
DELL Technologies /Forum
REAL
TRANSFORMATION
GLOBAL SPONSORS
intel
Microsoft

DELL Technologies /Forum

Comprendere e gestire i rischi nella Supply Chain

Fabio Battelli, Partner Deloitte

Deloitte.

La Cyber Security e le Terze Parti

Comprendere e gestire i rischi nella Supply Chain

Fabio Battelli, Partner
CISSP, CISA, CISM, ISO 27001, PRINCE2 e ITIL Certified

Negli ultimi anni i più clamorosi Data Breach sono avvenuti attaccando fornitori e terze parti collegate alle vittime…

Target

Nel 2013 oltre **110 milioni** di client interessati e 40 milioni di carte di credito rubate. Attacco avvenuto attraverso la violazione di un fornitore HVAC (Fazio Mechanical Service)

US Office of Personnel Management

Nel 2015 circa **22 milioni** di record sottratti. L'attacco sembra originato dal fornitore di "background check" del personale (KeyPoint Government Solution)

The Home Depot

Nel 2014 oltre **56 milioni** di carte di credito a rischio. L'attacco è partito da credenziali sottrate ad una terza parte che consentito di accedere a rete e sistemi

Circa 100 Istituti finanziari

Attacco APT diretto a molteplici operatori finanziari con il presunto coinvolgimento di supplier. Sottratto denaro per **1 MLD** di dollari

NIST

80%

Di tutti i dati breach sono stati originati dalla supply chain

45%

Di tutti i dati breach interessavano fornitori dismessi

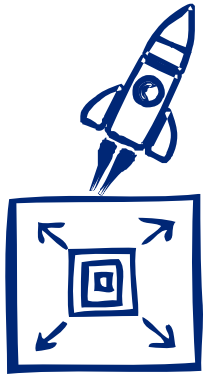
72%

Delle aziende non ha una piena visibilità della propria supply chain

59%

Delle società non ha alcun processo per valutare la sicurezza dei propri fornitori

Industry 4.0, IoT, Mobile e Cloud contribuiranno alla crescita esponenziale dell'universo digitale, accelerando lo sviluppo delle così dette "Extended Enterprise"…



Extended Enterprise

2013

4.4 ZB

L'universo digitale è enorme e cresce esponenzialmente…

2020

44 ZB

…ma anche rischi Cyber che minano la sicurezza delle informazioni e delle infrastrutture informatiche…

…generando opportunità ed innovazioni incredibili…

…rendendo le informazioni sempre più appetibili per le organizzazioni dedite al Cyber crime

Utilizzo di diverse metodologie e tecniche da parte di cybercriminali per ricavare un **guadagno economico** derivanti dall'attacco stesso

Utilizzo di determinate strategie e strumenti di attacco per sottrare intellectual property, finalizzato ad un **guadagno competitivo**

Dimensioni del fenomeno

CYBERCRIME

Costo mondiale del Cybercrime[1]
ca. 400 Miliardi $

Valore che considera sia i costi diretti (denaro sottratto a causa del crimine) sia i danni indiretti (danno di immagine, perdita di fatturato, costi di ripristino, ecc.)

≈

Volume di affari relativo al traffico di stupefacenti
ca. 411 Miliardi $

Redditività media del Cybercrime **20:1** *Rapporto medio tra profitto e costi necessari per realizzare i cyberattack[2]*

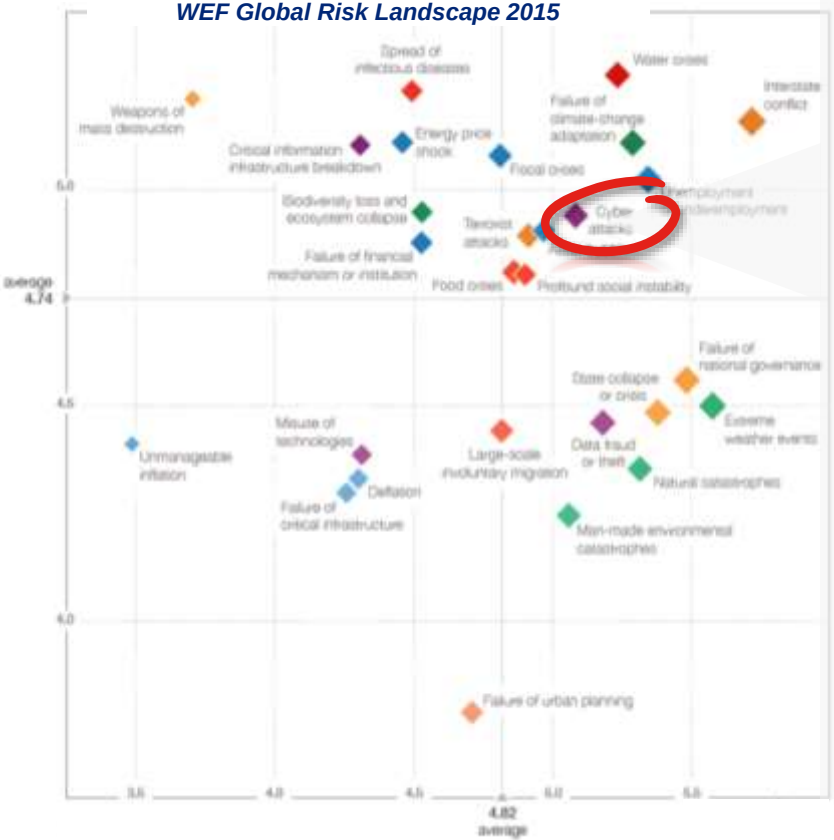
Investimento medio per acquistare un malware [3] **3.000 $**

Stima del profitto medio derivante dall'uso del malware **60.000 $**

[1]*Fonte: McAfee, Economic impact of cybercrime II – 2014*
[2]*Fonte: Cybercrime, Inc.: how profitable is the business? - 2014*
[3]*Fonte: Kaspersky Lab, Cybercrime blog - 2014*

Gli attacchi Cyber sono classificati al primo posto tra i rischi tecnologici dei prossimi 10 anni

WEF Global Risk Landscape 2015



Technological risks	18 months	10 years
Cyber attacks	23.3%	20.2%
Data fraud or theft		
Misuse of technologies		
Critical information infrastructure breakdown		

*«Secondo il WEF gli **attacchi Cyber** sono tra i **rischi più significativi** per i prossimi **10 anni**»*

WORLD ECONOMIC FORUM

Secondo diverse statistiche il Cyber Risk è anche quello che desta maggiori preoccupazioni dal punto di vista del Risk Manager

Cyber risks da parte dei Risk Manager*

2013
6%

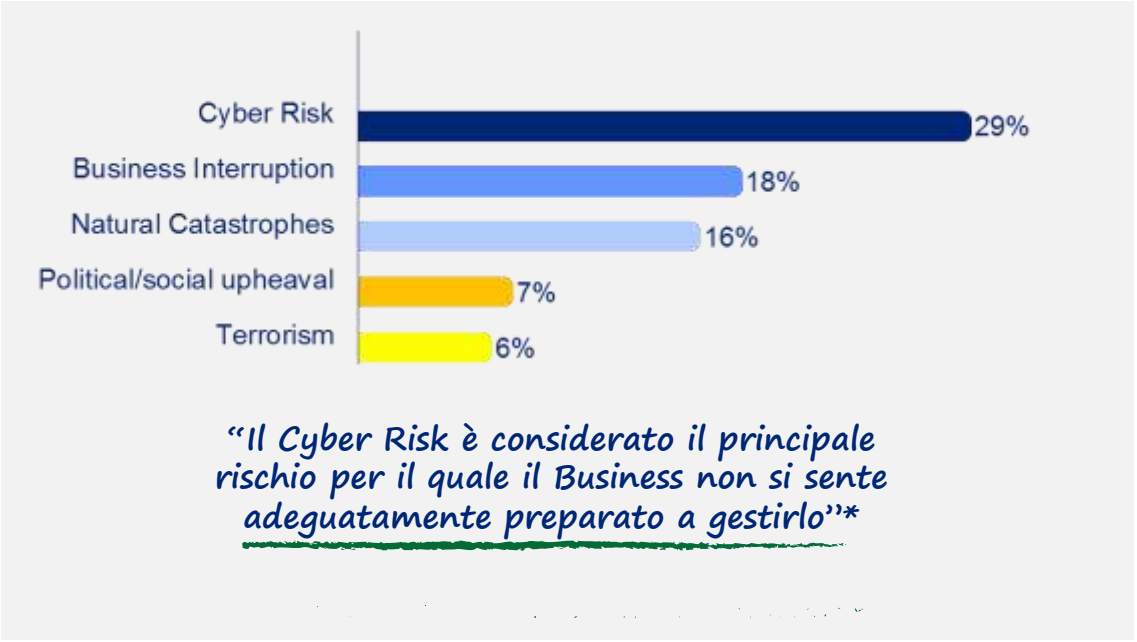
Ranked 15th

2014
12%

Ranked 8th

2015
17%

Ranked 5th



*"Il Cyber Risk è considerato il principale rischio per il quale il Business non si sente adeguatamente preparato a gestirlo"**

**Fonte: Jens Krickhahn, Practice Leader Cyber & Fidelity at AGCS Financial Lines Central & Eastern Europe Allianz Risk Barometer 2015. A survey of over 500 risk managers and experts from 40+ countries.*

Anche il Governo italiano negli ultimi anni ha fatto passi in avanti per lo sviluppo di una strategia Nazionale di Cyber Security

2006-14	Gen ‘13	Feb ‘14	Feb ‘15	Feb ‘17	Mar ‘17	Mag ‘18
Codice di Autodisciplina sugli obblighi del CdA in merito ai ”Principali Rischi afferenti all’emittente” e **Relazione sulla politica dell’informazione sulla Sicurezza**	Il **DPCM Monti** è la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale	**Quadro Strategico Nazionale e Piano Nazionale** individuano profili, indirizzi operativi, obiettivi da conseguire e linee d’azione per concretizzare il Quadro	**Cyber Security Framework Nazionale** per le Aziende, Organizzazioni e sistema Paese	**Il DPCM Gentiloni** è la Direttiva che definisce il nuovo programma nazionale in materia di Cyber Security	**Piano Nazionale 2017** individua i nuovi indirizzi operativi per la protezione cibernetica e la sicurezza informatica	**Attuazione della Direttiva NIS** riguardante la sicurezza dei sistemi, delle reti e informazioni
						

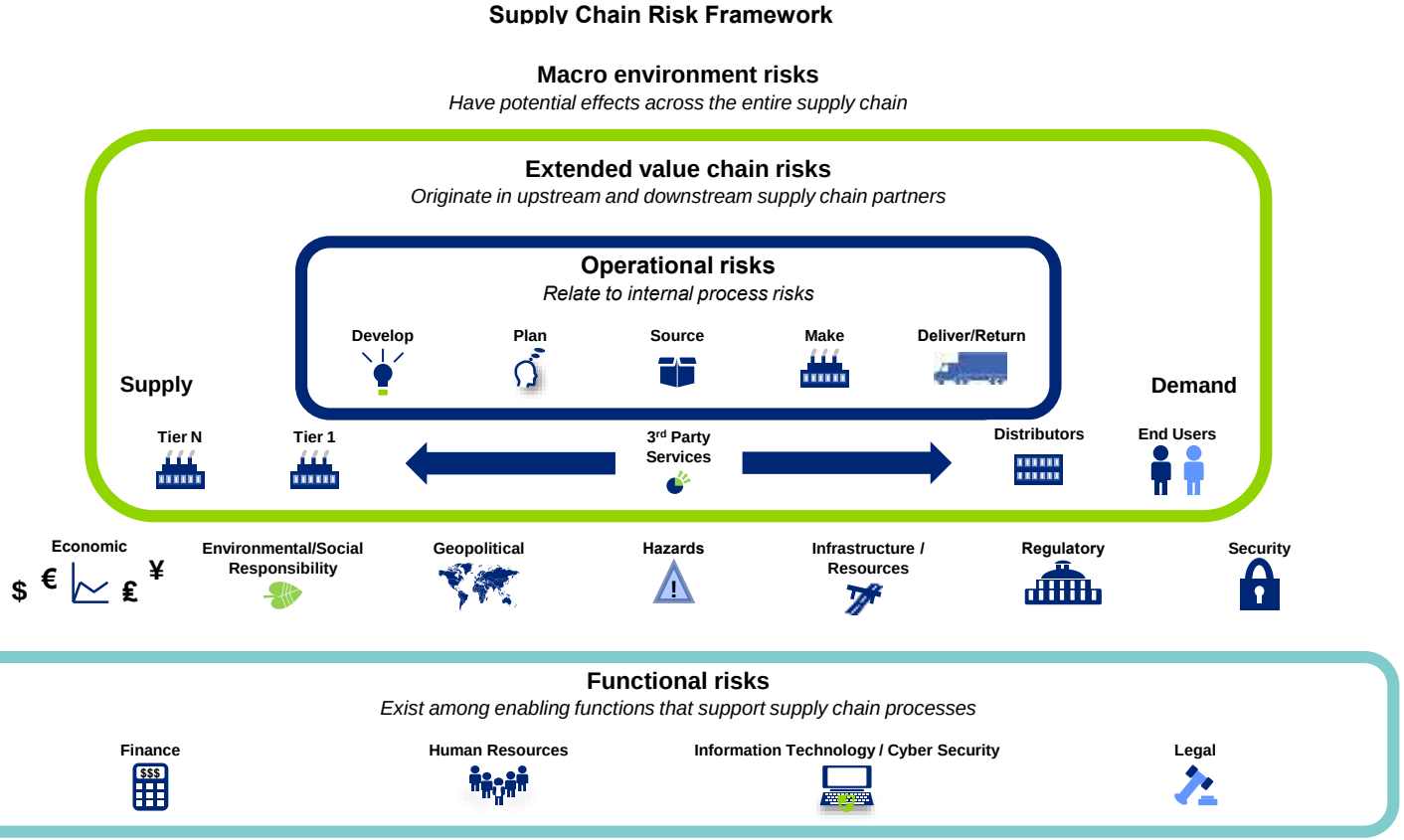
Il Codice di Autodisciplina di Borsa Italiana prevede obblighi e interventi per la gestione dei rischi

Il comitato di Corporate Governance di Borsa Italiana ha definito gli obblighi del Consiglio di Amministrazione in merito ai ”Principali Rischi afferenti all’emittente”

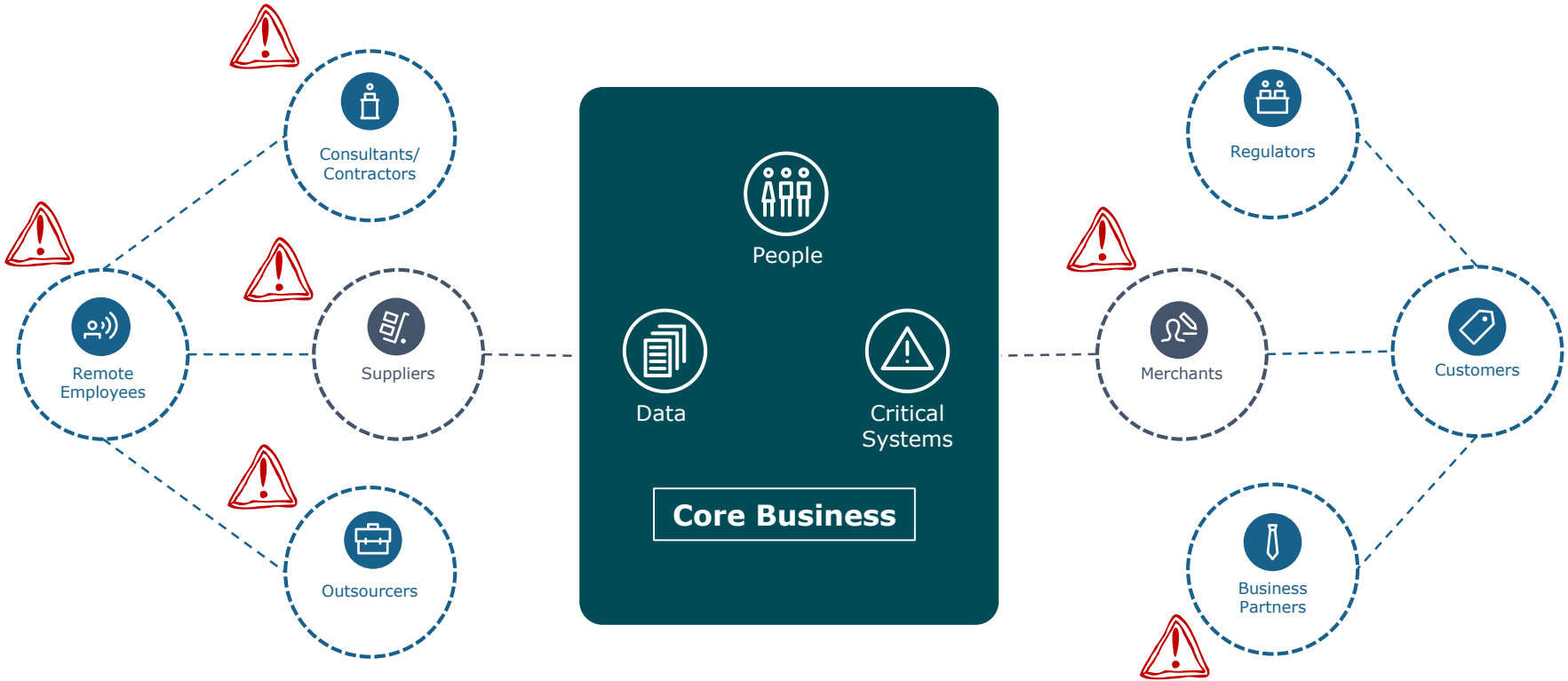
- Art. 7 – Sistema di controllo interno e di gestione dei rischi
- Criteri applicativi
- 7.C.1. Il consiglio di amministrazione, previo parere del comitato controllo e rischi:
- a) definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all’emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell’impresa coerente con gli obiettivi strategici individuati;

Le aziende quotate sono chiamate a rilasciare ogni anno una **dichiarazione di conformità**

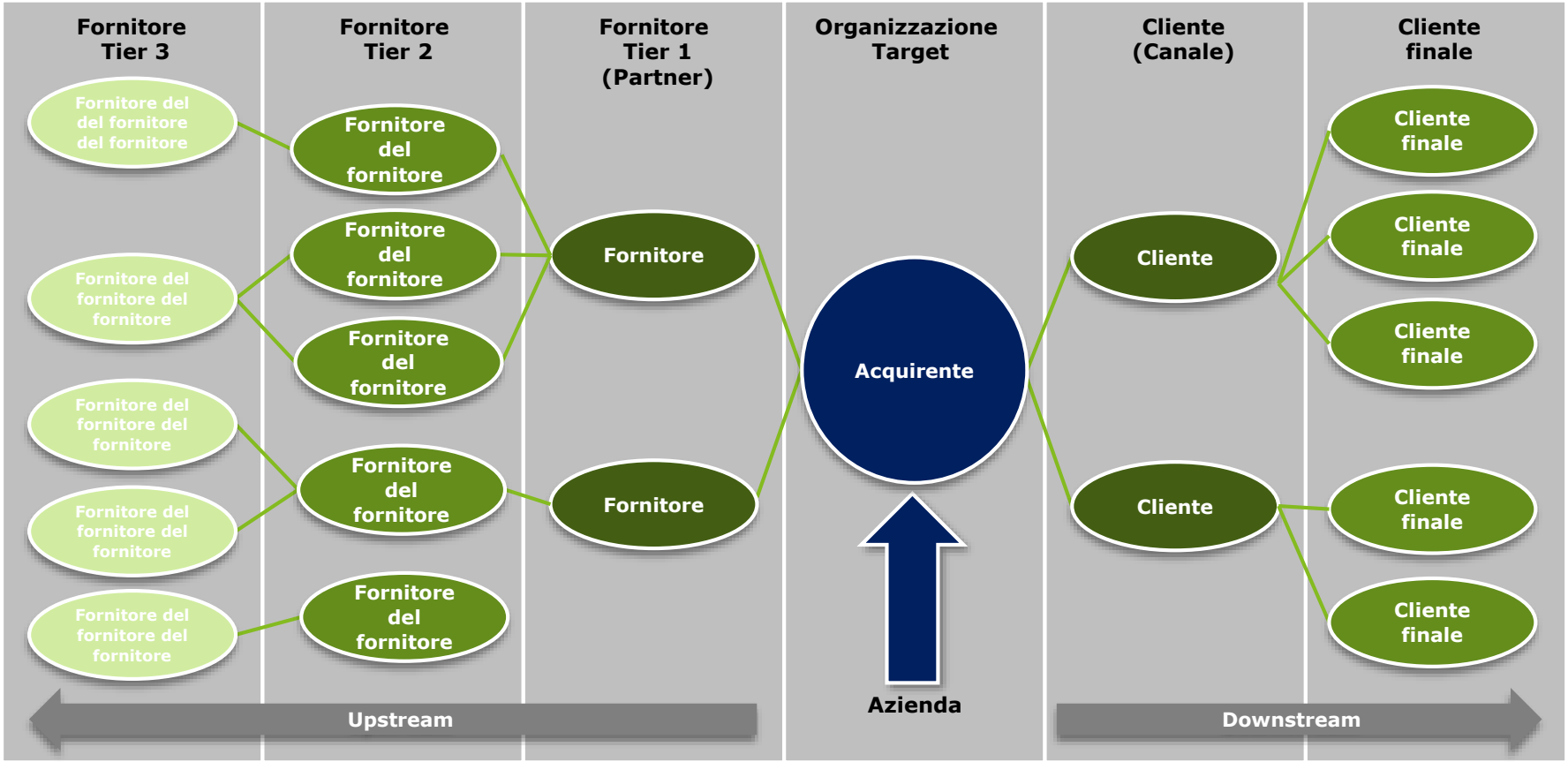
I rischi che interessano la Supply Chain sono molteplici e spesso correlati tra loro…



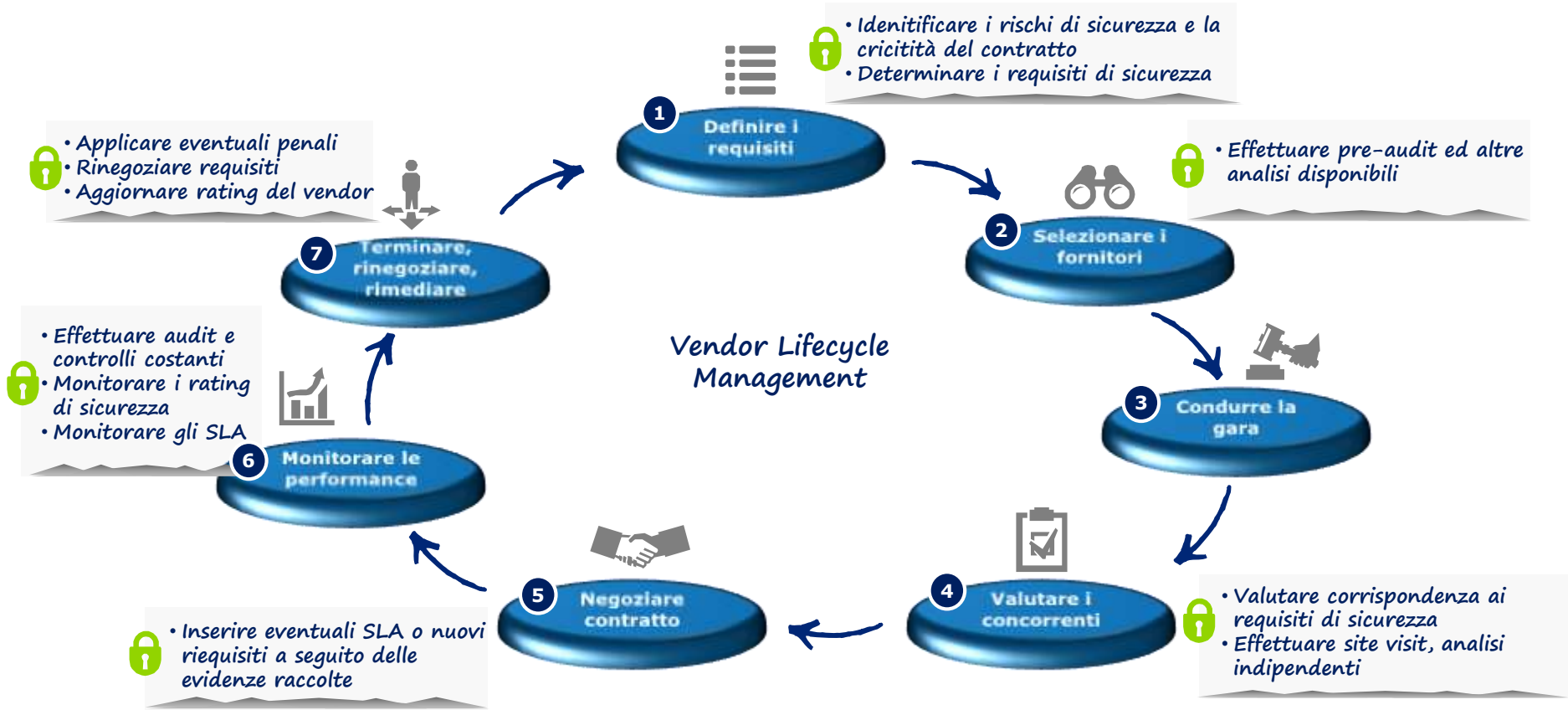
…tra questi il rischio Cyber introduce numerose vulnerabilità, ampliando notevolmente la superficie degli attacchi



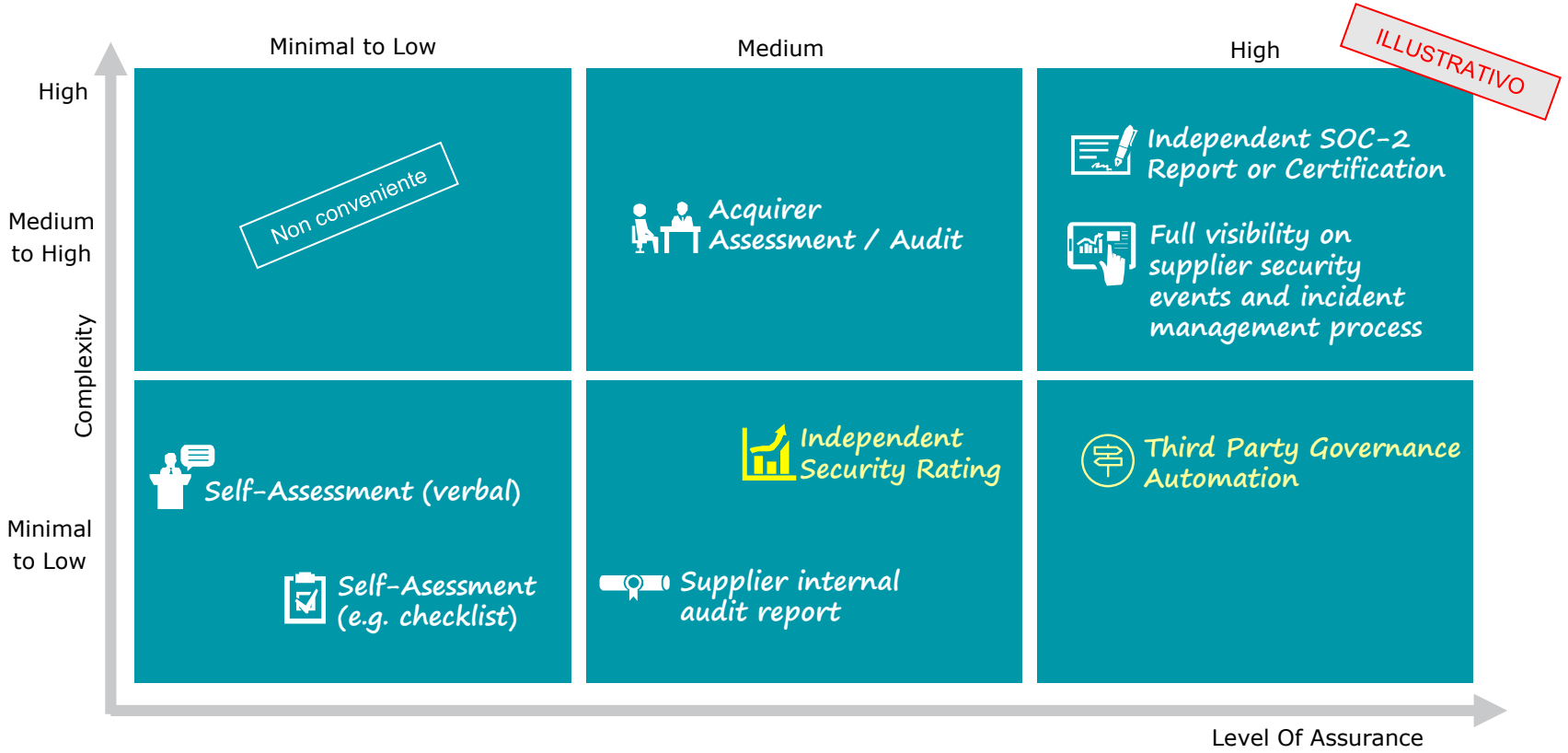
In alcuni settori la supply chain può raggiungere diramazioni complesse che rendono il controllo della cyber security molto sfidante



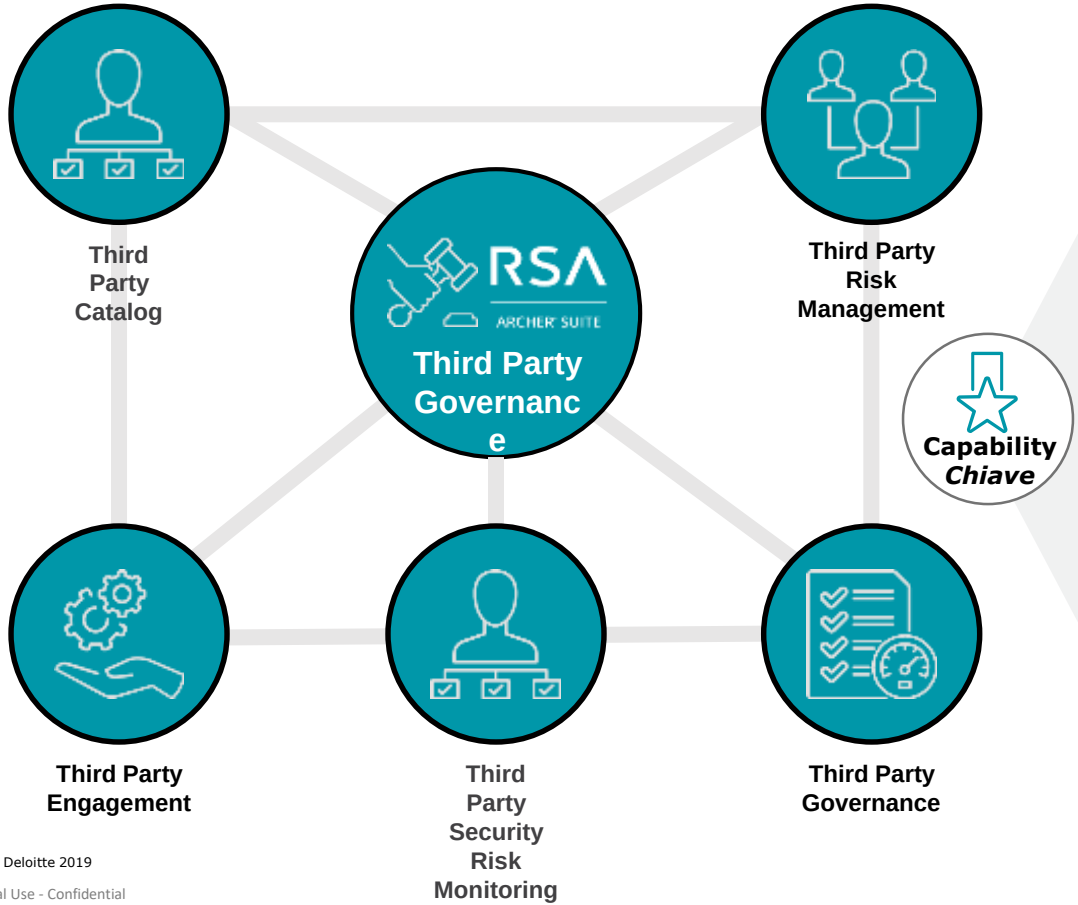
La gestione del rischio Cyber per risultare efficace dovrebbe essere perfettamente integrata nel ciclo di vita dei fornitori… (vendor management)



Monitorare le performance di sicurezza dei fornitori: esempio di differenti tecniche e livelli di "assurance"



3rd party Governance: automazione attraverso la soluzione Archer GRC



3rd Party Life-Cycle

Gestione del ciclo di vita del fornitore, dall'on-boarding alla dismissione

Business Context

Definizione delle dipendenze e del contesto di business/organizzativo in cui opera il fornitore

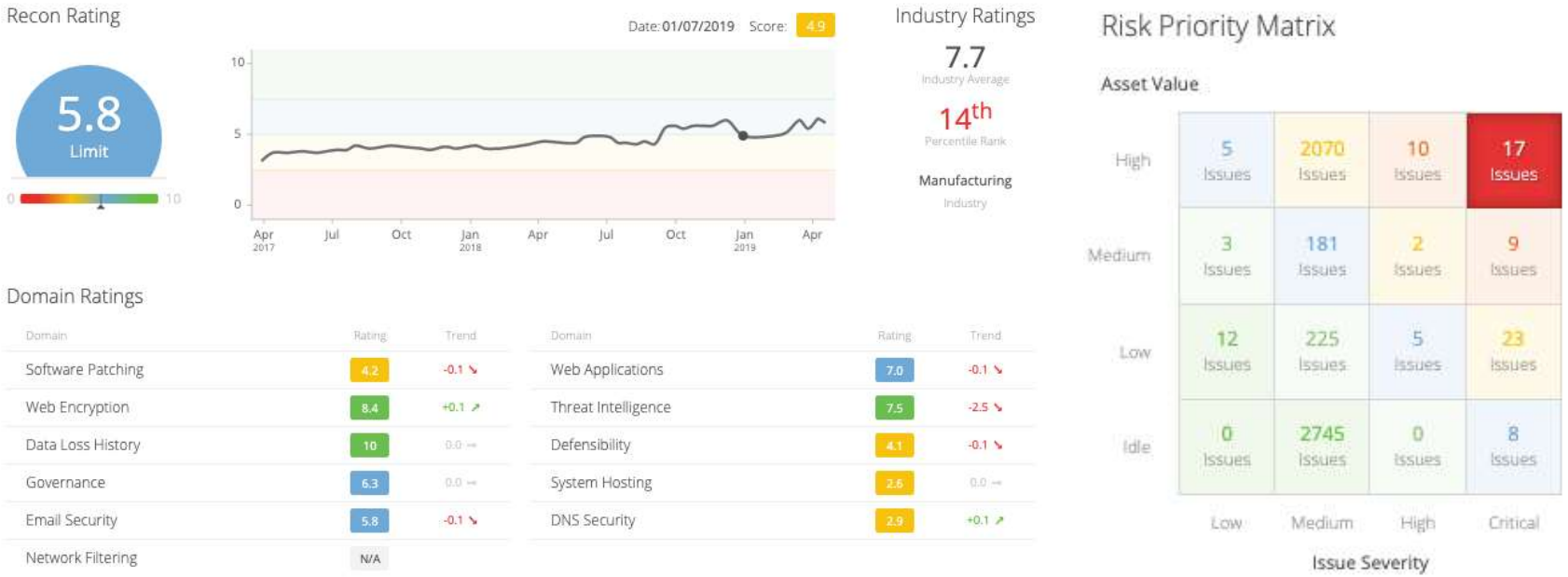
Integrated Risk Management

Prevenzione e gestione continua ed integrate dei rischi (cyber, finanziari, continuità, ecc), inclusi quelli riferiti alle quarte parti

Performance Management

Valutazione continua delle performance, incluso "**security rating**" assegnato al fornitore

Esempio di Security Rating



RSA ARCHER® SUITE + riskrecon

Deloitte.


DELL Technologies