Cyber security: policies e processi NIS e dintorni

30 Novembre 2021

Today’s team

Edoardo Tedeschi

Partner, TMT and Digital Business

T +39 02 7250 5585

E edoardo.tedeschi@simmons-simmons.com

Eugenia Lopresti

Lawyer, Milan

T +39 02 7250 5440

E eugenia.lopresti@simmons-simmons.com

Mauro Teresi

Of Counsel, Regulatory and Product Liability

T +39 02 7250 5559

E mauro.teresi@simmons-simmons.com

Sicurezza dei dati personali

Principali riferimenti normativi:

- GDPR
- Direttiva NIS (recepita in Italia con il D. Lgs. 65/2018)
- Regolamento UE 2019/881 «Regolamento sulla Cybersecurity»
- Linee Guida e raccomandazioni Enisa
- DPCM 30 luglio 2020 n. 131 «Regolamento in materia di perimetro di sicurezza nazionale cibernetica»
- Proposta della direttiva NIS 2

Sicurezza dei dati personali

Art. 32 GDPR «sicurezza del trattamento»

Il Titolare del trattamento deve assicurare:

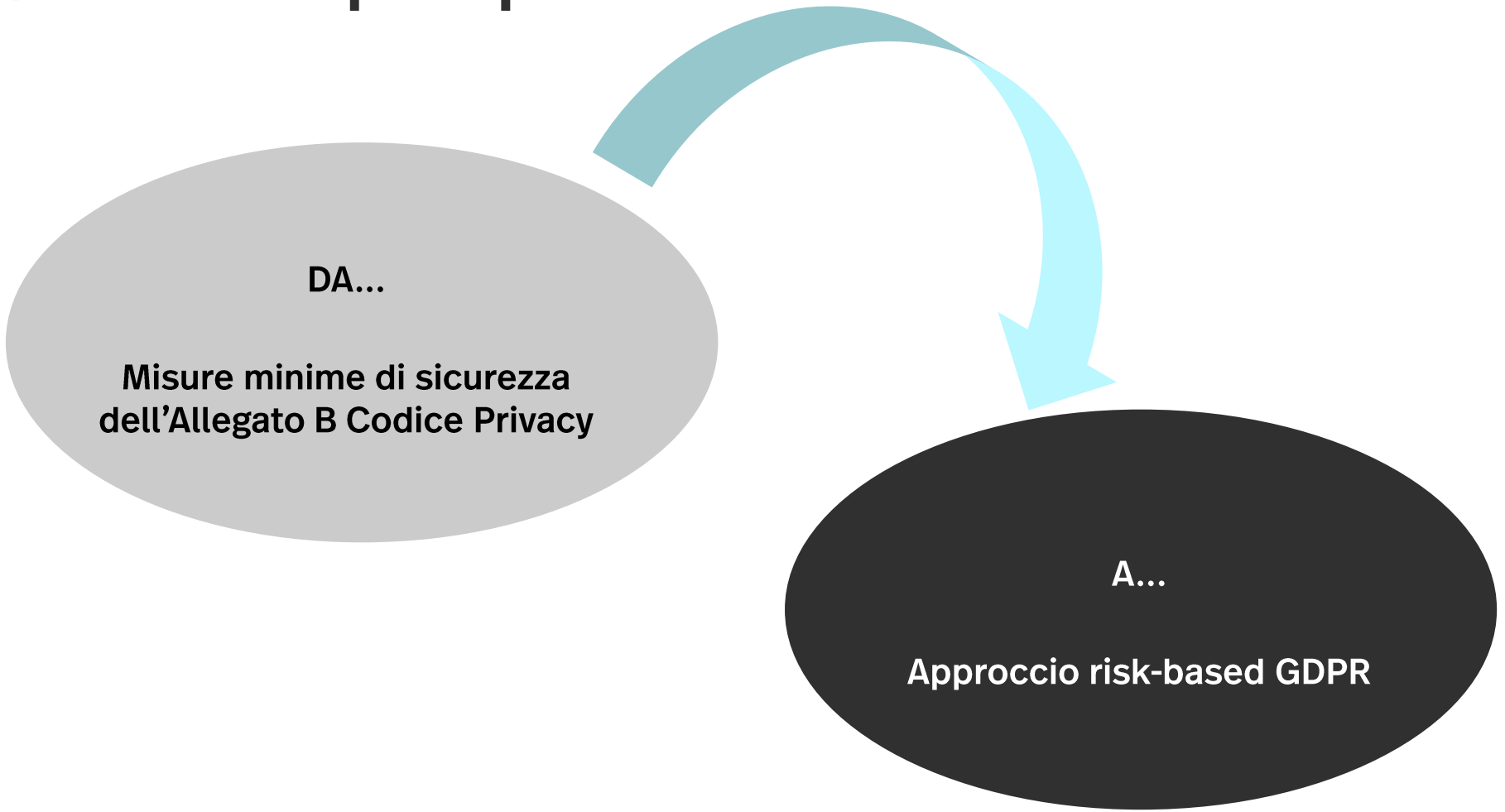
- **Riservatezza**: assicurarsi che le informazioni siano accessibili solo a chi è autorizzato ad averne accesso
- **Integrità**: salvaguardare l'accuratezza e la completezza delle informazioni
- **Disponibilità**: assicurarsi che utenti autorizzati abbiano accesso alle informazioni

Sicurezza dei dati personali

§ Art. 32 GDPR

Art. 32 GDPR «sicurezza del trattamento»

Cambio di prospettiva



Valutazione del rischio

ISO/IEC 27001 «Information Technology – security management system – Requirements

- È la norma per la gestione della sicurezza delle informazioni
- Si basa sulla valutazione e gestione dei rischi
- Applicabile a qualunque impresa a prescindere da uno specifico settore di business
- Specifica i requisiti per progettare, implementare, controllare, mantenere e migliorare un Sistema di gestione della Sicurezza delle Informazioni (SGSI)

Valutazione del rischio

ISO/IEC 27001 e ISO 9001 «sistema di gestione della qualità»

- L'impostazione ISO 27001 è coerente con quella della ISO 9001, in quanto vengono trattati i seguenti argomenti:
  - ✓ Approccio per processi
  - ✓ Politica per la sicurezza
  - ✓ Identificazione
  - ✓ Analisi dei rischi
  - ✓ Valutazione e trattamento dei rischi
  - ✓ Modello Plan-Do-Check-Act (PDCA)
  - ✓ Utilizzo di procedure e strumenti di Audit
  - ✓ Sorveglianza e miglioramento continuo

Incident Handling vs Data Breach

§ Data breach

Definizioni

- **Evento** (ISO): è un episodio osservabile in un sistema o in una rete consistente in un cambiamento osservabile all'interno del comportamento abituale di un sistema o di un processo

- **Incidente** (NIS): ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi

- **Violazione dei dati** (GDPR): è un incidente che riguarda o coinvolge, 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 (art. 4.12 GDPR)

Data protection impact assessment

§ DPIA

Art. 35 GDPR «Valutazione di impatto sulla protezione dei dati»

- Quando un trattamento, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare del trattamento effettua, **prima di procedere al trattamento**, una valutazione di impatto (**DPIA**).
- una singola valutazione di impatto può **esaminare un insieme di trattamenti simili** che presentano rischi elevati analoghi
- Il titolare quando svolge una DPIA si **consulta con il DPO** (qualora disegnato)

Data protection impact assessment

La DPIA è richiesta nei seguenti casi:

- **Valutazione sistematica e globale di aspetti personali relativi a persone fisiche**, basata su un trattamento automatizzato, compresa la profilazione
- Il trattamento su **larga scala di categorie particolari di dati personali**
- La **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico

Data protection impact assessment

La DPIA deve contenere almeno:

- Una **descrizione sistematica dei trattamenti** previsti e delle **finalità** del trattamento
- Una valutazione della **necessità e proporzionalità** dei trattamenti
- Una valutazione dei **rischi per i diritti e le libertà** degli interessati
- Le **misure** previste per affrontare i rischi

Se necessario il Titolare procede a un **riesame** per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati **almeno quando insorgono variazioni del rischio** rappresentato dalle attività relative al trattamento

Amministratori di Sistema

Provvedimento Garante 27/11/2008

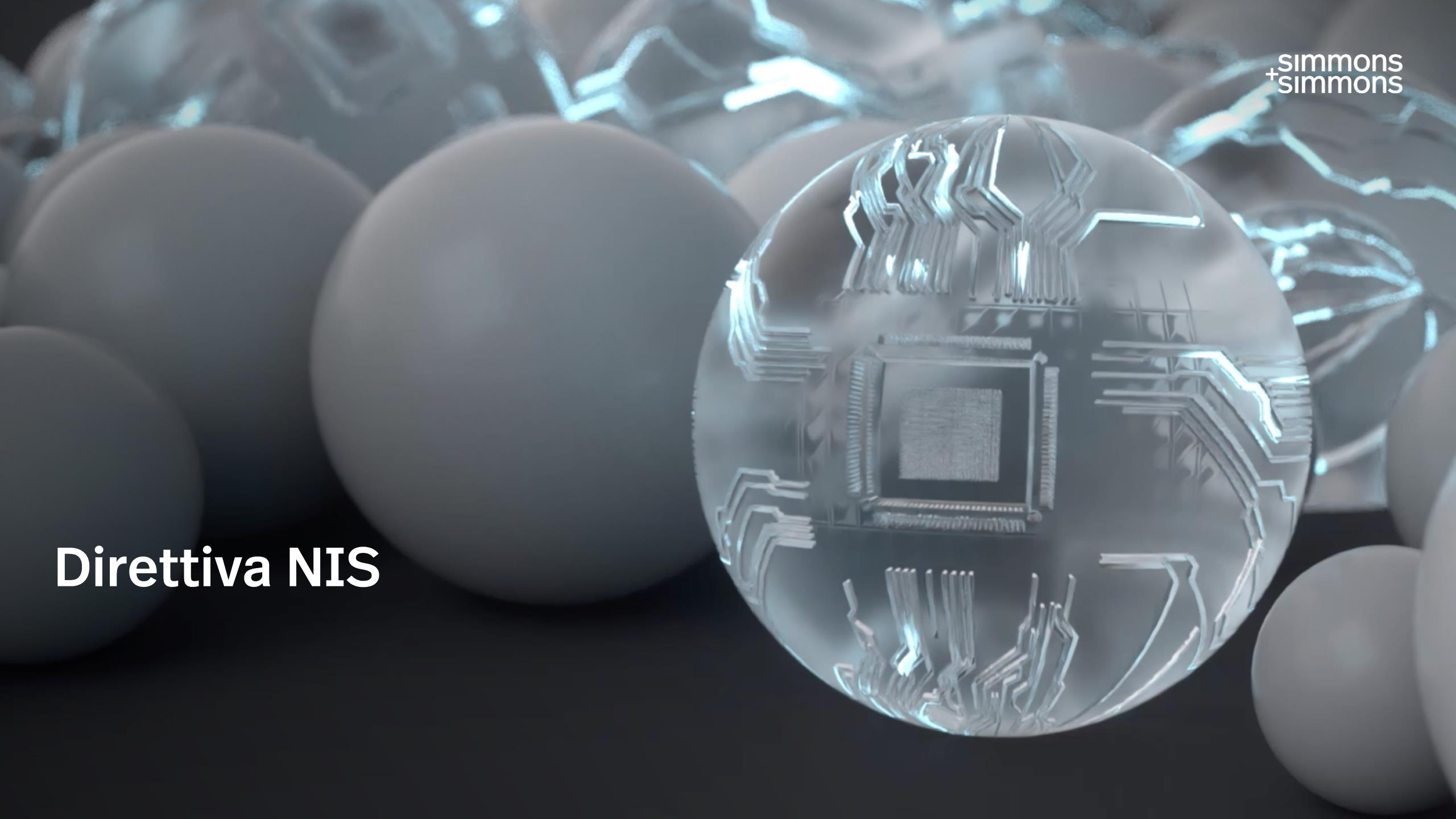
- **Amministratori di sistema**: figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché gli amministratori di basi dati, amministratori di reti, amministratori di apparati di sicurezza e amministratori di sistemi software complessi

Amministratori di sistema possono essere così suddivisi nelle seguenti macro aree:

Amministratori di Sistema

Peculiarità

- **Valutazione delle caratteristiche soggettive**
- **Designazione individuale e ambiti di operatività**
- **Elenco dei soggetti designati**
- **Verifica dell'operato**
- **Sistema di log management** (i file di log devono essere completi, inalterati, possibilità di verifica della loro integrità e conservati per almeno 6 mesi)



simmons+simmons

Direttiva NIS

Direttiva NIS

Quadro normativo e finalità della Direttiva NIS

- La direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, attuata in Italia con il D. Lgs. 65/2018 **reca misure per la creazione di un livello comune elevato di sicurezza delle reti e dei sistemi informativi** all'interno dell'Unione Europea e ha come obiettivo quello di :
  - ✓ Adottare una strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi
  - ✓ Designare le autorità nazionali competenti, punti di contatto unici e CSIRT (Computer Security Incident Response Team)
  - ✓ Creare una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (rete CSIRT)
  - ✓ Istituire un gruppo di cooperazione al fine di sostenere un gruppo di cooperazione
  - ✓ Stabilire obblighi di sicurezza e di notifica

Direttiva NIS

Ambito di applicazione della direttiva NIS

Considerando 7.
La presente direttiva si applica sia agli **operatori di servizi essenziali (OSE)** e che ai **fornitori di servizi digitali (FSD)** in modo da coprire tutti i relativi rischi e incidenti.

Le disposizioni in materia di misure di sicurezza e di notifica degli incidenti non si applicano, invece, alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (si applica il Codice del Consumo) e ai prestatori di servizi fiduciari (si applica il regolamento eIDAS)

Direttiva NIS

§ OSE

Operatori di servizi essenziali (OSE)

I criteri per identificare gli Operatori di servizi essenziali ai sensi dell'art.5.2 sono:

- Fornitura di **un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali**
- La fornitura di tale servizio **dipende dalla rete e dai sistemi informativi**
- Un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio

Direttiva NIS

§ OSE

Settori degli Operatori di servizi essenziali (OSE)

- Energia (elettrica, petrolio e gas)
- Trasporti (aereo, treno, per vie d'acqua, su strada)
- Settore bancario
- Infrastrutture dei mercai finanziari
- **Settore sanitario (istituti sanitari compresi ospedali e cliniche private)**
- Fornitura e distribuzione di acqua potabile
- Infrastrutture digitali

Direttiva NIS

§ OSE

Obblighi in materia di sicurezza e notifica per gli OSE

Gli OSE devono adottare:

- **Misure tecniche e organizzative adeguate e proporzionate** alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi
- Misure adeguate per **prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi al fine di assicurare la continuità di tali servizi
- **Notificare al CSIRT** italiano e, per conoscenza, all'Autorità competente NIS, senza ingiustificato ritardo gli incidenti aventi un impatto rilevante (numero di utenti interessati, durata dell'incidente, diffusione geografica)

Direttiva NIS

§ FSD

Fornitori di servizi digitali (FSD – outsource cloud)

Si qualifica come Fornitore di servizi digitale, qualsiasi persona giuridica che fornisce un **servizio digitale**.

Per servizi digitali si intende:

- **Mercato online**: un servizio digitale che consente ai consumatori e/o ai professionisti di concludere contratti di vendita o di servizi online con i professionisti sul web del mercato online
- **Mercato di ricerca online**: un servizio digitale che consente all'utente di effettuare ricerche su tutti siti web
- **Servizi cloud computing**: un servizio digitale che consente l'accesso a un insieme scalabile e elastico di risorse informatiche condivisibili

Direttiva NIS

§ FSD

Rilevanza dell'impatto di un incidente per i Fornitori di servizi digitali (FSD)

Si tiene conto in particolare dei seguenti parametri:

- Numero di utenti interessati dall'incidente
- Durata dell'incidente
- Diffusione geografica
- Portata della perturbazione del funzionamento del servizio
- Portata dell'impatto sulle attività economiche e sociali

Direttiva NIS

§ FSD

Valutazione della rilevanza di un incidente per i Fornitori di servizi digitali (FSD)

Sulla base del Regolamento UE 2018/151, un incidente si considera rilevante se si verifica almeno una delle seguenti condizioni:

- Indisponibilità del servizio fornito per oltre 5.000.000 di ore
- Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE
- Danni materiali superiori 1.000.000 di euro per almeno un utente in Europa

simmons+simmons

Proposta di Direttiva NIS 2

Verso la proposta di Direttiva NIS 2

Report Commissione Europea 2019 (i)

- La Commissione Europea ha valutato gli approcci adottati dagli Stati membri dell'Unione nell'adozione della Direttiva NIS. La relazione ha riportato che gli Stati hanno sviluppato **metodologie eterogenee** per identificare gli operatori essenziali ed esistono interpretazioni divergenti su ciò che costituisce un servizio essenziale ai sensi della Direttiva NIS.

- Inoltre, dal report è risultato che gli stati hanno adottato approcci divergenti e il rischio è che **l'applicazione della Direttiva risulti frammentata**.

Verso la proposta di Direttiva NIS 2

Report Commissione Europea 2019 (ii)

- La Commissione nel 2020 ha presentato una **proposta di revisione della Direttiva NIS (NIS 2)** che abrogherà e sostituirà la NIS.

- Una revisione della Direttiva NIS si è resa necessari anche alla luce dell'**accelerazione del processo di digitalizzazione** connessa alla pandemia da Codvi-19 e all'**aumento delle minacce cyber** ad essa connesse.

Proposta di Direttiva NIS 2

Maggiori novità (i)

- **Estensione di specifici obblighi in materia di cybersecurity a soggetti operanti in settori ad oggi non coperti dalla Direttiva NIS** (es. settore della produzione di dispositivi medici ed apparecchiature elettroniche)

- **L'identificazione degli operatori di servizi essenziali** effettuata dai Ministeri verrà superata poiché sarà la Direttiva stessa a definire il proprio ambito di applicazione

- Tra le misure di sicurezza **vengono aggiunte l'utilizzo della crittografia e i controlli sulla sicurezza informatica dei propri fornitori**

Proposta di Direttiva NIS 2

Maggiori novità (ii)

- **La notifica** viene previsto che vada effettuata **entro 24 ore**

- **Sanzioni pari ad massimo di almeno 10 milioni di euro o fino al 2% del fatturato totale annuo** mondiale dell'impresa interessata (incremento importante rispetto all'attuale sanzione italiana pari ad un massimo di 150.000 euro)

Proposta di Direttiva NIS 2

Il contesto europeo del healthcare (i)

- La Direttiva NIS 2 si pone come obiettivo quello di risolvere alcune criticità della Direttiva NIS. La Direttiva NIS, infatti, ha promosso l'istituzione di misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in tutto l'Europa, applicabile anche nel settore sanitario.

- La direttiva NIS è solo una delle normative in tema cybersecurity in ambito healthcare. Ricordiamo tra le altre soprattutto il GDPR e la **Guidance on Cybersecurity for medical devices della Commissione Europea** (pubblicata a gennaio 2020)

Proposta di Direttiva NIS 2

Il contesto europeo del healthcare (ii)

- L'11 novembre 2021 ENISA ha pubblicato il **report sulla capacità del CSIRT nel settore sanitario dall'attuazione della Direttiva NIS**.

Lo scopo del rapporto è quello di offrire approfondimenti sulle attuali tendenze di risposta agli incidenti (IR) al fine di trarre raccomandazioni pratiche sullo sviluppo delle capacità IR nel settore sanitario.

ENISA (i)

Rapporto CSIRT dell'11 novembre 2021

- Enisa ha ricevuto **742 segnalazioni** su incidenti di sicurezza informatica con impatto significativo dai settori critici ai sensi della Direttiva NIS.

- **Il settore sanitario** ha registrato un **aumento del 42% di tali incidenti** rispetto all'anno precedente.

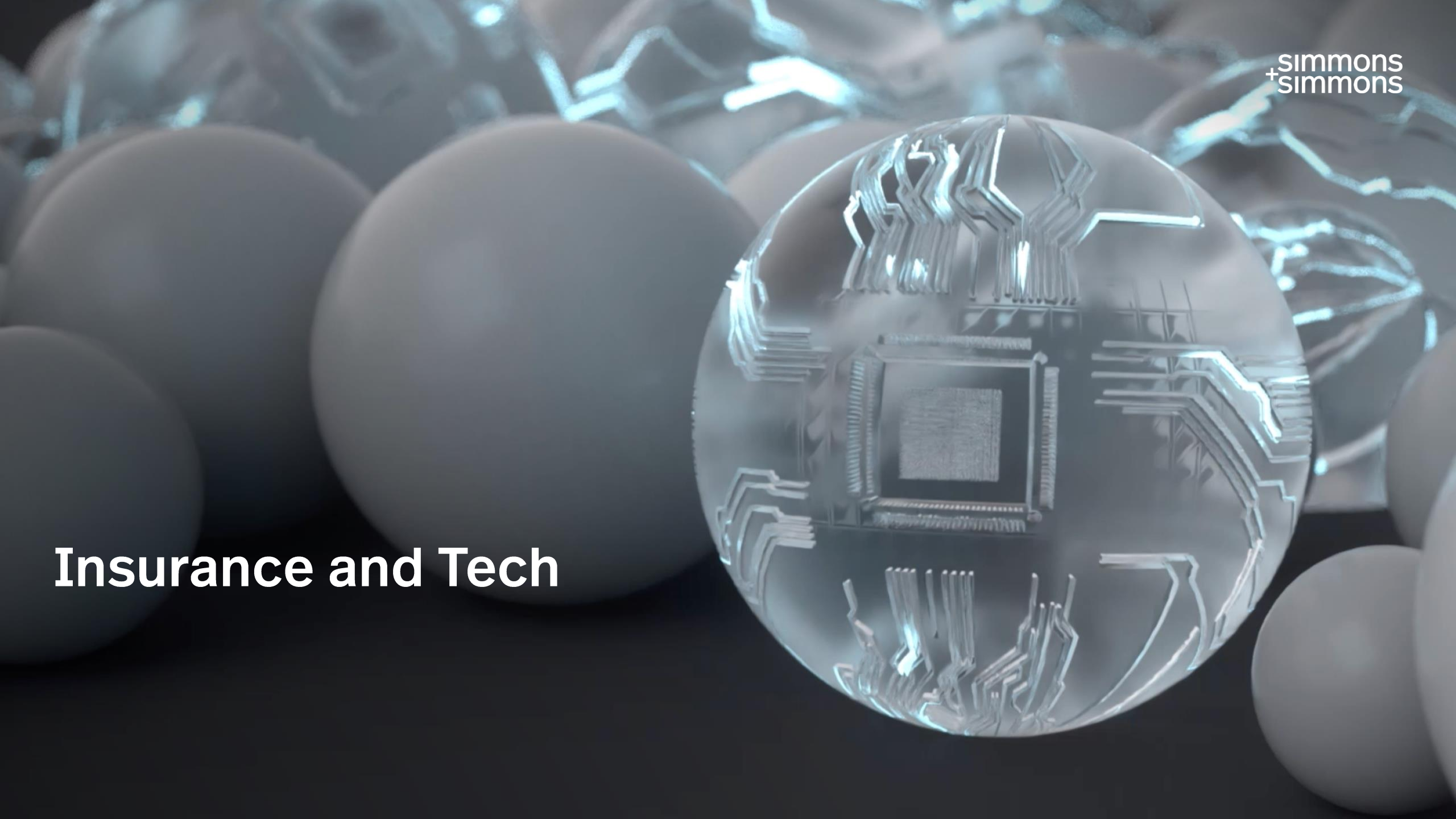
- Gli attacchi di sicurezza informatica nel settore sanitario possono mettere a **rischio la vita dei pazienti**. Questi attacchi possono colpire anche l'intera filiera sanitaria con conseguenze dannose per tutte le parti interessate

ENISA (ii)

Rapporto CSIRT dell'11 novembre 2021

- Il numero di minacce informatiche è in aumento proporzionalmente alla crescente popolarità di tecnologie emergenti come IoT, AI, biga data, cloud computing e la molteplicità dei dispositivi connessi tra loro

- Il rapporto CSIRT ha, dunque, come obiettivo quello di formulare raccomandazioni per rafforzare la capacità di risposta degli incidenti (IRC) nel settore sanitario



simmons
+simmons

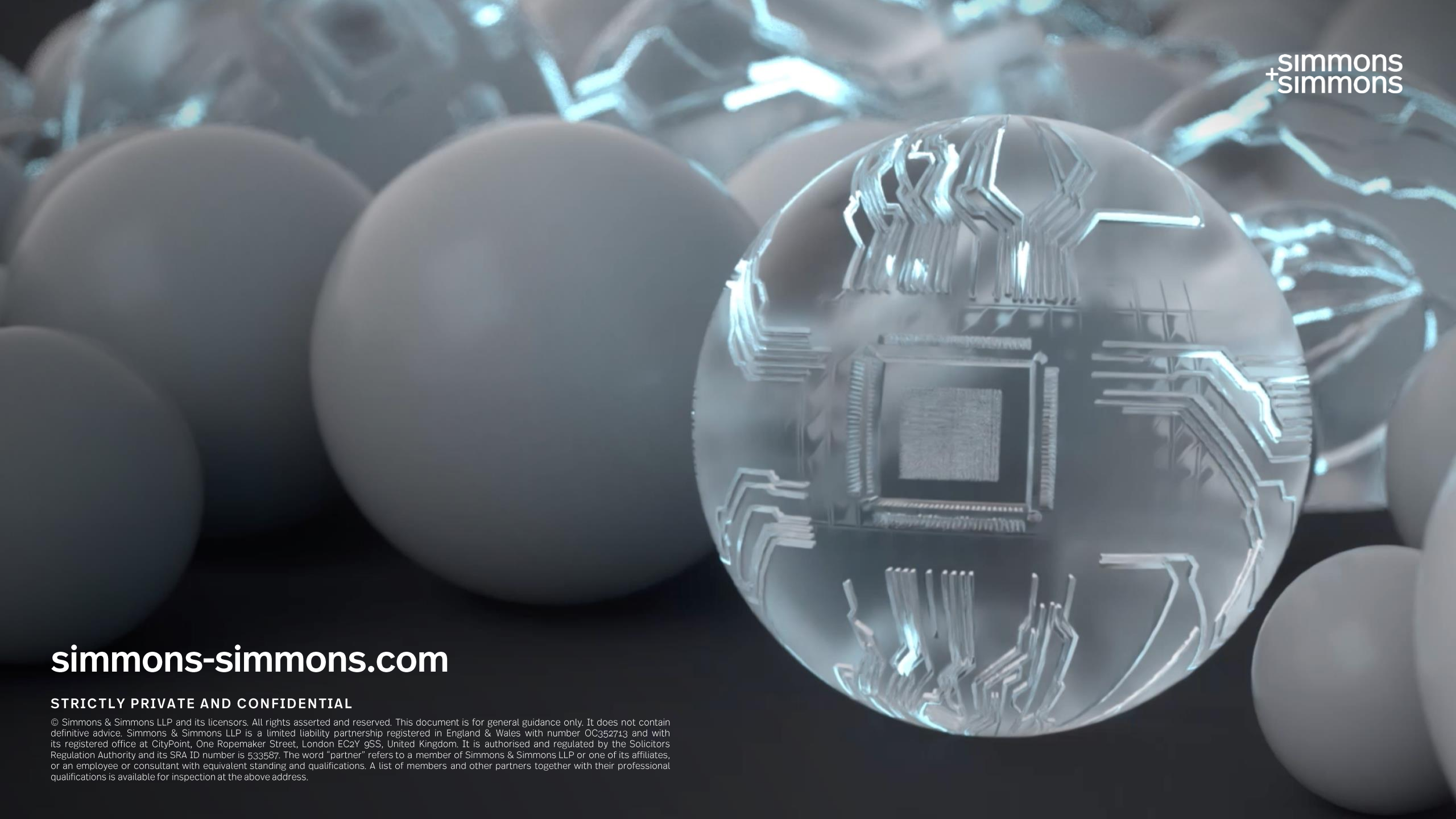
Insurance and Tech

Insurance and Tech

Come muoversi

- L’analisi del rischio e la sussistenza di polizze aggiornate
- L’adeguatezza della copertura sui rischi cyber
- Audit e confronto con i broker/Compagnie
- Phishing e cos’altro… (dolo o colpa)

Grazie.



simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.