REGIONE PIEMONTE

CSI your digital partner

WEBINAR

SICURI di essere SICURI?

Direttiva NIS2: la scadenza si avvicina...

I rischi e la sicurezza della catena di fornitura

Federico Lucia | CSI Piemonte

Chi sono

Giurista informatico specializzato in **criminalità informatica** e **digital forensics**, sono **Risk Manager** certificato **RIMAP® Professional**, nonché lead auditor ISO 45001, ISO 27001 e ISO 22301 e implementer della norma ISO 27701.

Manager presso il **CSI Piemonte,** ho pluriennale esperienza in materia di **Business Continuity**, **Risk Management**, **Safety** e **Security**.

Docente e formatore, sono Program Manager del **CSI Digital Campus**.

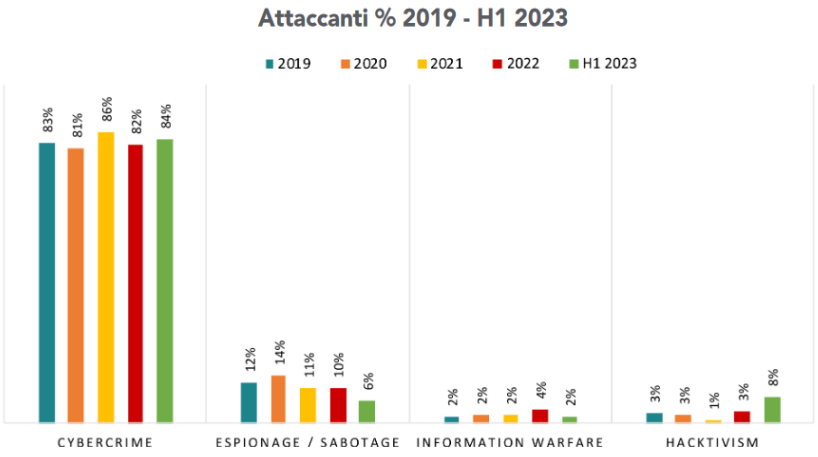
Sono membro di **ANRA** e della **Clusit Community for Security**, nonché segretario consigliere dell'associazione **Digital Forensics Alumni**.

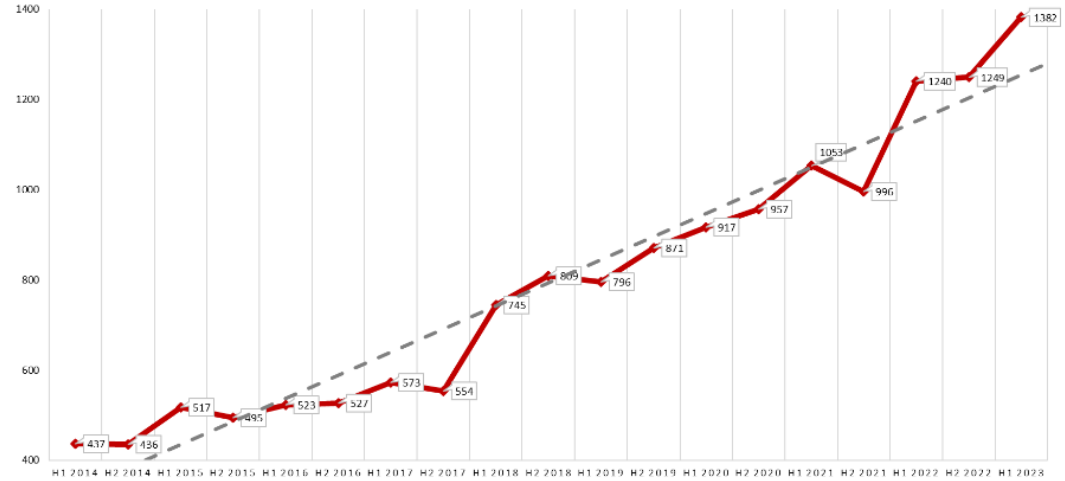
Autore di svariati articoli presso giornali e riviste del settore, ho inoltre collaborato alla realizzazione del libro «**Il Nuovo Codice della Privacy**», in collaborazione con l'Università di Modena e Reggio Emilia.

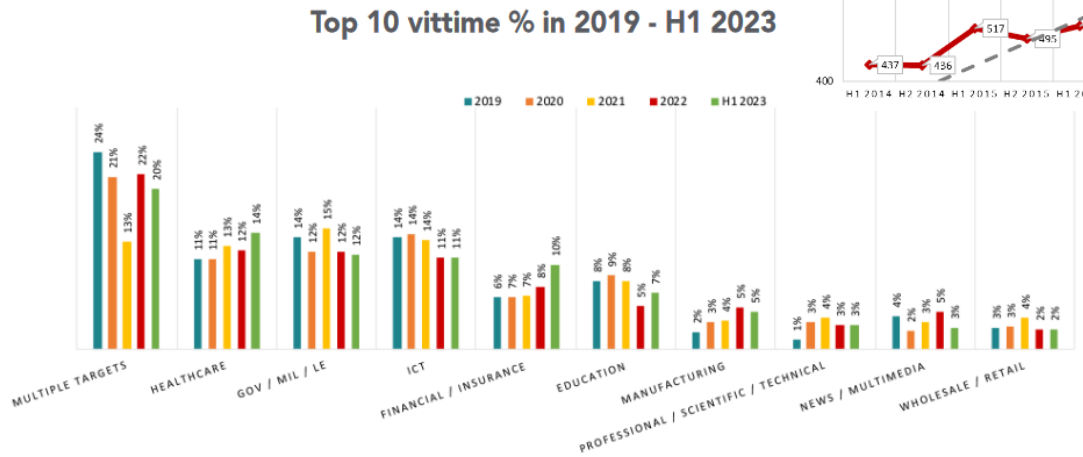
Nel 2023 sono stato premiato nella categoria «**Innovation of the Year**» alla prima edizione degli **Italian Risk Awards**.

Source: Allianz Risk Barometer 2024. Total number of respondents: 955. Respondents could select more than one risk. Top 4 answers.

IL CONTESTO | distribuzione degli attacchi IT







Source: Clusit – Rapporto 2023 sulla Sicurezza ICT in Italia
aggiornamento giugno 2023

2021

La Evergreen si incaglia nel canale di Suez

Danno: 9.6bn $ / giorno (tutto il mondo)

2023

Crisi del Mar Rosso

Danno: 95M € / giorno (solo l'Italia… per ora…)

IL CONTESTO | tanto non capiterà mai… parte 2…

PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

PA Digitale S.p.A. informa

che i suoi sistemi, a causa di un significativo evento di sicurezza che ha interessato il proprio fornitore di servizi cloud Westpole S.p.A., non sono disponibili a partire dalla prima mattina dell'8 dicembre 2023.

Da preliminari comunicazioni ricevute, la società Westpole S.p.A. notificava di aver riscontrato la cifratura della propria intera infrastruttura informatica, che risultava così interamente compromessa.

PA Digitale S.p.A. esprime il proprio rammarico per questa spiacevole vicenda, indipendente dalla propria volontà e al di fuori del proprio controllo e sta attivamente operando per ottenere dal fornitore Westpole S.p.A. il ripristino di un'infrastruttura affidabile, assieme ad una dettagliata ricostruzione dell'evento e delle conseguenze.

L'obiettivo di PA Digitale S.p.A. è quello di assicurare il rapido ripristino a partire dai prossimi giorni delle funzioni essenziali e, progressivamente, il patrimonio informativo e di dati disponibile.

Al momento non risulta esfiltrazione di dati.

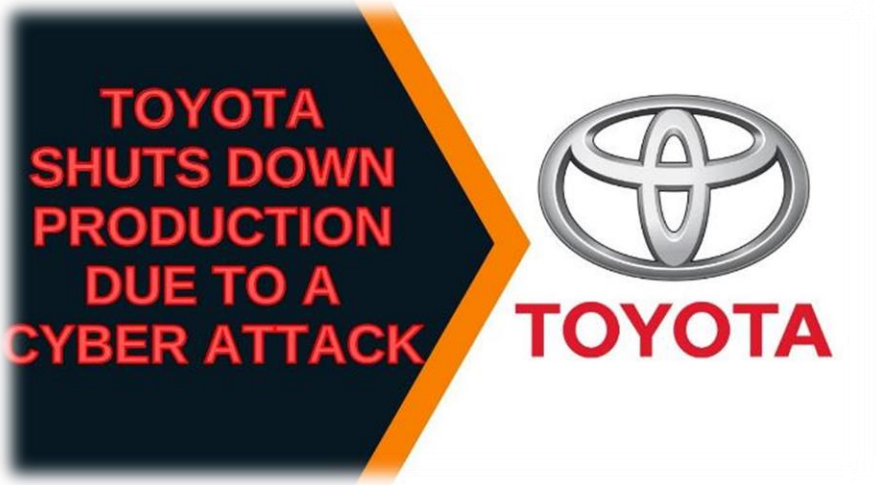
Westpole S.p.A. prima e conseguentemente PA Digitale S.p.A. poi hanno provveduto alla denuncia dell'accaduto alle Autorità competenti.

PA Digitale S.p.A., perciò, non appena otterrà le necessarie informazioni sull'incidente dal fornitore dei servizi cloud Westpole S.p.A., procederà a comunicazioni di dettaglio agli utenti.

Pieve Fissiraga, 11/12/2023

Attacco Ransomware a Westpole

Oltre 1.000 enti della PA impattati.
Vulnerabilità di Business Continuity della catena di fornitura.
Impattati anche servizi critici e soggetti private.



Attacco Ransomware a Kojima Industries

Arresto di 28 catene di produzione su 14 stabilimenti di Toyota.
Perdite per circa 13.000 automobile anche a causa del processo produttivo Just In Time della casa automobolistica.

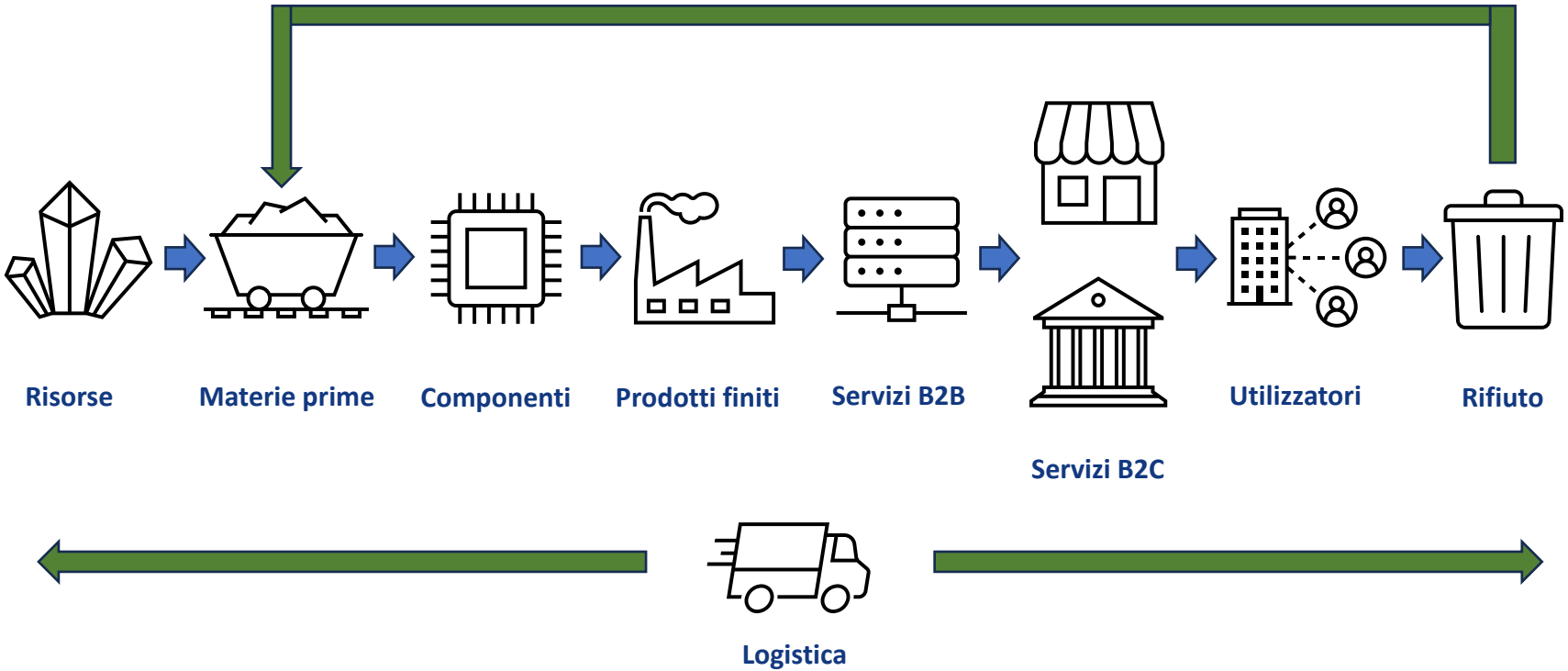
- Degrado del **contesto geopolitico** e **cyberwarfare**
- **Shortage** di risorse e **aumento dei costi** della logistica
- **Attacchi informatici** sempre più sofisticati (ed economici…)
- Difficile **visibilità e controllo sui fornitori** (e sui loro fornitori…)
- Mancanza di **competenze e risorse**

- Valutare i **rischi connessi alla supply chain** (approccio olistico)
- Adottare **misure di mitigazione**
- **Cooperazione** tra organizzazioni e istituzioni

Effetto Domino

Gli incidenti sono il risultato finale di una catena di fattori di incidenti. Tanti piccoli eventi possono portare ad un grande evento.

La catena del valore



(C) Riservatezza - Confidentiality

Garantire la riservatezza (privacy) dei dati creati, custoditi, trasmessi e diffusi evitandone l'accesso a utenti non autorizzati

(I) Integrità - Integrity

Garantire la protezione del dato da qualsiasi tentativo di manomissione dello stesso, prevenendo alterazione o cancellazione non autorizzata.

(A) Disponibilità - Availability

Garantire la continuità alla fruizione e all'accesso di dati e servizi, impedendo interruzioni nell'erogazione di servizi hardware e software

- **Malware** e ransomware
- Aumento dei **costi**
- **Potere contrattuale**
- **Data breach**
- Business **Interruption**
- **Vulnerabilità** del software
- Difficoltà di **monitoraggio**
- Perdita di **controllo**
- Fattore umano: **atti dolosi da insider**
- Fattore umano: **shortage competenze**
- Fattore umano: **errore**
- Attacchi alla supply chain: «**island hopping**»
- Attacchi alla supply chain: «**watering hole**»
- **Compliance**

Risk Management

+

Supply Chain Management

=

Supply Chain Risk Management

COME SI VALUTA?

- Definire gli **obiettivi**
- Identificare le **aree di rischio** e identificare i **fornitori critici su quelle aree**
- Definire le **soglie di tolleranza**
  - Risk appetite (propensione al rischio)
  - Risk tolerance (devianza tollerabile rispetto alla propensione)
  - Risk capacity (massimo livello di rischio sopportabile)
- **Analizzare** il rischio (Probabilità e Impatti)
- **Valutare** il rischio rispetto alle soglie
- Identificare gli **indicatori di rischio** e i parametri di controllo (**KRI**)
- Identificare gli **indicatori di performance** e i parametri di controllo (**KPI**)
- Scegliere l'**azione di trattamento** dei rischi valutati
- **Monitoraggio** e **revisione** periodica

SCEGLIAMO I MIGLIORI….!

- Screening e classificazione dei fornitori, con rating di affidabilità
- Diversificare la catena di fornitura ove possibile
- Richiedere attestazioni e certificazioni (es. ISO 27001, ISO 22301)
- Prevedere clausole di notifica, monitoraggio e audit di 2° parte
- Prevedere clausole di garanzia nei confronti dei sub-fornitori

… E MANTENIAMO IL CONTROLLO!

- Coinvolgiamoli nelle esercitazioni e nei test
- Prevediamo monitoraggi e audit periodici basati sul rischio
- Condividiamo informazioni su minacce, vulnerabilità, rischi, azioni di mitigazione
- **Formazione e consapevolezza**

GRAZIE!

federico.lucia@csi.it
risk-bc@csi.it
digitalcampus@csi.it

DIGITALCAMPUS
guidiamo l'innovazione