protiviti® Insights
Face the Future with Confidence

Settembre CYBER SECURITY 2021

a cura di / Enrico Ferretti
Managing Director

SUPPLY CHAIN SECURITY

Come gestire i rischi cyber connessi alle esternalizzazioni di processi e servizi

Il Governo ha di recente portato a 223 i soggetti inclusi nel **Perimetro di Sicurezza Nazionale Cibernetico** con il DPCM n. 81 del 14 aprile 2021, che integra un precedente DPCM (n. 131 del 30 luglio 2020) sugli obblighi per le imprese che nella catena di approvvigionamento utilizzano servizi/beni ICT di terze parti.

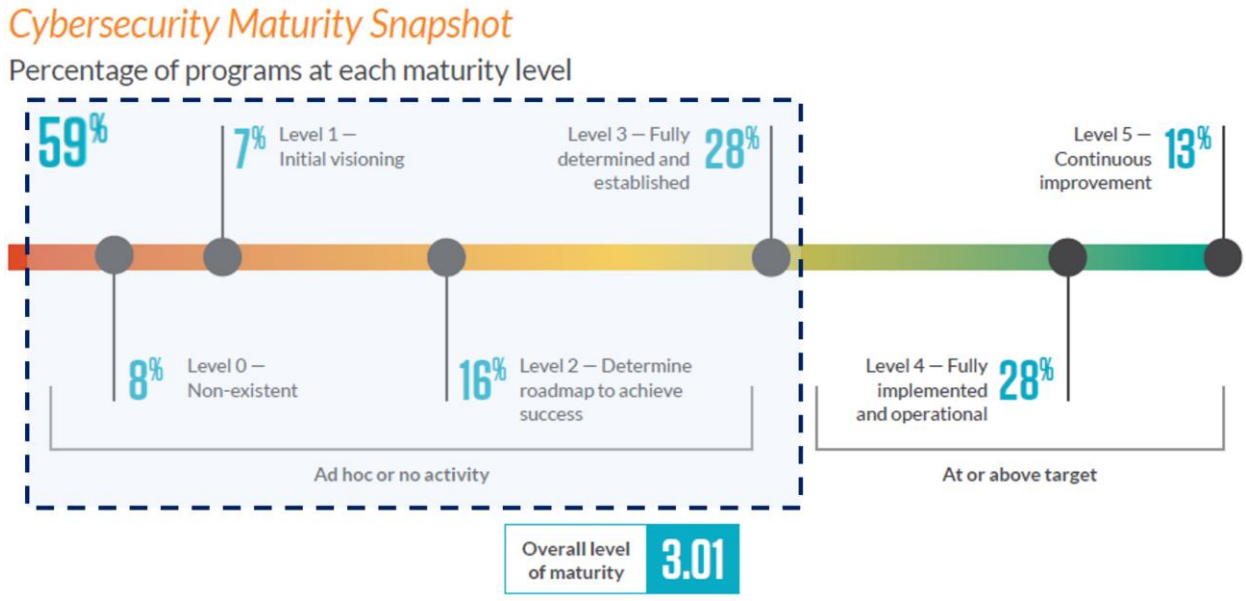
Il quadro disegnato da queste norme attribuisce alla cybersecurity una centralità per gli interessi del Paese: diventa, quindi, prioritaria la gestione dei rischi in tutte le fasi della supply chain, in particolare il monitoraggio dei rischi connessi all'utilizzo di "terze parti".

Questo soprattutto per le aziende che erogano servizi essenziali (per esempio, energia, telecomunicazioni e trasporti) o servizi digitali (per esempio, fornitori di servizi cloud, marketplace digitali).

A che punto sono le imprese nei programmi di ***Gestione dei rischi delle terze parti***? Protiviti ha condotto un'indagine a livello globale volta a rilevare il livello di maturità di tali programmi di, **intervistando circa 550** tra manager e professionisti di aziende di settori diversi, ai quali è stato chiesto di fornire una valutazione utilizzando una scala da 0 a 5 *(vedere lo schema)*.

At or above target	Level 5: Continuous improvement; or
	Level 4: Fully implemented and operational
Transitional	Level 3: Fully determined and established
Ad hoc or no activity	Level 2: Determine roadmap to achieve success;
	Level 1: Initial visioning; or
	Level 0: Non-existent

Tra i vari elementi presenti in un programma di gestione del rischio terze parti, spicca la compente Cyber Security: il risultato, riportato nella grafica qui sotto, indica che circa il 60% delle aziende si colloca su un valore minore o uguale alla media (3,01).



Analizzando la distribuzione delle risposte ricevute, si rileva come ci sia un divario importante tra i settori con livello di maturità superiore (come Servizi Finanziari, Assicurazioni, Healthcare e Telecomunicazioni) e gli altri settori (come Manifatturiero, Automotive, Logistica).

Morale: la maggioranza delle imprese deve ancora investire molto per raggiungere livelli adeguati di sicurezza e mitigare i rischi legati all'esternalizzazione di processi e servizi.

Tutto questo mentre i cyber attack verso la supply chain crescono in numero e qualità.

- Il più grave, nel 2020, è stato l'attacco alla piattaforma SolarWinds Orion: un gruppo di hacker, sfruttando una falla nella rete, ha inserito una backdoor in un

  aggiornamento software della piattaforma consentendo loro di accedere alle reti di tutti i clienti di SolarWinds che, inconsapevolmente, hanno scaricato e installato l'aggiornamento *malevolo* sui propri sistemi. Le vittime sono state circa 17.000, soprattutto in USA, UK e Singapore, ed un'indagine condotta tra diverse di loro ha stimato una media di 12 milioni di Dollari di danni.

- Altro caso che ha fatto notizia è stato l'attacco alla Colonial Pipelines**,** la più grande rete di condutture degli Stati Uniti, che si è vista costretta a chiudere circa 9.000 chilometri del proprio oleodotto causando per diversi giorni una grave mancanza di approvvigionamento di carburante in tutta la costa orientale degli Stati Uniti. L'attacco è avvenuto attraverso un ransomware, probabilmente veicolato attraverso una e-mail di phishing, installato involontariamente da un dipendente dell'azienda. Un nuovo esempio di come la vulnerabilità dell'infrastruttura di un'organizzazione possa mettere in crisi un'intera comunità di clienti, causando, oltre all'interruzione di approvvigionamento, anche un aumento del prezzo del petrolio.

L'importanza di gestire adeguatamente i rischi di cyber security della Supply Chain è testimoniata anche da specifici obblighi introdotti da recenti normative, come il Decreto Presidente della Repubblica n. 54/2021 sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC).

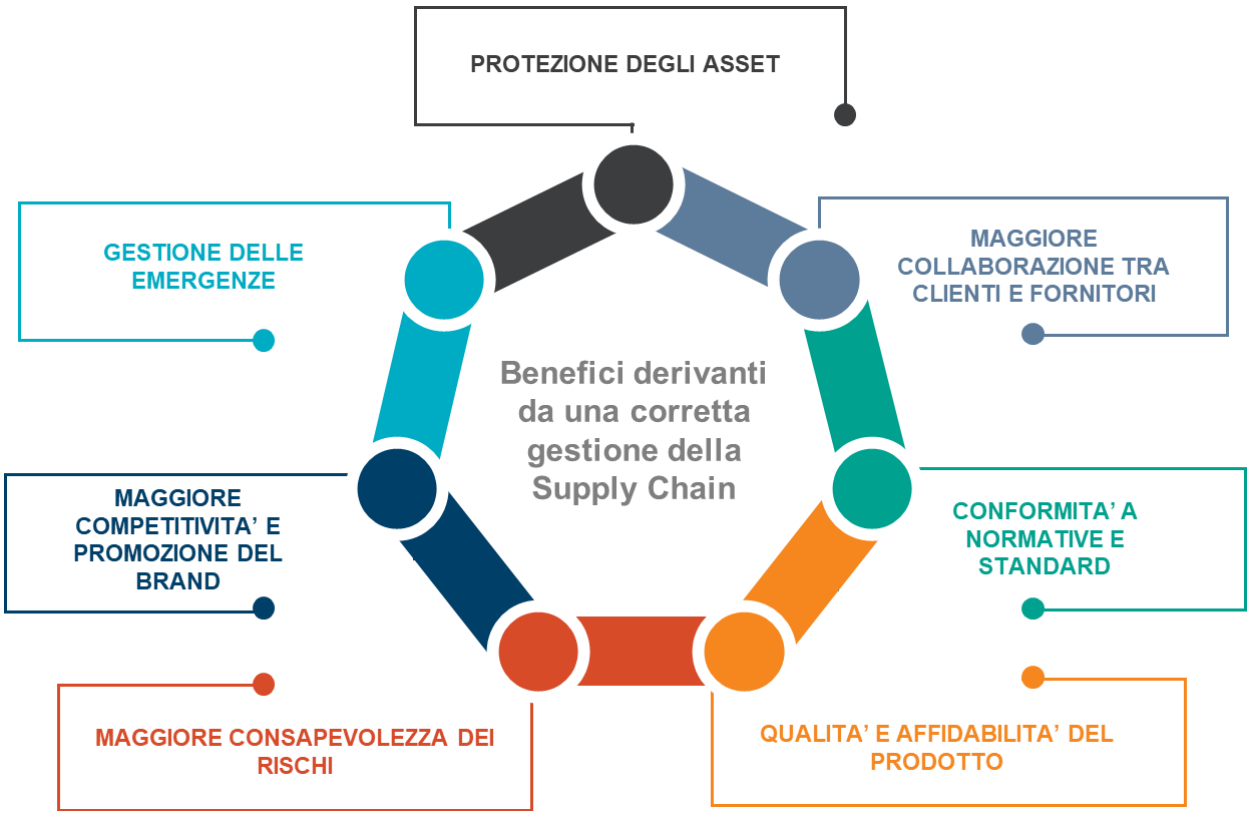
Il Decreto stabilisce procedure e termini per le valutazioni del CVCN (Centro di Valutazione e Certificazione Nazionale) e dei CV (Centri di Valutazione) sui servizi e/o forniture ICT che le organizzazioni incluse nel Perimetro intendono acquistare da terze parti, sulla base del livello di rischio associato alla fornitura richiesta. La non ottemperanza potrebbe comportare gravi sanzioni, amministrative e penali.

Sta quindi prendendo forma uno scenario di rischi e adempimenti, formali e sostanziali. Come gestire e integrare nei propri sistemi produttivi componenti e/o servizi di terze parti contenendo i rischi di sicurezza? Protiviti ha sviluppato un approccio metodologico alla Supply Chain Security che in questa edizione dell'Insights spieghiamo in dettaglio.

La Supply Chain Security in 4 fasi

La mancata adozione di un approccio strutturato alla gestione della Security nella Supply Chain può esporre le organizzazioni a scenari di rischio rilevanti (*evidenziati nella grafica qui sotto*).

I benefici di una buona gestione, in termini di sicurezza e logistica sono numerosi (*vedere la grafica*):



L'approccio suggerito da Protiviti parte dagli standard internazionali applicabili alla Supply Chain (ISO 28000 e NIST SP 800-161) e agli ambiti di sicurezza interessati (ISO 27001 e ISO 22301) e dall'adozione di strumenti di supporto per individuare le criticità nelle diverse fasi.

Protiviti ha sviluppato strumenti specifici per la gestione della sicurezza, che si articolano in quattro le fasi operative:

1. L'identificazione del contesto e dei criteri di valutazione

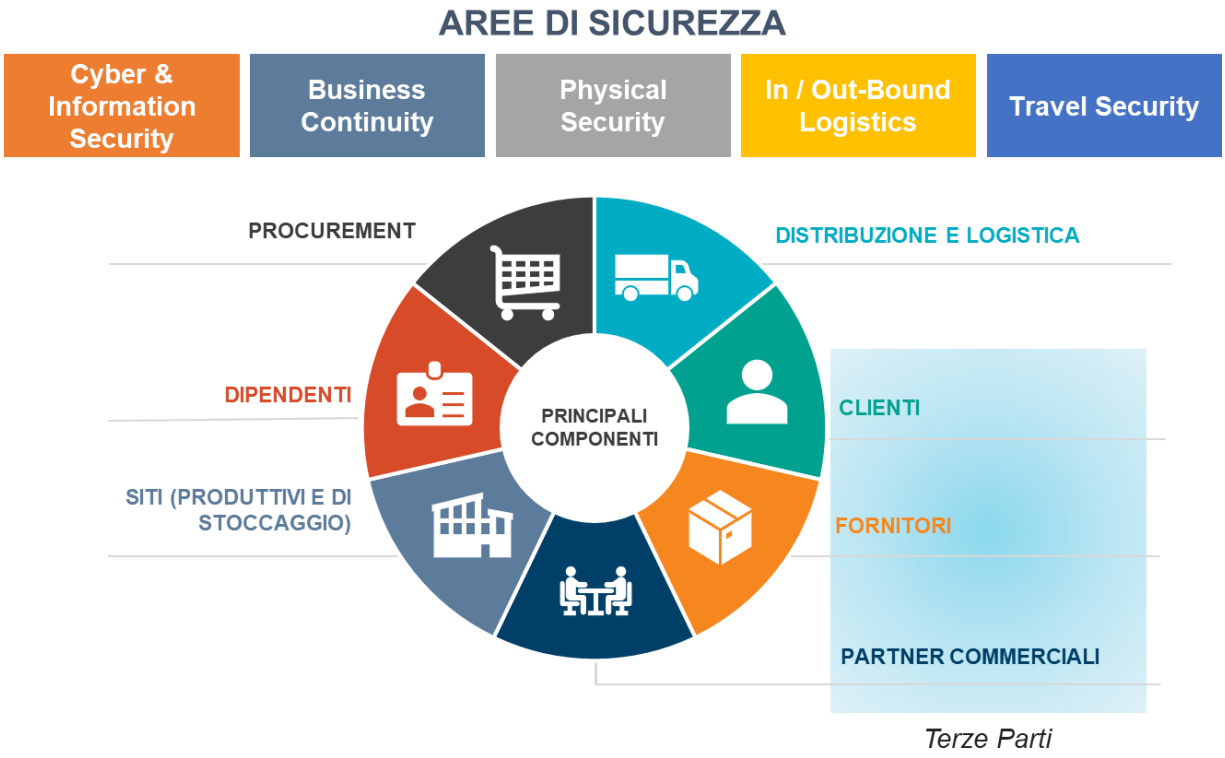
La comprensione del contesto e l'analisi della documentazione esistente (per esempio, procedura di selezione dei fornitori, valutazioni passate) è il primo passo da compiere. Questo consente di definire le aree di intervento e identificare puntualmente i soggetti da coinvolgere nelle successive attività (per esempio, qualità e continuità del servizio offerto, sicurezza delle informazioni e protezione dei dati personali, formazione dei dipendenti in ambito sicurezza, incidenti di sicurezza occorsi).

In accordo con le specifiche esigenze dell'impresa, si definiscono gli elementi funzionali alle successive valutazioni. Queste informazioni risultano necessarie per definire gli elementi cardine (per esempio, minacce, soglie di valutazione, rischio residuo accettabile) che poi permetteranno di verificare l'attuazione dei presìdi di sicurezza.

2. La definizione del modello di valutazione

Il passo successivo è la progettazione e applicazione di un framework di controlli, basati sui principali standard e normative, che considera le minacce delle singole fasi operative. Il framework di Protiviti, con oltre 150 controlli in cinque aree della sicurezza (Cyber & Information Security, Business Continuity, Physical Security, In/Out-Bound Logistic, Travel Security), consente di determinare il livello di maturità delle misure di sicurezza adottate (*vedere grafico seguente*).

Il framework coinvolge tutte le componenti della Supply Chain (per esempio, terze parti, servizi di distribuzione e logistica, risorse umane, siti produttivi).



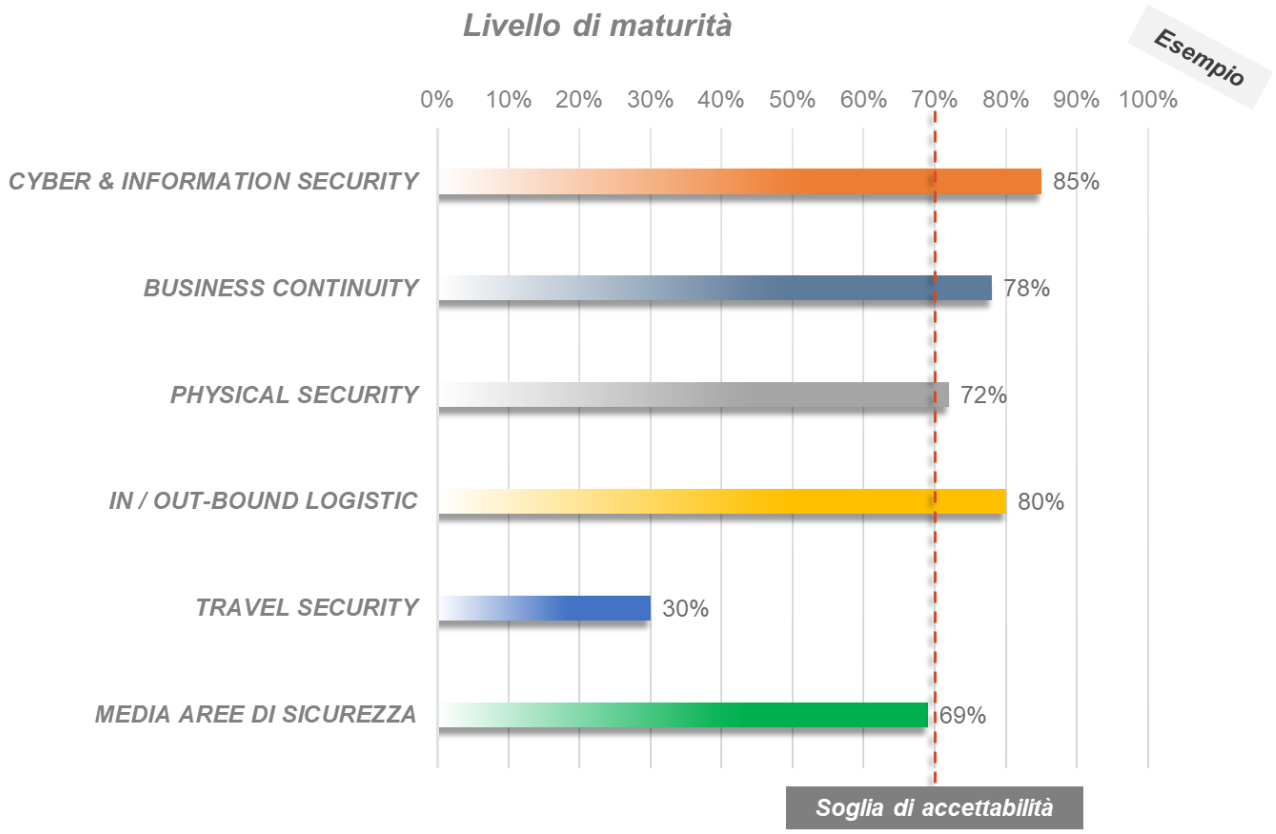
3. La selezione degli strumenti di supporto

L'analisi degli strumenti operativi in uso consente di verificare la maturità dell'organizzazione rispetto a una gestione strutturata del rischio cyber. L'obiettivo è rendere efficace e snello il modello di Risk Management impiegando strumenti adeguati a valutare i livelli di sicurezza e compliance. Potranno essere modelli di assessment o questionari di dettaglio, che permettano di determinare un livello di rischio preliminare associato al fornitore da utilizzare come parametro per le successive analisi.

4. L'esecuzione dei controlli

Nella fase finale, si selezionano le componenti della Supply Chain e/o le terze parti rilevanti con il relativo status contrattuale (per esempio, contratto da stipulare, fornitura in corso, scadenza di contratto). L'obiettivo è definire una graduatoria delle priorità di analisi della sicurezza, per eseguire la verifica puntuale delle misure in essere e definire gli opportuni piani di miglioramento.

Una corretta valutazione attraverso l'applicazione del framework consente di avere un quadro chiaro della sicurezza e delle potenziali minacce. Questo consente di determinare non solo le contromisure, ma anche le evidenze da produrre per garantirne la corretta applicazione.



L'approccio di Protiviti per costruire sistemi integrati

L'approccio di Protiviti alla gestione della Supply Chain Security e del Third Party Risk Management è fondato su competenze di procurement, operation, compliance, risk management, security e audit. È un approccio che risponde efficacemente all'esigenza delle organizzazioni di gestire i rischi attraverso sistemi integrati.

Protiviti ha un'esperienza pluriennale nel Cyber Risk Management e nel Cyber Security Advisory costruita assistendo grandi gruppi e imprese. I numerosi mandati di Risk Management su complesse Supply Chain hanno permesso di testare e affinare la metodologia rendendola applicabile in tutte le imprese che intendono adottare un approccio *risk based*.

CONTATTI

— **Enrico Ferretti** / Managing Director / enrico.ferretti@protiviti.it