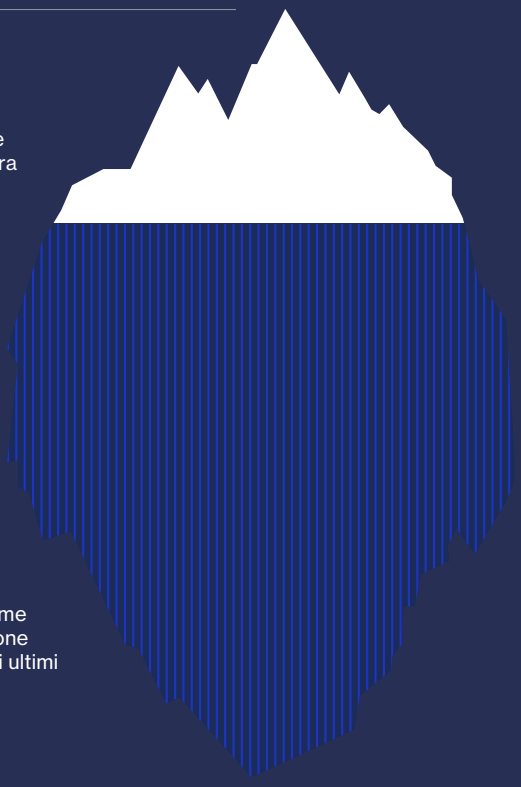
- Più della metà delle aziende coinvolte nel sondaggio è consapevole del fatto che il GDPR potrebbe significare per loro un'investigazione da parte dell'ente regolatore (64%), sanzioni pecuniarie (58%), conseguenze sul valore azionario (57%) e sulla loro reputazione (52%), ma solo il 13% ha ritenuto di poter perdere la clientela.

1.2 Conclusione

Le aziende europee si trovano ad affrontare uno scenario relativo alle minacce cyber che è in continua evoluzione. L'introduzione del GDPR accrescerà l'attenzione sulla sicurezza dei dati in quanto gli enti preposti, gli azionisti e i clienti lo useranno per rendere le aziende responsabili rispetto all'introduzione di più elevati standard di sicurezza informatica. Collaborando a stretto contatto con consulenti preparati quali avvocati, esperti di sicurezza informatica e assicuratori, le aziende possono comprendere meglio i rischi che devono affrontare e contribuire a mitigarli al fine di proteggere i loro bilanci.

42%

aziende preoccupate per una futura violazione dei dati



92%

aziende vittime della violazione dei dati negli ultimi cinque anni

97%

aziende che hanno sentito parlare del nuovo regolamento dell'UE (GDPR)

57%

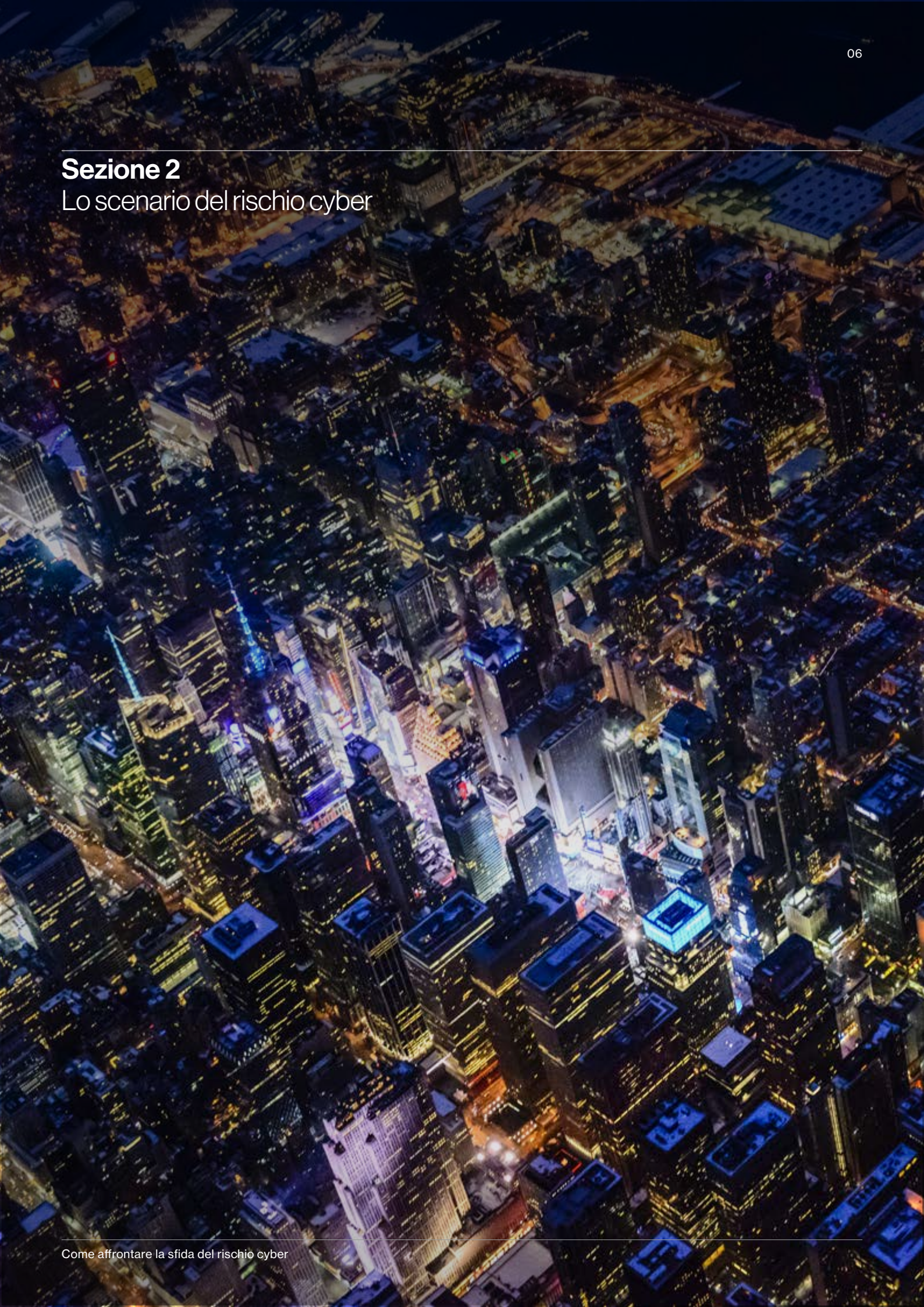
aziende che hanno una conoscenza scarsa o nulla riguardo al nuovo regolamento dell'UE (GDPR)

Come può aiutare un'assicurazione cyber

- Secondo questo sondaggio, il 73% dei dirigenti d'azienda ha una conoscenza limitata dell'assicurazione cyber e il 50% non sa che è disponibile una copertura cyber per le violazioni dei dati.
- L'assicurazione cyber non solo copre la perdita finanziaria dopo un attacco cyber, ma offre anche la consulenza di esperti per migliorare la sicurezza e un supporto sul campo durante il periodo della crisi.
- Collaborare fin dall'inizio con sottoscrittori che comprendono questo rischio costituirà un vantaggio per la strategia di sicurezza di un'azienda. I sottoscrittori possono aiutare le aziende a identificare i rischi e i loro punti vulnerabili, riducendo quindi la probabilità di una violazione.
- Tutto questo contribuisce a proteggere i bilanci dell'azienda, oltre a migliorare gli standard di sicurezza informatica e di mitigazione del rischio nell'intero settore.

Visitate www.lloyds.com/cyber

Sezione 2
Lo scenario del rischio cyber



2.1 Il rischio cyber è in aumento

Oggi, praticamente ogni azienda, indipendentemente dalle dimensioni o dalla sede, si affida alla tecnologia digitale. I retailer, le società di servizi finanziari, le aziende della grande distribuzione adesso usano tutti le tecnologie digitali per gestire i loro affari, monitorare il magazzino, progettare i prodotti e archiviare i dati dei clienti.

Se questo da una parte aiuta a rendere le aziende più efficienti, a ridurne i costi e ad aprire nuovi mercati, dall'altra le rende anche più vulnerabili agli attacchi cyber.

Per questo motivo la sicurezza informatica ha assunto un'importanza notevole per le aziende. Il rischio cyber ora viene considerato una minaccia che ciascuna azienda deve valutare, mitigare e gestire, allo stesso modo degli altri rischi tradizionali come i danni alla proprietà, il terrorismo e i disastri naturali.

La maggiore consapevolezza dei rischi informatici tra le aziende è il risultato di alcuni incidenti importanti che si sono verificati in tutto il mondo negli ultimi anni. Il più recente e famoso attacco cyber avvenuto nel Regno Unito ha coinvolto l'azienda di telecomunicazioni TalkTalk nell'autunno 2015. In altre parti d'Europa, ci sono stati attacchi contro la stazione televisiva francese TV5 Monde, il sistema di controllo del traffico aereo svedese, le compagnie petrolifere ed energetiche norvegesi e un'acciaieria tedesca, per citarne solo alcuni. Negli Stati Uniti, una serie di incidenti informatici ha dominato le pagine dei giornali dal 2014, tra cui attacchi contro Sony, Target, Home Depot ed Experian.

Di conseguenza, il mercato dei Lloyd's, che ha lanciato la prima polizza di assicurazione cyber 10 anni fa, ha assistito alla rapida crescita dell'offerta di coperture cyber. Ora il mercato dei Lloyd's conta ben 65 assicuratori in grado di offrire coperture cyber, con una capacità complessiva di 300 milioni di sterline. Con un giro d'affari pari a un quarto del mercato assicurativo cyber globale, i Lloyd's sono pertanto il centro globale per questo tipo di assicurazione.

Questo rapporto, preparato sulla base di un sondaggio che ha coinvolto 346 vertici di importanti società in tutta Europa, analizza il modo in cui i business leader stanno affrontando la sfida della sicurezza informatica e che cosa stanno facendo per garantire che le loro organizzazioni siano pronte in caso di un attacco cyber.

Il rapporto esamina anche il livello di preparazione delle imprese europee riguardo all'applicazione del regolamento UE sulla protezione generale dei dati (GDPR), che dovrebbe entrare in vigore nel 2018. Questo nuovo regolamento rafforzerà considerevolmente la normativa esistente e le responsabilità correnti riguardo alle modalità di elaborazione e salvaguardia dei dati dei consumatori adottate dalle aziende. Introduce inoltre una serie di requisiti per le imprese vittime di una violazione dei dati, come l'obbligo di segnalare una violazione informatica entro 72 ore dal fatto per non rischiare sanzioni di elevata entità.

Questo rapporto si concentra su un solo tipo di incidente cyber: la violazione dei dati. Questo perché la protezione dei dati riservati dei clienti – soprattutto se di natura finanziaria o medica – è considerata una priorità per la maggior parte delle aziende. I dati rappresentano la loro principale risorsa digitale e, di conseguenza, l'obiettivo della maggior parte degli attacchi cyber.

2.2 Violazioni dei dati

In quale misura la violazione dei dati costituisce un problema per le aziende europee oggi? Per quantificare la dimensione del problema, nel sondaggio abbiamo chiesto agli intervistati se la loro organizzazione avesse subito una violazione dei dati.

Il 92% degli intervistati ha dichiarato che la loro azienda aveva subito una violazione dei dati negli ultimi cinque anni, mentre il 3% ha dichiarato che l'avevano "evitata per poco". Solo il 5% ha dichiarato di non aver subito una violazione dei dati o di non esserne al corrente.

Quali delle seguenti dichiarazioni riflette meglio l'esperienza della sua azienda per quanto riguarda la violazione dei dati negli ultimi 5 anni:

Base: Totale degli intervistati (346): Regno Unito (100) Francia (31) Germania (34) Italia (30) Spagna (30) Paesi Bassi (31) Norvegia (30) Danimarca (30)

2.3 Minacce interne ed esterne

Le violazioni dei dati possono essere il risultato di diversi metodi di attacco cyber, alcuni altamente sofisticati e dolosi, altri relativamente innocenti o accidentali. Nel sondaggio abbiamo chiesto quale tipo di minaccia preoccupa di più le aziende.

Le categorie di minacce cyber sono "interne" o "esterne". Le minacce interne tipicamente sono quelle che hanno origine nell'azienda stessa, o in seguito a un errore umano, come lo smarrimento o il furto di informazioni e attrezzature, o per l'azione di un dipendente disonesto che provoca intenzionalmente una fuga di informazioni confidenziali. Le minacce esterne tendono a essere più hi-tech e comprendono tecniche come hacking, phishing, ransomware e malware (vedi il glossario qui di seguito).

Il sondaggio ha scoperto che la maggior parte delle aziende è più preoccupata per le minacce esterne piuttosto che per quelle interne. Le minacce interne che preoccupano maggiormente le aziende secondo il nostro sondaggio sono di tipo low-tech e il 42% degli intervistati ha dichiarato che la preoccupazione principale riguarda lo smarrimento fisico dei documenti cartacei. La stessa percentuale di intervistati ha anche indicato come minaccia chiave la deliberata violazione delle informazioni da parte di un dipendente.

La minaccia esterna che desta maggior preoccupazione è l'attacco di hackers. Metà (51%) delle aziende intervistate si è detta preoccupata per un potenziale attacco di hackers a scopo di lucro, mentre il 46% ha dichiarato di temere un attacco di hackers per motivi politici. Il 41% ha indicato gli attacchi di hackers da parte di un concorrente come una minaccia importante.

Non sorprende che l'hacking sia la minaccia principale se si considerano le recenti importanti violazioni di dati. TalkTalk, Sony e Home Depot sono solo alcune delle società che sono recentemente cadute vittime di attacchi cyber. Mentre la vera motivazione di questo tipo di incidenti è spesso incerta, gli attacchi di questa natura possono essere usati per rubare le informazioni sui clienti per poi rivenderle al miglior offerente.

Ci possono anche essere motivazioni politiche, soprattutto per quelle aziende che operano in settori sensibili da un punto di vista geopolitico, come quello energetico o delle risorse naturali. Gruppi di hacker disonesti con obiettivi politici specifici attaccano le organizzazioni individuali con sempre maggior frequenza. Se è vero che è difficile misurare con precisione il livello di spionaggio aziendale, il fatto che un attacco di hackers da parte dei concorrenti sia terzo nella lista delle preoccupazioni dei dirigenti suggerisce che viene considerato come una grave minaccia.

Glossario delle minacce cyber

- Hacking – la ricerca e lo sfruttamento delle debolezze di un sistema informatico o di una rete, di solito a scopo di lucro
- Phishing – il tentativo di ottenere informazioni sensibili fingendosi una persona o un'organizzazione di fiducia in un'e-mail
- Whaling – un attacco di phishing il cui perpetratore si finge un alto dirigente, spesso un CEO
- Malware – (abbreviazione del termine inglese "malicious software") si riferisce a qualsiasi software utilizzato per interrompere le operazioni di computer, raccogliere informazioni sensibili o accedere ai sistemi informatici privati
- Ransomware – un tipo di malware che colpisce provocando problemi di funzionamento ad un computer e richiede il pagamento di un riscatto per ripristinarne la piena funzionalità.

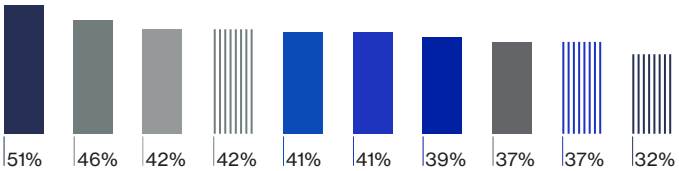
51%

Il 51% degli intervistati è preoccupato della possibilità di subire un attacco di hackers a scopo di lucro

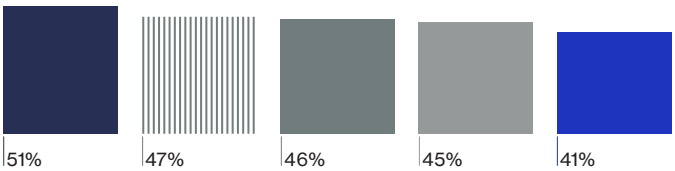
2.3 Minacce interne ed esterne

- Attacchi di hackers – a scopo di lucro
- Attacchi di hackers – da parte di un concorrente
- Attacchi di hackers – per motivazioni politiche
- Errore umano/divulgazione accidentale
- Phishing
- Smarrimento, smaltimento o furto dell'attrezzatura
- Ransomware
- Malware
- Perdita fisica di documenti cartacei o dispositivi non elettronici
- Deliberata violazione delle informazioni da parte di un dipendente

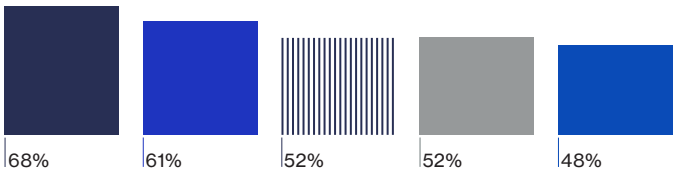
Totale



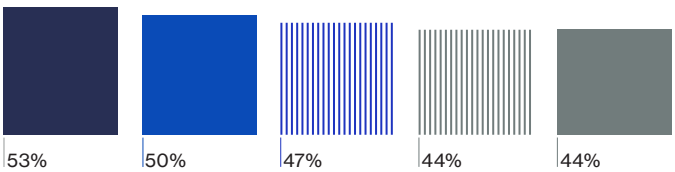
Regno Unito



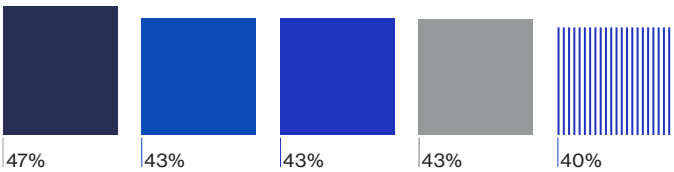
Francia



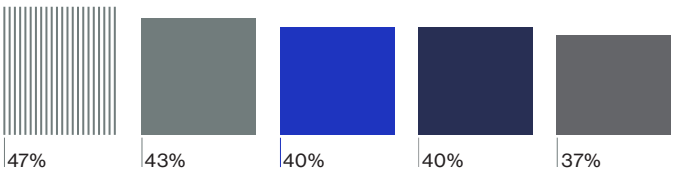
Germania



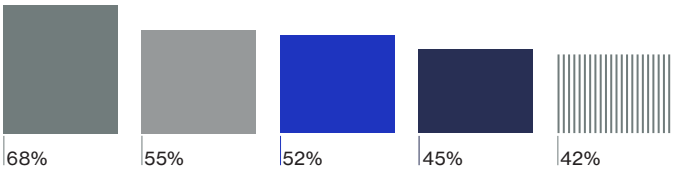
Italia



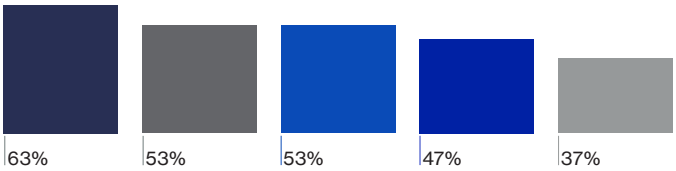
Spagna



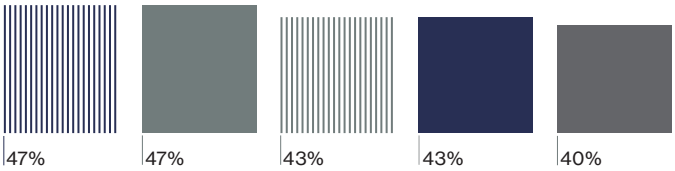
Paesi Bassi



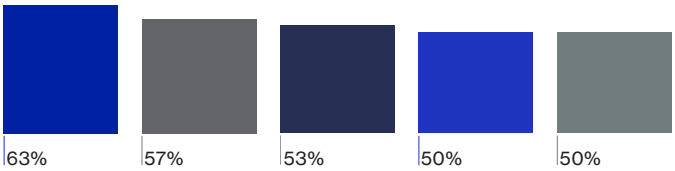
Norvegia



Svezia



Danimarca



Base: Totale degli intervistati (346): Regno Unito (100) Francia (31) Germania (34) Italia (30) Spagna (30) Paesi Bassi (31) Norvegia (30) Danimarca (30)

2.4 Un'errata percezione della sicurezza informatica

Nonostante il 92% delle aziende abbia subito una violazione di dati negli ultimi cinque anni, solo il 42% degli intervistati ha espresso preoccupazione per una futura violazione.

92%

Il 92% ha subito una violazione dei dati

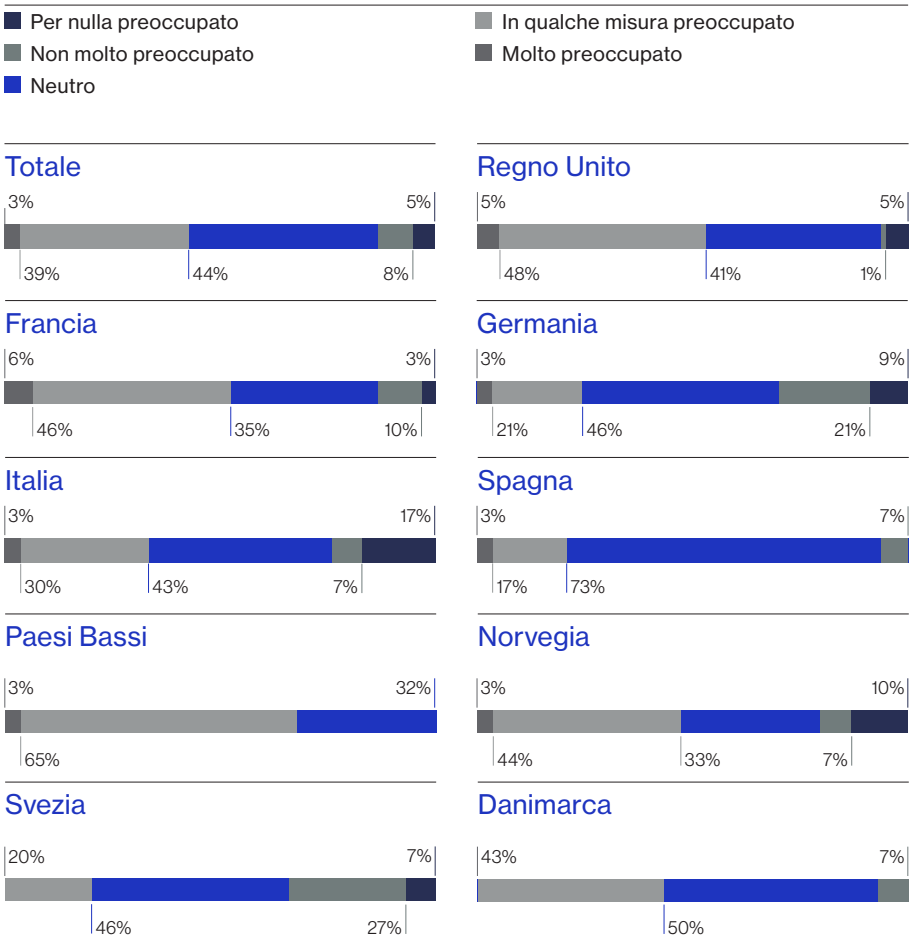
42%

Il 42% appare preoccupato per una futura violazione dei dati

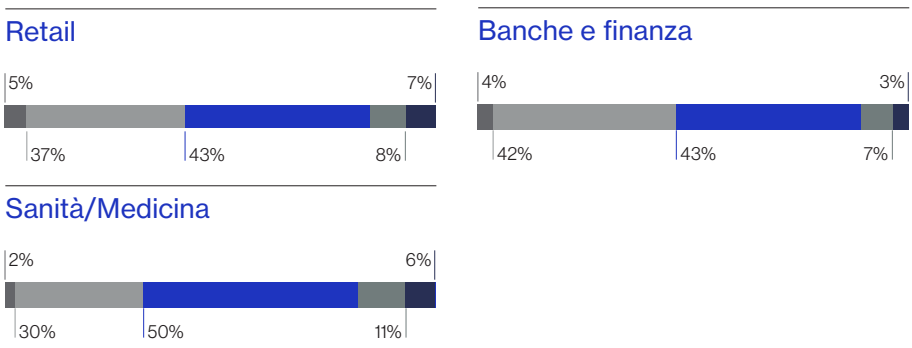
I risultati variano leggermente da settore a settore. Le aziende di servizi finanziari tendono a essere le più preoccupate per un'eventuale violazione (46%), il che è comprensibile se si considera il volume di informazioni sensibili che detengono sui loro clienti. La aziende del settore sanitario sono meno preoccupate (32%), il che è piuttosto sorprendente, se si considera che i dati medici sono più preziosi e che, come tali, sono sempre più ricercati dagli hacker.

Secondo questi risultati o le aziende hanno fiducia nelle misure di sicurezza informatica che hanno adottato o sono noncuranti della loro resilienza agli attacchi cyber. Qualunque sia la risposta, il fatto è che la tecnologia adottata dagli attacchi cyber è in continua evoluzione, rendendo quasi impossibile organizzare una protezione valida al 100% per le aziende. Se le aziende non prendono seriamente la sicurezza informatica, saranno vulnerabili ad attacchi cyber in futuro.

Esprima il suo livello di preoccupazione per un'eventuale futura violazione dei dati ai danni della sua azienda usando una scala da 1 a 5, dove 1 indica "per nulla preoccupato" e 5 indica "molto preoccupato".



Base: Totale degli intervistati (346): Regno Unito (100) Francia (31) Germania (34) Italia (30) Spagna (30) Paesi Bassi (31) Norvegia (30) Danimarca (30)



Base: Totale degli intervistati (346): Retail (109) Banche e Finanza (95) Sanità / Medicina (90)

Sezione 3
Preparazione e risposta

3.1 Se manca la preparazione...

Come discusso nel capitolo precedente, il 92% delle imprese ha subito una violazione dei dati negli ultimi cinque anni. Il sondaggio ha chiesto agli intervistati quale pensavano fosse il loro livello di preparazione in caso si ripetesse un tale incidente. Alle aziende è stato chiesto di descrivere la loro preparazione per affrontare una violazione in base a tre criteri:

1. Organizzazione di una risposta coordinata alla crisi: per esempio, comunicare la notizia ai clienti e aggiornare i sistemi IT.
2. Gestione del danno reputazionale: per esempio, attraverso pubbliche relazioni, pubblicità e altre attività di marketing.
3. Implicazioni normative: per esempio, cooperare nell'ambito di un'investigazione o rispondere ai cambiamenti imposti dal regolamento.

93%

Il 93% delle imprese dicono di essere "preparate" o "molto preparate" per organizzare una risposta coordinata alla crisi

89%

L'89% ha detto la stessa cosa per quanto riguarda la gestione del danno reputazionale

87%

L'87% sulla gestione delle implicazioni normative

La maggior parte delle imprese avrà adottato processi e procedure per far fronte agli incidenti cyber; questo non significa però che siano pienamente preparate. Molte aziende si concentrano sullo sviluppo di un piano di risposta che stabilisce che cosa faranno nel caso di una violazione dei dati, ma c'è tutta una serie di misure, sia precedenti che posteriori alla violazione, che devono essere implementate perché un'organizzazione sia davvero pienamente preparata.

Le aziende dovrebbero garantire che i loro sistemi siano rigorosamente testati e convalidati dall'esterno prima di potersi sentire sicure del proprio livello di preparazione. Anche allora, è essenziale che rimangano costantemente vigili e aggiornino regolarmente i loro piani per tenere il passo con le nuove minacce.

3.2 Chi si prende la responsabilità?

La sicurezza dei dati una volta era interamente affidata al reparto IT. Oggi, l'importanza della sicurezza dei dati è tale che è salita di livello nelle priorità del top management.

Questo cambiamento è avvenuto molto rapidamente. Secondo il sondaggio Marsh dell'anno scorso [2015], solo il 17% delle imprese europee indicava il rischio cyber come uno dei primi cinque rischi aziendali, mentre il 25% non lo considerava affatto. Quasi due terzi delle imprese (65%) avevano dichiarato che la responsabilità primaria per i rischi informatici nelle loro organizzazioni risiedeva presso gli uffici IT, mentre solo l'11% aveva dichiarato che ne era responsabile il consiglio di amministrazione.

Secondo il sondaggio dei Lloyd's, condotto nove mesi più tardi, i consigli di amministrazione europei sono ora molto più coinvolti per fronteggiare meglio il rischio cyber.

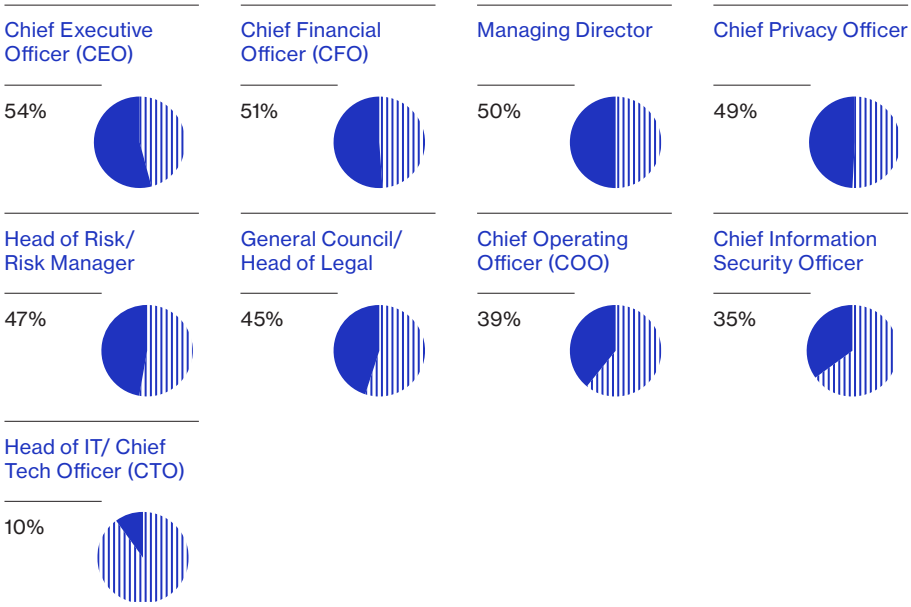
Agli intervistati è stato chiesto chi all'interno della loro società aveva preso le decisioni sulla protezione contro la violazione dei dati e per la pianificazione in caso tale evento si verificasse. La maggioranza degli intervistati (54%) ha detto che era il CEO. Solo una percentuale molto più bassa di intervistati ha dichiarato che tali decisioni erano state prese dai dirigenti preposti agli uffici IT: solo il 35% ha detto che il Chief Information Security Officer aveva gestito questo rischio nella loro azienda, e solo il 10% ha citato il CIO o CTO per tale ruolo. Nel 96% dei casi, un rappresentante del top management è stato citato come la figura primaria.

È probabile che la recente serie di violazioni ampiamente pubblicizzate e le loro conseguenze – crollo del valore azionario, costi, contenzioso legale – abbia spinto i CEO a sviluppare rigorose strategie di sicurezza informatica. Gli azionisti si aspettano che il CEO si assuma la responsabilità per la sicurezza informatica e che faccia tutto il possibile per mitigare i rischi che alla fine hanno un impatto sulla performance finanziaria della società.

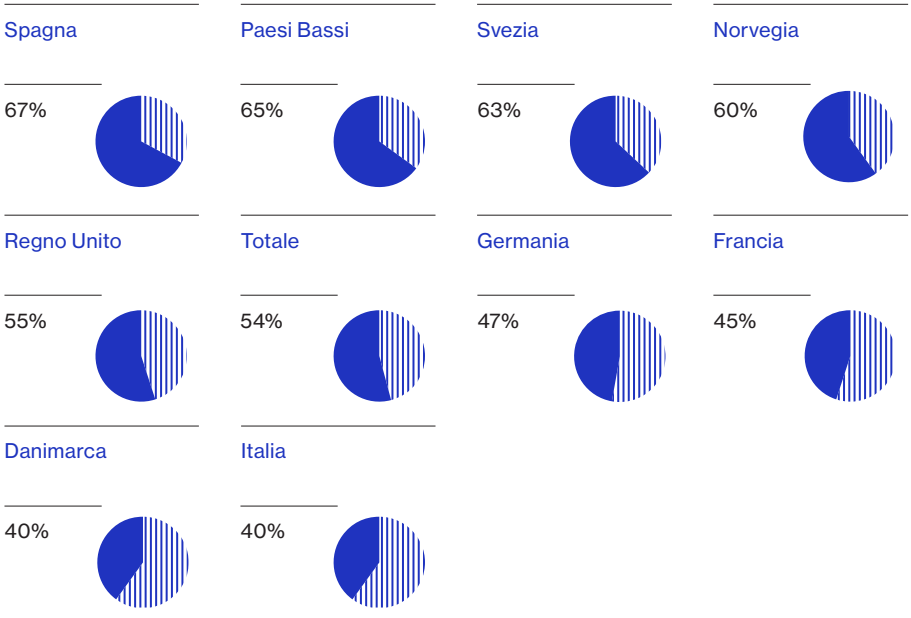
Anche i CEO hanno un ovvio motivo per prendere sul serio la questione, dal momento che il loro posto di lavoro è direttamente collegato alle conseguenze di violazioni della sicurezza informatica. I CEO del retailer statunitense Target e della società aerospaziale austriaca FACC hanno entrambi perso il lavoro per motivi legati agli incidenti informatici.

È incoraggiante vedere che, come dimostra il sondaggio, sempre più CEO stanno prendendo sul serio i rischi informatici. I prossimi cambiamenti del regolamento UE dovrebbero portare la questione alla ribalta per le aziende in tutta Europa.

Chi è responsabile, all'interno della sua azienda, per le decisioni sulla protezione contro la violazione dei dati e per la pianificazione in caso tale evento si verificasse?



Chief Executive Officer (CEO)



Base: Totale degli intervistati (346):

Sezione 4
Comprendere il GDPR

4.1 Una nuova era per la normativa cyber

L'introduzione del Regolamento generale sulla protezione dei dati (GDPR) nel 2018 trasformerà la normativa informatica in Europa. Questo avrà anche implicazioni significative per le aziende in tutto il mondo, molte delle quali non sono ancora completamente chiare alle aziende stesse.

Il GDPR sancisce i diritti fondamentali alla privacy dei consumatori, come "il diritto di essere dimenticati" e il diritto di opporsi alle attività di profilazione, che le imprese devono rispettare.

È importante sottolineare che il GDPR non si applica solo alle aziende degli Stati membri dell'UE. Qualsiasi azienda che offra beni e servizi ai cittadini dell'Unione europea, o che ne monitori il comportamento, deve rispettare le sue regole. Ciò significa che molte aziende degli Stati Uniti e dell'Asia, per esempio, rientreranno nell'ambito giurisdizionale del GDPR.

Chiaramente il GDPR non può essere ignorato. Questo sondaggio ha chiesto agli intervistati come si stavano preparando alla sua introduzione, che avrà luogo tra meno di due anni.

Cos'è il GDPR?

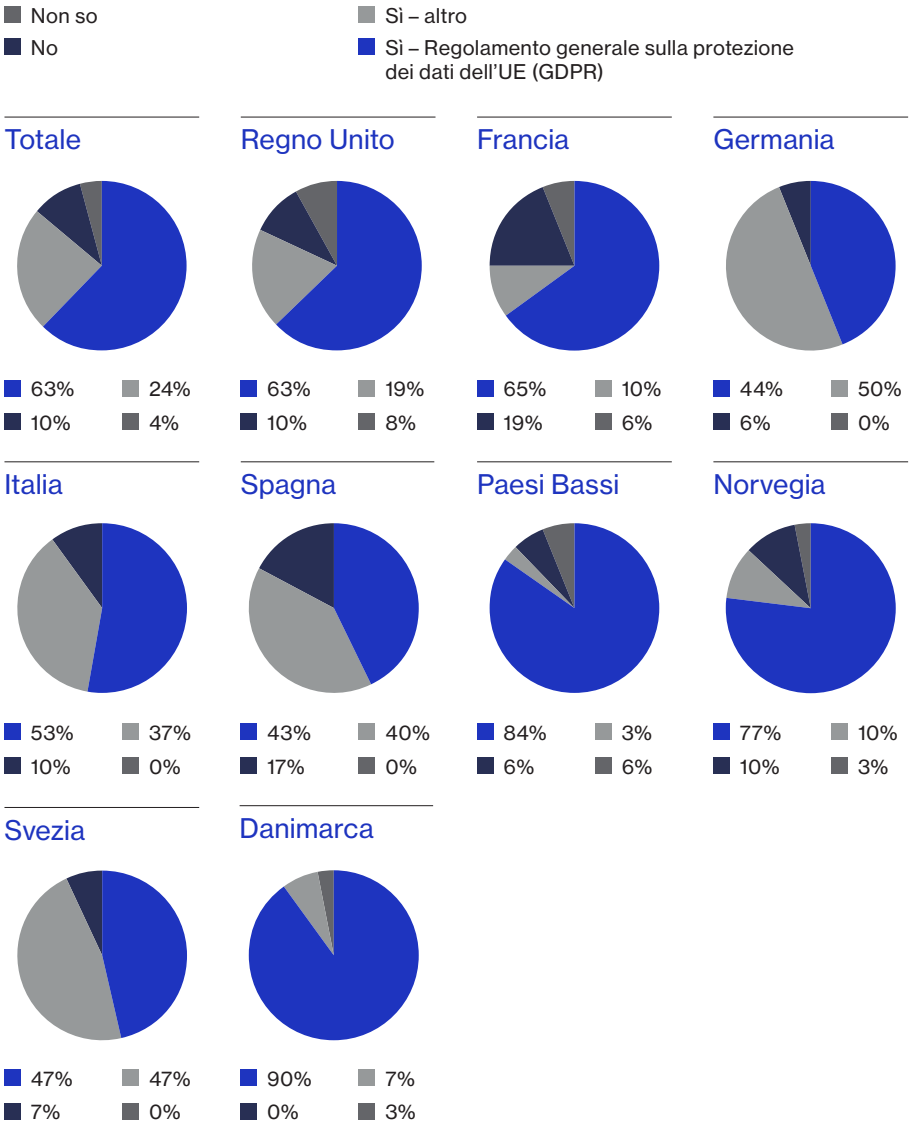
- Il Regolamento generale sulla protezione dei dati (GDPR) è un componente della legislazione comunitaria che armonizza le diverse leggi di protezione dei dati in tutta l'Europa e porta la legislazione dell'UE al passo con le possibilità tecnologiche dell'epoca dei Big Data
- In particolare, impone alle aziende di segnalare le violazioni della sicurezza al proprio ente regolatore entro 72 ore e di avvertire i cittadini colpiti senza alcun ritardo
- Sancisce multe fino al 4% del fatturato annuo mondiale o a 20 milioni di euro, se tale importo è superiore, per le aziende vittime di una violazione dei dati. Anche gli individui possono richiedere un risarcimento da parte delle organizzazioni per l'eventuale perdita finanziaria o disagio che abbiano subito.
- Entrerà in vigore il 25 maggio 2018 in tutti gli Stati membri dell'UE, ma riguarda tutte le aziende che svolgono affari con i cittadini dell'UE, indipendentemente da dove abbiano sede.

4.2 Consapevolezza e comprensione

Considerata l'importanza del GDPR, il fatto che è stato annunciato pubblicamente nel 2012 e la sua imminente implementazione, ci si aspetterebbe che le aziende avessero dei piani già organizzati, pronti per essere messi in atto. L'indagine ha rivelato un quadro molto più variegato.

Dal sondaggio risulta che la maggior parte delle aziende è consapevole del GDPR. Quando è stato chiesto ai dirigenti se erano a conoscenza di eventuali nuove disposizioni che avrebbero potuto influenzare lo scenario relative alla protezione dei dati, il 63% ha citato il GDPR. Il 24% ha fatto riferimento ad altre norme, che potrebbero includere cambiamenti a livello nazionale per la protezione dei dati.

È consapevole del nuovo regolamento o di eventuali cambiamenti nel regolamento relativo alla protezione dei dati?



Base: Totale degli intervistati (346): Regno Unito (100) Francia (31) Germania (34) Italia (30) Spagna (30) Paesi Bassi (31) Norvegia (30) Danimarca (30)

4.2 Consapevolezza e comprensione

Quando si è specificato il GDPR, il 97% delle imprese ha dichiarato di averne sentito parlare. Tuttavia, dietro a questo dato si nascondono livelli di comprensione approfondita molto più bassi. Solo il 7% degli intervistati, infatti, ha dichiarato di conoscere "molto bene" il GDPR, mentre più della metà (57%) ha ammesso di saperne "poco" o "niente". Considerata l'importanza del GDPR per le aziende, questo dato rivela una conoscenza sorprendentemente scarsa dello stesso.

Quale è il suo livello di conoscenza del Regolamento sulla protezione generale dei dati (GDPR)?

- Conosco molto bene il GDPR dell'UE
- Ho sentito parlare del GDPR dell'UE ma non ne conosco i dettagli
- Non ho mai sentito parlare del GDPR dell'UE e non lo conosco affatto
- Ho una conoscenza professionale del GDPR dell'UE
- Ho sentito parlare del GDPR dell'UE ma non ne conosco i dettagli

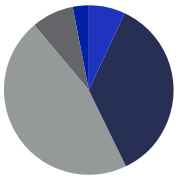
97%

Il 97% degli intervistati ha sentito parlare del GDPR

57%

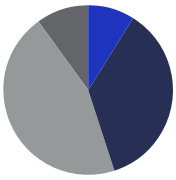
Il 57% ha ammesso di sapere "poco" o "niente" del GDPR

Totale



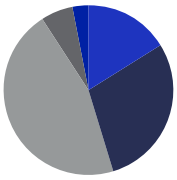
7% | 36% | 46% | 8% | 3%

Regno Unito



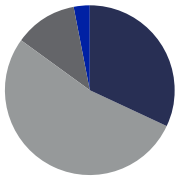
9% | 36% | 45% | 10% | 0%

Francia



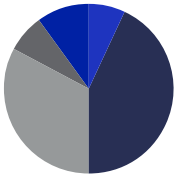
16% | 29% | 45% | 6% | 3%

Germania



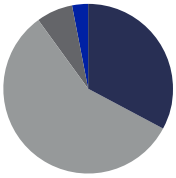
0% | 32% | 53% | 12% | 3%

Italia



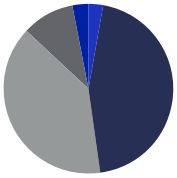
7% | 43% | 33% | 7% | 10%

Spagna



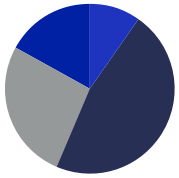
0% | 33% | 57% | 7% | 3%

Paesi Bassi



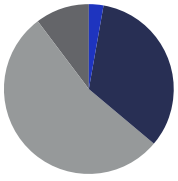
3% | 45% | 39% | 10% | 3%

Norvegia



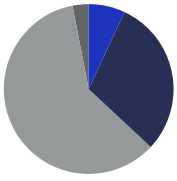
10% | 47% | 27% | 0% | 17%

Svezia



3% | 33% | 53% | 10% | 0%

Danimarca



7% | 30% | 60% | 3% | 0%

Il regolamento GDPR prevede, per esempio, la possibilità di sanzioni pecuniarie consistenti nei confronti delle aziende che non sono conformi (fino al 4% del fatturato globale). Stabilisce, inoltre, più elevati standard di trasparenza sull'utilizzo dei dati dei clienti, sulla sicurezza dei sistemi di tutela e sui tempi entro i quali i clienti devono essere avvertiti di un'eventuale violazione. Nessuno di questi requisiti sono semplici da rispettare: richiederanno tempo, investimenti e impegno.

Questo risultato suggerisce che le aziende devono impegnarsi maggiormente per capire l'impatto effettivo del regolamento GDPR sulla loro organizzazione e le proprie responsabilità.

Base: Totale degli intervistati (346): Regno Unito (100) Francia (31) Germania (34) Italia (30) Spagna (30) Paesi Bassi (31) Norvegia (30) Danimarca (30)

4.3 Riconoscere le implicazioni per le aziende

Nonostante la maggioranza dei vertici aziendali abbia ammesso di sapere ben poco del GDPR, il 66% di loro ha dichiarato di aver compreso le implicazioni del GDPR nel caso di una violazione di dati nei confronti della loro azienda.

Approfondendone gli aspetti, gli intervistati si sono concentrati su due aree chiave: impatti normativi e finanziari. In cima alla lista figura l'investigazione da parte degli enti preposti, citata dal 64% delle aziende come l'implicazione più probabile. Subito dopo compaiono le sanzioni pecuniarie o multe (58%) seguite dall'impatto sui profitti o sul valore azionario (57%). Solo il 13% si è detto preoccupato della perdita di clientela.

64%
controlli da parte degli enti preposti

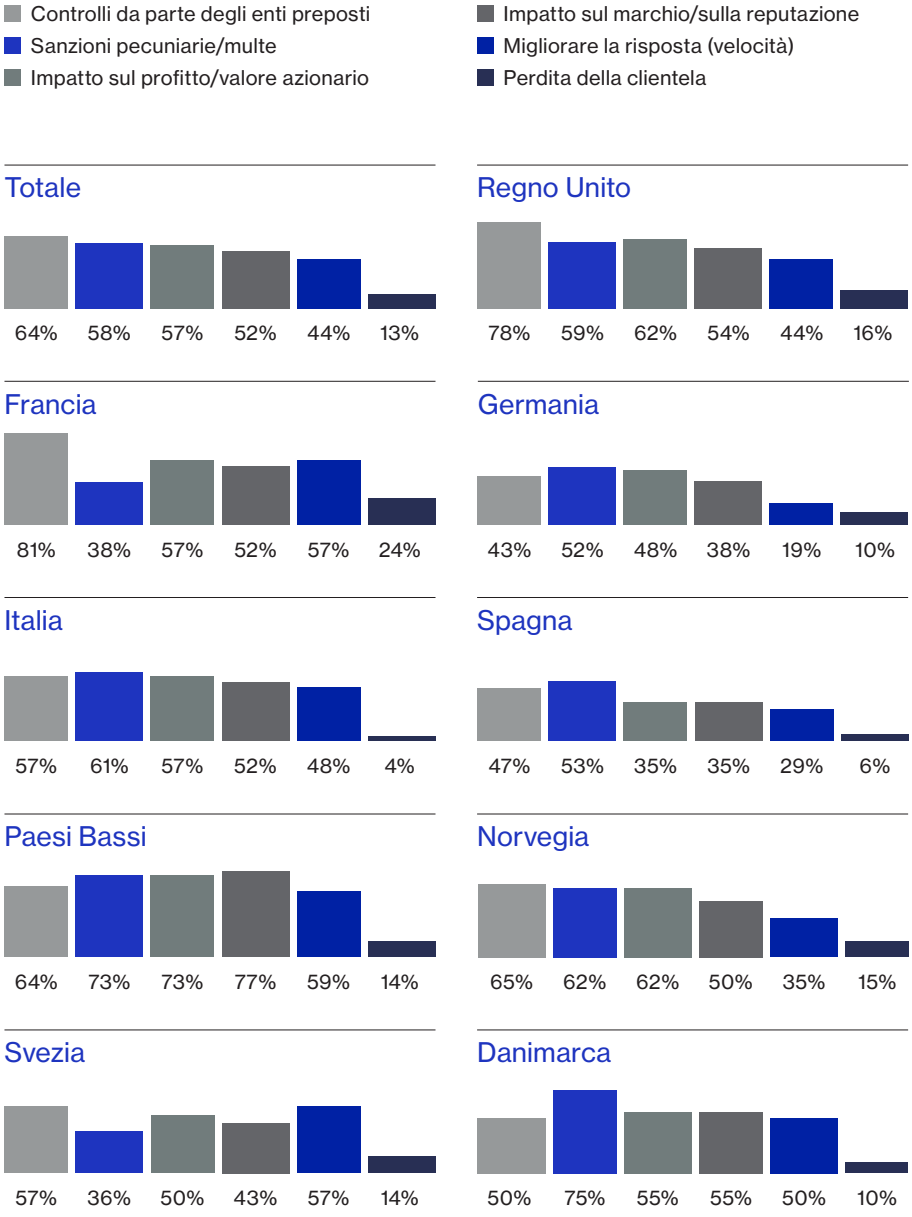
58%
sanzioni pecuniarie o multe

57%
impatto sul profitto o sul valore azionario

13%
perdita della clientela

Il sondaggio mostra che le grandi aziende europee sono più preoccupate per le potenziali implicazioni finanziarie del regolamento GDPR nel caso di una violazione dei dati. L'attacco cyber contro TalkTalk, per esempio, è costato all'azienda circa 60 milioni di sterline e ha causato una riduzione del 10% del valore azionario il giorno in cui venne annunciato l'incidente. Secondo il regolamento GDPR, è probabile che l'impatto finanziario di una violazione dei dati sia anche maggiore.

In considerazione delle attuali procedure di sicurezza dei dati nella sua azienda, quali implicazioni potrebbe avere il GDPR?



Base: Totale dei partecipanti (227): Regno Unito (63) Francia (21) Germania (21) Italia (23) Spagna (17) Paesi Bassi (22) Norvegia (26) Danimarca (20)

Sezione 5
Conclusione

5.1 Conclusione

Il rischio cyber è il rischio più complesso, attuale e critico che le aziende si trovano ad affrontare oggi: è solo questione di tempo prima che un'azienda cada vittima di una violazione o di un attacco cyber.

Gli incidenti cyber hanno il potenziale di provocare l'interruzione dell'attività, sanzioni pecuniarie, controlli da parte degli enti preposti e danni alla reputazione. Sono tutte gravi minacce per il fatturato, il valore azionario e persino la sopravvivenza di un'azienda. Può essere complicato per i vertici sapere cosa fare per proteggere le loro organizzazioni e far fronte a questa situazione.

I risultati di questo sondaggio mostrano che, mentre molte aziende credono di essere preparate per il GDPR, in realtà hanno una scarsa comprensione delle sue implicazioni. Inoltre, esempi recenti di violazione dei dati sembrano suggerire che le aziende non sono pronte per gli attacchi cyber quanto credono di essere.

A soli 18 mesi dall'entrata in vigore del GDPR, le aziende hanno ancora tempo di organizzare le proprie procedure e i propri sistemi per renderli conformi al GDPR. Nel frattempo, è fondamentale che le aziende continuino a rivedere la loro strategia per il rischio cyber e a migliorare loro comprensione della minaccia. Le minacce informatiche non spariranno mai, anzi, diventeranno sempre più complesse con il passare del tempo. È quasi impossibile proteggersi al 100% dagli attacchi cyber.

Ecco tre passi che i dirigenti dovrebbero prendere in considerazione per proteggere le loro organizzazioni.

1 Identificate i rischi specifici a cui siete esposti

Mappate i modi più probabili in cui un incidente cyber potrebbe verificarsi nella vostra organizzazione. Create piani specifici per mitigarli. Quali sono i rari eventi che non avete considerato? I vostri piani di risposta dovrebbero essere testati e aggiornati con scadenza regolare. Chiedete ai consulenti esterni di controllarli. Lavorate insieme su possibili scenari e simulazioni. Assicuratevi di prepararvi su cosa fare prima e dopo una violazione, e non solo su come contattare i clienti coinvolti.

2 Promuovete la consapevolezza del rischio cyber e del regolamento presso tutti i livelli della vostra organizzazione

Molti incidenti cyber iniziano con un errore umano, dalla divulgazione accidentale al phishing. La consapevolezza di questi problemi è una questione di cultura e deve discendere dai vertici dell'azienda. Assicuratevi che tutti i dipendenti ricevano un'adeguata formazione al riguardo e sappiano, per esempio, cosa impone il regolamento GDPR.

3 Non smettete mai di imparare

La tecnologia digitale è in continua evoluzione, e di conseguenza lo sono anche le minacce informatiche correlate. Sviluppate una cultura di "continuous learning" e di condivisione delle informazioni sul rischio cyber. Comprendete che il 100% della sicurezza informatica non esiste, il che rende tanto più importante impegnarsi nella mitigazione dei rischi, per esempio con un'assicurazione cyber.

5.2 Come può aiutare un'assicurazione cyber

1 Secondo questo sondaggio, il 73% dei dirigenti ha una conoscenza limitata dell'assicurazione cyber e il 50% non sa che è disponibile una copertura cyber per la violazione dei dati.

2 L'assicurazione cyber non offre solo la copertura delle perdite finanziarie dopo un attacco cyber, ma anche la consulenza di esperti per migliorare la sicurezza e il sostegno sul campo durante il periodo di crisi.

3 Le polizze cyber sono diverse tra loro ma è probabile che coprano i costi delle operazioni legali e forensi per identificare come è avvenuta la violazione dei dati e chi ne è responsabile, oltre che i costi delle notifiche ai clienti e dell'interruzione dell'attività.

4 Collaborare fin dall'inizio con sottoscrittori che comprendono questo rischio costituirà un vantaggio per la strategia di sicurezza di un'azienda. I sottoscrittori possono aiutare le aziende a identificare i rischi e i punti vulnerabili, e pertanto possono mitigare l'evenienza di un attacco.

5 Tutto questo contribuisce a proteggere i bilanci dell'azienda, oltre a migliorare gli standard di sicurezza informatica e di mitigazione del rischio nell'intero settore.

Sono disponibili rapporti specifici per i seguenti Paesi: Danimarca, Francia, Germania, Italia, Norvegia, Paesi Bassi, Regno Unito, Spagna e Svezia.

Per ulteriori informazioni e per contattare un Lloyd's broker cyber, visitare lloyds.com/cyber