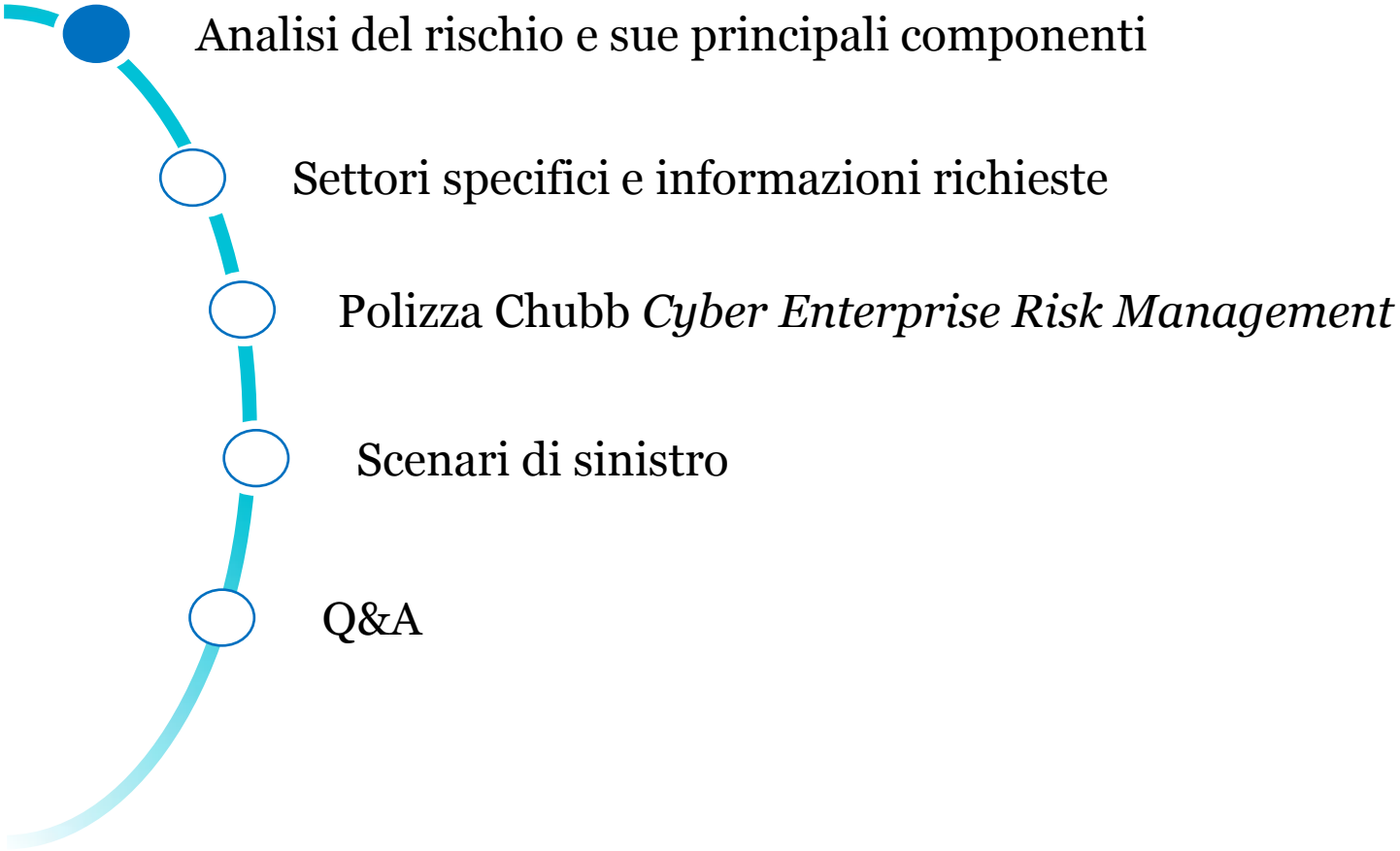
Club Assicuratori Romani 2017

Comprendere, valutare e assicurare il rischio cyber

CHUBB®

Alberto Froldi, Cyber Unit, Chubb

Agenda


Analisi del rischio e sue principali componenti
Settori specifici e informazioni richieste
Polizza Chubb *Cyber Enterprise Risk Management*
Scenari di sinistro
Q&A

L'impatto economico del rischio cyber

Costo medio annuo **per una PMI** a causa del rischio cyber

€ 35.000

PMI (<50 dipendenti) che hanno subito attacchi informatici **con danno**

43,7%

Fonti:
- 2016 Italian Cybersecurity Report – CIS Sapienza – CINI
- Cyber attacks: preliminary evidence from the Bank of Italy's business surveys – Banca d'Italia

Le informazioni assuntive richieste

Questionario Chubb Cyber ERM Standard:

- Valido per tutte le tipologie di rischio
- Basato sullo standard *ISO/IEC 27001*

Questionario Chubb Cyber ERM Semplificato:

- Pensato per le PMI

Le principali componenti del rischio

- Tipologia di attività svolta
- Maturità della IT governance riguardo a tematiche di cybersecurity
- Livello di preparazione degli utenti del sistema informativo
- Tipologia e quantità di dati personali gestiti
- Erogazione di servizi web-based
- Dipendenza dei sistemi produttivi dai sistemi informativi (manifatturiero)
- Livello complessivo di cyber-resilienza (DR/BC Plan, RTO/RPO)

Settori specifici e informazioni richieste

Fornitori di servizi IT (Gestione di asset IT, Servizi cloud, Hosting, …)

- Dettaglio delle attività svolte
- Metodologia di fornitura dei servizi utilizzate (cloud, gestione remota, pay-per-use, licenza, …)
- Eventuali misure di sicurezza specifiche a protezione della porzione di perimetro esposto verso l'esterno e verso la rete dei clienti
- Livello di ridondanza dei sistemi
- RTO e RPO totali e per servizi critici
- Qualora si gestiscano dati per conto di terzi, stima della quantità dei dati trattati

Settori specifici e informazioni richieste

Istituti Sanitari (Ospedali, Cliniche private, Ambulatori, Laboratori, …)

- Stima del numero di dati sanitari gestiti
- Descrizione delle modalità di archiviazione dei dati sanitari e specifiche misure di sicurezza a protezione di tali dati (crittografia, archiviazione in area segregata)
- Dettaglio di eventuali servizi esposti su internet

Settori specifici e informazioni richieste

Istituzioni Finanziarie (Banche, Assicurazioni, Società di factoring…)

- Descrizione delle modalità di archiviazione dei dati di carte di pagamento e specifiche misure di sicurezza a protezione di tali dati (crittografia, archiviazione in area segregata)
- Dettaglio di eventuali servizi esposti su internet
- Livello di ridondanza dei sistemi
- RTO e RPO totali e per servizi critici
- Livello PCI-DSS

La polizza Cyber

Struttura del contratto e Garanzie fondamentali

Responsabilità Civile

La Compagnia pagherà il **Risarcimento** e le **Spese** per:

Violazione obblighi di riservatezza
- Violazione di dati personali
- Violazione di informazioni aziendali di terzi
- Violazione involontaria delle Norme sulla privacy

Sicurezza della rete
- Violazione della rete aziendale

Media Liability
- Diffamazione, oltraggio, plagio
- Violazione di copyright

nell'ambito della prestazione di servizi multimediali

Danni propri

Interruzione d'attività
La Compagnia pagherà le **Perdite per interruzione delle attività** subite durante il **Periodo di indennizzo** e le **Spese Extra**

Perdita di Dati
La Compagnia pagherà i **Costi di recupero** in conseguenza di un **incidente relativo ai Dati**

Cyber Estorsione
La Compagnia pagherà il **riscatto** (ove non vietato dalla legge) e le **spese** a seguito di una ***cyber* estorsione**

Danni Coperti

Risarcimento

Spese Legali

Incident Response

Computer Forensic

Costi di Notifica

Spese di Consulenza

Spese per PR

Costi di decontaminazione

Costi di ricostruzione dei dati

Spese Extra

Perdita di profitto

CHUBB®

La polizza Cyber

Sruttura del contratto e Garanzie fondamentali

Responsabilità Civile

- una richiesta scritta di risarcimento pecuniario o non pecuniario
- un procedimento civile
- una procedura arbitrale
- un procedimento di un organo di vigilanza
- una comunicazione scritta di un Atto illecito, effettivo o presunto, dal quale potrebbe derivare una Richiesta di risarcimento

Danni Propri

Interruzione d'attività

Perdita di profitto durante il **periodo di indennizzo** esclusivamente e diretta conseguenza di:

- Attacco informatico
- Errore umano
- Errore di programmazione
- black-out, sbalzi o diminuzioni di tensione che colpiscono il Sistema informatico

Perdita di Dati

Costi di recupero in coseguenza della presa di possesso dei **Dati**, la relativa corruzione o distruzione, causata da:

- Attacco informatico
- Errore umano;
- Errore di programmazione;
- black-out, sbalzi o diminuzioni di tensione che colpiscono il Sistema informatico

Cyber Estorsione

Qualunque credibile minaccia, o serie di minacce connesse, fatta da terzi **al fine di estorsione**

La polizza Cyber
Le principali Esclusioni

Non sono coperti i **Sinistri:**

- che presumono, si basano su, derivano da o sono attribuibili a interruzione della rete o guasti che non dipendono da infrastrutture sotto il controllo operativo dell'Assicurato
- Guerra, terrorismo, sciopero. La presente esclusione non si applica ad **Atti di cyber-terrorismo** che danno origine a un **Sinistro**
- Furto di denaro o titoli

Esclusivamente per le sezioni **Perdita di Dati** e **Interruzione d'attività,** non sono coperti i **Sinistri**:

- che presumono, si basano su, derivano da o sono attribuibili alla normale usura o al graduale deterioramento dei Dati, ivi compresi dei mezzi di elaborazione dati.
- che presumono, si basano su, derivano da o sono attribuibili ad azioni di un'autorità pubblica o del governo, ivi compreso il sequestro, la confisca o la distruzione del vostro Sistema informatico o dei Dati

La polizza Cyber

Le principali Estensioni

Computer Crime

- Perdita finanziaria a seguito del furto di denaro o titoli per mezzo di un attacco di attacco informatico perpetrato da parte di terzi

Hardware

- Danno ai dispositivi ubicati presso il locali dell'Assicurato o in viaggio (es: Centro Elaborazione Dati, dispositivi endpoint, dispositivi di archiviazione, etc…) utilizzati per archiviare, processare, modificare o controllare dati

La polizza Cyber

Termini e Garanzie fondamentali

Privacy Liability

- Solo dati personali? E per quanto riguarda le informazioni aziendali?
- E' necessario l'Atto Doloso Informatico per far scattare la copertura? (*trigger)*
- Richiami testuali al Nuovo Regolamento sul trattamento dei Dati?

Definizione di Atto Doloso Informatico

- La più ampia possibile: al fine di comprendere qualsiasi tipologia di codice malevolo
- *Malware* è il termine più generico

Errore Umano / Errore di programmazione

- Come vengono trattate tali fattispecie nel testo di polizza?

La polizza Cyber

Termini e Garanzie fondamentali

Definizione di Sistema Informatico dell'Assicurato

- Cosa accade se i Dati si trovano presso un fornitore esterno di servizi IT?

Spese Extra

- Costi per rimuovere i Malware dal Sistema Infomatico
- Aumento dei costi del lavoro
- Spese per esternalizzare il lavoro
- L'uso di dispositivi esterni presi a noleggio

Incident Response

- Servizio gratuito di gestione e pronto intervento in caso di crisi/disastro
- Numero verde internazionale attivo 24/7
- Discovery Plan
- Computer Forensic
- Consulenza tecnico/giuridica

Scenari di sinistro

Scenario 1: Phishing

Descrizione dell'evento:

Un dipendente di un negozio di elettronica ha ignorato le policy aziendali in materia di sicurezza e ha aperto un file, apparentemente innocuo, allegato ad una e-mail. Il giorno successivo il sistema informatico utilizzato per processare gli ordini e i pagamenti manifesta malfunzionamenti impedendo il regolare svolgimento delle attività.

Danni:

- Investigazioni di computer forensic
- Ripristino dei sistemi
- Aumento dei costi del lavoro
- Fermo d' attività

Garanzie attivate:

- Perdita di dati
- Interruzione d'attività

Scenari di sinistro
Scenario 2: Compromissione di asset tecnologico

Descrizione dell'evento:

Una società manifatturiera ha affittato una fotocopiatrice per un periodo di due anni. La macchina ha immagazzinato numerose informazioni sensibili di clienti e dipendenti. Allo scadere del contratto d'affitto, la società manifatturiera restituisce la macchina alla compagnia concedente tramite una società intermediaria. Prima che la macchina venisse restituita alla concedente, un dipendente della società intermediaria ha acceduto ai dati contenuti nella macchina per scopi infausti.

Danni:

- Investigazioni di computer forensic
- Consulenza legale
- Servizi di call center
- Servizi di monitoraggio e ripristino dell'identità

Garanzie attivate:

- Perdita di dati
- Responsabilità derivante da violazione di obblighi di riservatezza

Scenari di sinistro
Scenario 3: Furto di laptop

Descrizione dell'evento:

Il laptop di un dirigente è stato trafugato da un'auto aziendale. Il laptop conteneva informazioni sensibili di clienti e dipendenti. Nonostante i file fossero criptati, il livello generale di protezione e robustezza delle password era debole e il PIN di accesso alle informazioni criptate è stato compromesso.

Danni:

- Investigazioni di computer forensic
- Spese legali
- Servizi di call center
- Servizi di monitoraggio e ripristino dell'identità

Garanzie attivate:

- Perdita di dati
- Responsabilità derivante da violazione di obblighi di riservatezza

Q&A

Chubb. Insured.