Questionario Cyber Enterprise Risk Management

Questo documento permette a Chubb di raccogliere le informazioni necessarie per valutare i rischi connessi ai sistemi informativi dell'azienda da assicurare. Si prega di notare che il completamento di questo questionario non vincola Chubb né l'azienda alla conclusione di un accordo per l'emissione di una polizza. Se la politica di sicurezza dei sistemi informativi delle società/sussidiarie dell'eventuale assicurato varia, si prega di completare il questionario per ogni eventuale assicurato.

1. Identificazione dell'azienda richiedente

Ragione sociale:

Indirizzo:

Codice Fiscale/Partita IVA

Sito/i Web:

Numero di dipendenti:

Fatturato annuale:

Margine netto annuo:

Percentuale di Fatturato generato in:

USA/Canada: UK:

Unione Europea: Resto del Mondo:

2. Profilo dell'azienda/delle aziende da assicurare

2.1 Attività dell'azienda

[Si prega di descrivere le principali attività dell'azienda da assicurare]

CHUBB®

2.2 Società Controllate

[Si prega di fornire l'elenco delle società controllate da assicurare e descrizione dell'attività. Se l'azienda ha filiali al di fuori dell'UE, si prega di fornire i dettagli]

Nome	Sede	Attività

2.3 Criticità dei sistemi informativi

[Si prega di valutare il periodo di interruzione durante il quale l'azienda subirà un impatto significativo sulla sua attività.]

Settori (o Attività)	Massimo periodo di interruzione prima di avere un impatto negativo				
	Immediato	**> 12 h**	**> 24 h**	**> 48 h**	**> 5 giorni**
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

3. Sistemi informativi

	< 100	**101 - 1000**	**> 1000**
Numero di utenti del sistema informativo	☐	☐	☐
Numero di Laptop	☐	☐	☐
Numero di Server	☐	☐	☐

	Si	No
Disponete/Siete proprietari di un sito web?	☐	☐
Disponete/Siete proprietari di un servizio di e-commerce ?	☐	☐

In caso affermativo:
Qual è la quota di fatturato generata dal sito web? (% o effettivo)

CHUBB®

4. Sistema di Sicurezza delle Informazioni (SSI)

4.1 Security policy e risk management		Sì	No
1	Una politica di SSI è stata formalizzata e approvata dalla direzione aziendale e/o sono state definite e comunicate a tutto lo staff regole di sicurezza approvate dai rappresentanti dello staff	☐	☐
2	Sono formalizzati ed effettuati regolari training (almeno annuali) agli utenti sull'uso sicuro del sistema informativo	☐	☐
3	Sono identificati i rischi inerenti i sistemi informativi critici e sono implementati opportuni controlli per mitigarli	☐	☐
4	Sono condotti audit regolari del SSI ed è assegnata priorità all'implementazione delle raccomandazioni risultanti	☐	☐
5	Le risorse informative sono classificate in accordo alla loro criticità e sensibilità	☐	☐
6	I requisiti di sicurezza che si applicano alle risorse informative sono definiti in accordo alla loro classificazione	☐	☐

4.2 Protezione dei sistemi informativi		Sì	No
1	L'accesso ai sistemi informativi critici richiede un sistema di doppia autenticazione	☐	☐
2	Agli utenti è richiesto di aggiornare regolarmente le password	☐	☐
3	Le autorizzazioni di accesso al sistema si basano sui ruoli dei singoli utenti ed esiste una procedura per la gestione delle autorizzazioni	☐	☐
4	Sono definiti riferimenti di configurazione sicura per workstation, laptop, server e dispositivi mobili	☐	☐
5	E' attuata la gestione centralizzata dei sistemi informatici e il monitoraggio delle configurazioni	☐	☐
6	I laptop sono protetti da un personal firewall	☐	☐
7	Un software antivirus è installato su tutti i sistemi e sono monitorati gli aggiornamenti	☐	☐
8	Sono regolarmente distribuite ed installate le security patches	☐	☐
9	Un DRP (Disaster Recovery Plan) è implementato e aggiornato regolarmente	☐	☐
10	I backup dei dati sono portati a termine quotidianamente, sono testati regolarmente e copie di essi sono depositate regolamermente in una località remota rispetto a quella ove risiedono i sistemi	☐	☐

4.3 Sicurezza della rete e delle operazioni		Sì	No
1	E' installato ed operativo un firewall per il filtraggio del traffico tra la rete interna e internet con un controllo aggiornato del flusso di informazioni in entrata ed in uscita	☐	☐
2	Un IDS/IPS (Intrusion Detection/Prevention System) è implementato, aggiornato e monitorato regolarmente	☐	☐
3	Gli utenti interni all'azienda hanno accesso a Internet attraverso dispositivi di rete protetti da antivirus e sistemi di monitoraggio del traffico web	☐	☐
4	È implementata la segmentazione della rete per separare le aree critiche dalle aree non critiche	☐	☐
5	Sono effettuati regolarmente penetration test ed è implementato un remediation plan ove necessario	☐	☐
6	Sono effettuati regolarmente vulnerability assessment ed è implementato un remediation plan ove necessario	☐	☐
7	Sono rese effettive procedure di incident management e change management	☐	☐
8	Eventi riguardanti la sicurezza, come rilevazioni di virus, tentativi di accesso, e simili, sono registrati (tramite log file) e monitorati regolarmente	☐	☐

CHUBB®

4.4 Sicurezza fisica della sala computer		Sì	No
1	I sistemi critici sono collocati in almeno una sala computer dedicata con accesso limitato e allarmi operativi funzionanti sono inviati ad una sede di monitoraggio	☐	☐
2	I CED che ospitano sistemi critici hanno un'infrastruttura resiliente che include ridondanza dei sistemi di alimentazione, impianti di condizionamento e connessioni di rete	☐	☐
3	I sistemi critici sono duplicati in funzione di un'architettura Active/Passive o Active/Active	☐	☐
4	I sistemi critici sono duplicati in due sedi separate	☐	☐
5	Sono implementati rilevatori antincendio e sistemi automatici di estinzione in aree critiche	☐	☐
6	L'alimentazione è protetta da UPS e batterie, entrambi sottoposti a regolari programmi di manutenzione	☐	☐
7	L'alimentazione è sostenuta da generatore elettrico soggetto a regolare contratto di manutenzione e testato regolarmente	☐	☐

4.5 Outsourcing		Sì	No
[Si prega di compilare in caso una o più funzioni del sistema informativo è data in outsourcing]			
1	Il contratto di outsourcing include requisiti di sicurezza che devono essere osservati dall'outsourcer	☐	☐
2	I Service Level Agreements (SLA) sono definiti con l'outsourcer al fine di gestire gli incidenti e vengono applicate penalità all'outsourcer in caso di non conformità con i SLA	☐	☐
3	Il/I comitato/i di direzione e controllo si coordina con il service provider per la gestione e il perfezionamento del servizio	☐	☐
4	L'assicurato ha rinunciato al diritto di ricorso contro l'outsourcer nel contratto di outsourcing	☐	☐

Quali sono le funzioni del sistema informativo date in in outsourcing?	Si	No	Outsourcer
Desktop management	☐	☐	
Server management	☐	☐	
Network management	☐	☐	
Network security management	☐	☐	
Application management	☐	☐	
Utilizzo di cloud computing	☐	☐	
Se si, si prega di specificarne la natura			
Software as a Service	☐	☐	
Platform as a Service	☐	☐	
Infrastructure as a Service	☐	☐	
Altro, si prega di specificare:			

5	Il contratto di outsourcing contiene una disposizione che richiede al service provider di sostenere una polizza assicurativa coprente indennità professionale, errori e omissioni	☐	☐

CHUBB®

5. Dati personali trattenuti dall'azienda

5.1 Tipo e numero di record (archivi/documenti/registri)

Il numero di record contenenti informazioni personali trattenuti per l'attività da assicurare:

Totale: Per nazione: UK/I:

Europe (EU): USA/Canada: Resto del mondo:

Categorie di dati personali raccolti/trattati:	Si	No	Quantità
Informazioni commerciali e di marketing	☐	☐	
Carte di credito o informazioni sulle transazioni finanziarie	☐	☐	
Informazioni di natura sanitaria	☐	☐	
Altro, si prega di specificare:			

I dati sono trattati: ☐ Per fini propri ☐ Per conto di terze parti

5.2 Politica di protezione delle informazioni personali

		Sì	No
1	E' stata formalizzata ed approvata dall'amministrazione una politica sulla privacy e/o sono definite e comunicate allo staff interessato regole per la sicurezza dei dati personali	☐	☐
2	Sono forniti corsi di formazione e sensibilizzazione almeno annualmente al personale autorizzato ad accedere a o a trattare con dati personali	☐	☐
3	È nominato un funzionario incaricato della protezione dei dati personali	☐	☐
4	Viene firmato nel contratto di assunzione, da parte dello staff interessato, un accordo o una clausola di riservatezza	☐	☐
5	Gli aspetti legali relativi alla politica sulla privacy sono convalidati da un avvocato o dalla divisione legale	☐	☐
6	Sono implementate misure di monitoraggio per garantire la conformità con le leggi e regolamentazioni per la protezione dei dati personali	☐	☐
7	Le pratiche/prassi aziendali relative alle informazioni personali sono state sottoposte a auditing da un ispettore esterno negli ultimi due anni	☐	☐
8	Un Data Breach Response Plan è implementato e i ruoli sono stati comunicati con chiarezza ai membri della squadra operativa	☐	☐

5.3 Raccolta di dati personali

		Sì	No
1	Avete notificato al Garante per la protezione dei dati personali il Responsabile del trattamento dei dati personali nominato in azienda e avete ottenuto la rispettiva autorizzazione Se non applicabile, si prega di spiegare:	☐	☐
2	E' stata pubblicata sul sito aziendale una politica sulla privacy revisionata da un legale/dipartimento legale	☐	☐
3	È richiesto il consenso prima di raccogliere i dati personali e gli interessati possono accedere e, se necessario, correggere o cancellare i loro dati personali	☐	☐
4	Ai proprietari è fornita in modo chiaro la possibilità di rinunciare ad operazioni mirate di marketing	☐	☐
5	Trasferite i dati personali a terzi: Se si, si prega di rispondere alle seguenti:	☐	☐
5.a	I terzi sono contrattualmente obbligati a trattare i dati personali esclusivamente per conto vostro e secondo le vostre istruzioni	☐	☐
5.b	I terzi sono contrattualmente obbligati a implementare sufficienti misure di sicurezza per proteggere i dati personali	☐	☐

CHUBB®

5.4 Controlli per la protezione dei dati personali		Sì	No
1	L'accesso ai dati personali è limitato ai soli operatori che lo necessitano per svolgere il proprio incarico e le autorizzazioni di accesso sono revisionate regolarmente	☐	☐
2	I dati personali sono criptati quando archiviati nei sistemi informatici, così come i relativi backup	☐	☐
3	I dati personali sono criptati quando trasmessi attraverso la rete	☐	☐
4	I dispositivi mobili e gli hard disk dei laptop sono criptati	☐	☐
5	La politica di sicurezza delle informazioni proibisce la copia di dati personali non criptati su dispositivi di archiviazione mobili o la trasmissione di tali dati via email	☐	☐

Se gli archivi di dati personali contengono dati relativi alle carte di credito, si prega di rispondere alle seguenti:

Il vostro livello PCI DSS è:

Livello 1: ☐ Livello 2: ☐ Livello 3: ☐ Livello 4: ☐

	Sì	No
Chi tratta i pagamenti (voi stessi o terzi) rispetta il PCI DSS	☐	☐
Se No:		
I dati relativi alle carte di credito sono archiviati criptati o solo una parte di essi è archiviata	☐	☐
Il tempo di mantenimento dei dati relativi alle carte di credito non eccede la durata di pagamento e i requisiti legali/normativi	☐	☐
Il trattamento dei dati relativi alle carte di credito è esternalizzata	☐	☐
Se Si:		
E' richiesto a chi si occupa del trattamento i pagamenti di indennizzarvi in caso di violazione della sicurezza	☐	☐

Si prega di indicare il nome di chi si occupa del trattamento dei pagamenti, il tempo di mantenimento dei dati relativi alle carte di credito e ogni ulteriore misura di sicurezza:

CHUBB®

5.5 Incidenti

Si prega di fornire una descrizione di qualunque incidente relativo alla sicurezza informatica o alla privacy accaduto nei precedenti 36 mesi. Gli incidenti includono qualunque accesso non autorizzato a qualunque computer, sistema informatico o database, intrusione o attacco, impossibilità d'utilizzo di qualunque computer o sistema, interruzione premeditata, corruzione, o distruzione di dati, programmi, o applicazioni, qualunque evento di cyber estorsione; o qualunque altro incidente simile ai precedenti, inclusi quelli che hanno generato una richiesta di risarcimento, azione amministrativa, o procedimento da parte di un'autorità di vigilanza.

Data:

Descrizione dell'incidente:

Commenti:

Nessun individuo o ente per cui è richiesta copertura è a conoscenza di alcun fatto, circostanza, o situazione, che ha ragione di suppore possa causare alcuna richiesta di risarcimento **(claim)** che possa ricadere nell'ambito della copertura proposta.

Nessuno ☐ o, tranne:

Persona da contattare per ulteriori informazioni:

Nome: Titolo: Telefono:

E-mail: Compilato da:

Il sottoscritto certifica che tutte le dichiarazioni contenute nel presente questionario sono complete e corrette. Tutte le modifiche che avvengono dopo la presentazione del questionario o durante il periodo di assicurazione devono essere comunicate alla ACE European Group Limited, immediatamente.
I dati personali relativi al firmatario (nome, cognome, funzione e firma) sono obbligatori e saranno trattati da ACE in ottemperanza alle vigenti leggi. Tali dati saranno trattati dai sottoscrittori autorizzati e dal personale del gruppo ACE European Group Ltd incaricati della gestione di applicazioni di protezione dei dati relative a Rischi e offerte. Il titolare dei dati ha il diritto di ottenere una copia dei propri dati personali che lo riguardano, ottenere la rettifica o la cancellazione dei dati personali scaduti o inesatti e di opporsi al loro trattamento per motivi legittimi. Se si desidera esercitare tali diritti alla privacy, si prega di inviare la tua richiesta scritta, insieme a una copia di un documento d'identità, al seguente indirizzo: ACE European Group Limited, Ufficio Technical Lines, viale Monza 258, 20128 Milano.

Nome e Cognome del firmatario

Ruolo

Data

Firma

Chubb. Insured.℠