L'IMPORTANZA DELLA CYBERSECURITY PER LE ORGANIZZAZIONI PRIVATE E PUBBLICHE

APAFORM, 25 Gennaio 2024

Greta Nasi

Agenda

- I Trend cybersecurity

- Threats, target e modelli decisionali

- Spunti per un'efficace gestione della strategia cyber: Re-framing dei modelli decisionali

Cybersecurity

Cybersecurity is "a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international policies through information-technological means"

Stevens, 2016
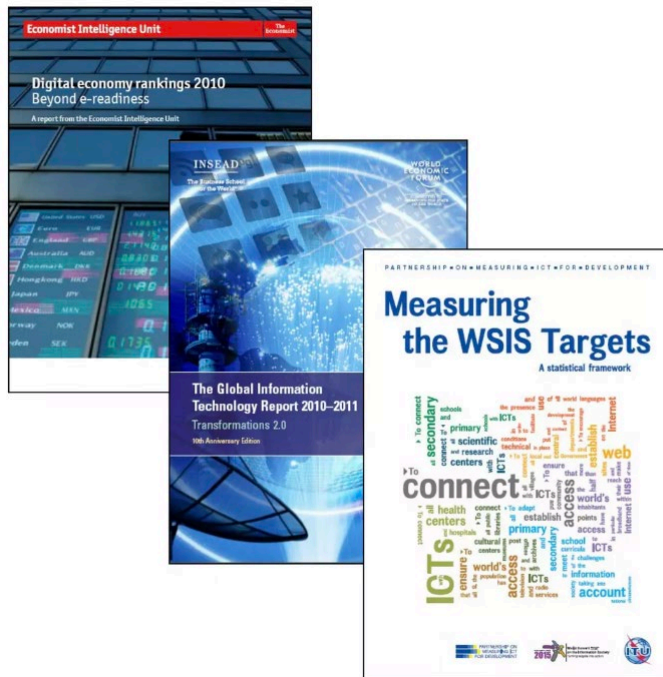
I trend attuali

Trend in cybersecurity

Globalizzazione

Cyberspace

Digital Transformation

Globalization

ICT & crescita economica, social well-being

Information society come determinante di migliori condizioni economiche e di vita

Digitale come elemento facilitatore
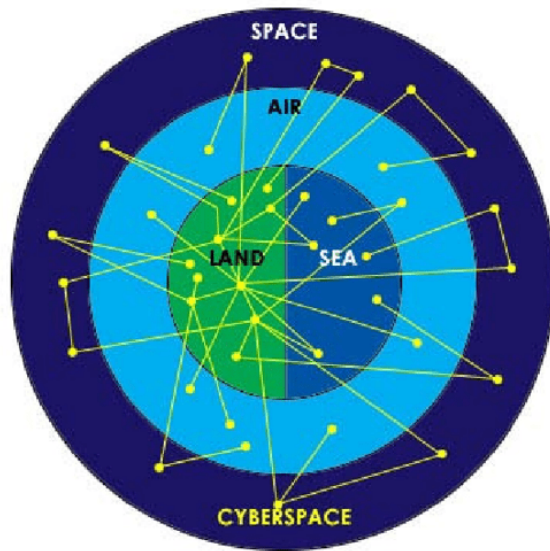
Connectivity e domini 1/2

25 billion connected devices by 2025

Working patterns has been accelerated by the COVID-19 pandemic – **40%** of EU workers switched to telework in early 2020.

IoT devices da from 15.1 billion in 2020 a 29 billion IoT devices in 2030.

Connectivity e domini 2/2

Cyberspace

Cyberspace is a virtual reality environment accessed through computer networks.

— William Gibson, Neuromancer, 1984

Cyberspace is a new strategic environment with its own structures and imperatives (Fischerkeller, M. P., Goldman P.O, Harknett R. J, 2022)

Cyberspace & cybersecurity

- Pervasività e uso di tecnologia implica la dipendenza

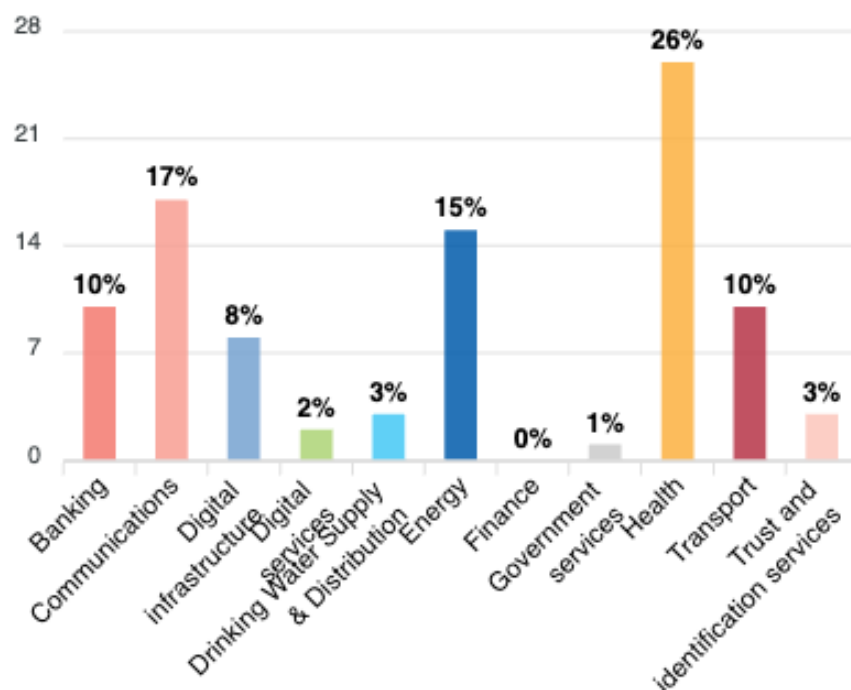- Aumento degli attacchi

- Impatto su fiducia nelle istituzioni
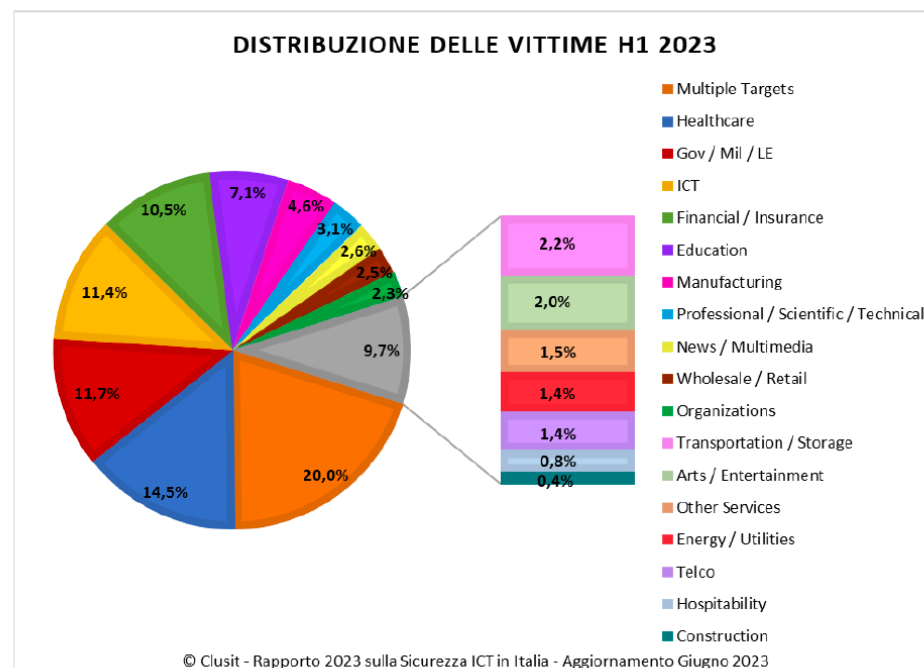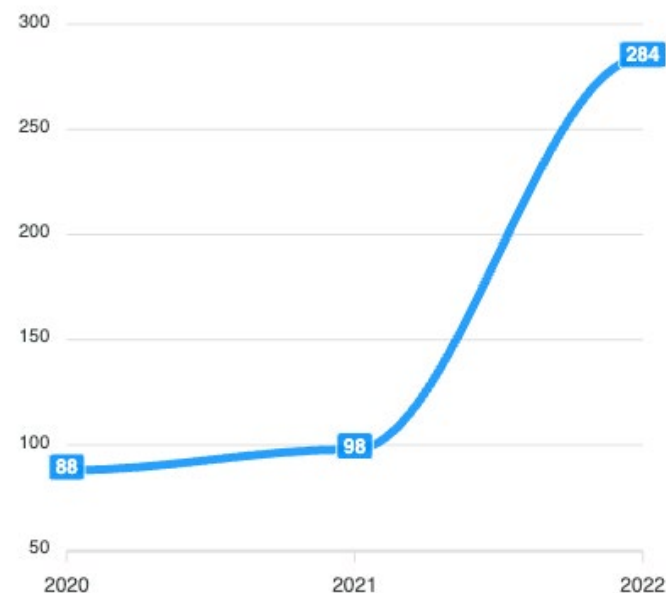

Rapporto Clusit Primo Semestre 2023

Trends, gap e proposta di re-framing dei modelli decisionali

Alcuni dati sugli attacchi

ENISA CIRAS, 2022

L'accelerazione dei cyber threats

Geopolitical threats.
The conflict between Russia and Ukraine has leaped into cyberspace through multiple cyberattacks, affecting several countries.

Attacks against the energy industry.
During the energy crisis in the EU, the EU energy industry has been the target of several cyberattacks that have jeopardized its operations.

Ransomware.
Security measures and the emergence of new ransomware operators increase competition. 60% of affected organizations may have paid the ransom.

Zero-day exploits.
Cyberhackers can better identify and exploit these vulnerabilities to achieve their goals.

Cyber attacks against public agencies.
Attacks against government institutions, including healthcare organizations, have increased by over 150% compared to 2021.

AI-enabled Disinformation/misinformation.
Escalating AI-enabled disinformation, deep fakes and disinformation-as-a-service

DDoS attacks.
DDoS attacks are growing in magnitude and getting more complex, moving towards mobile networks and IoT.
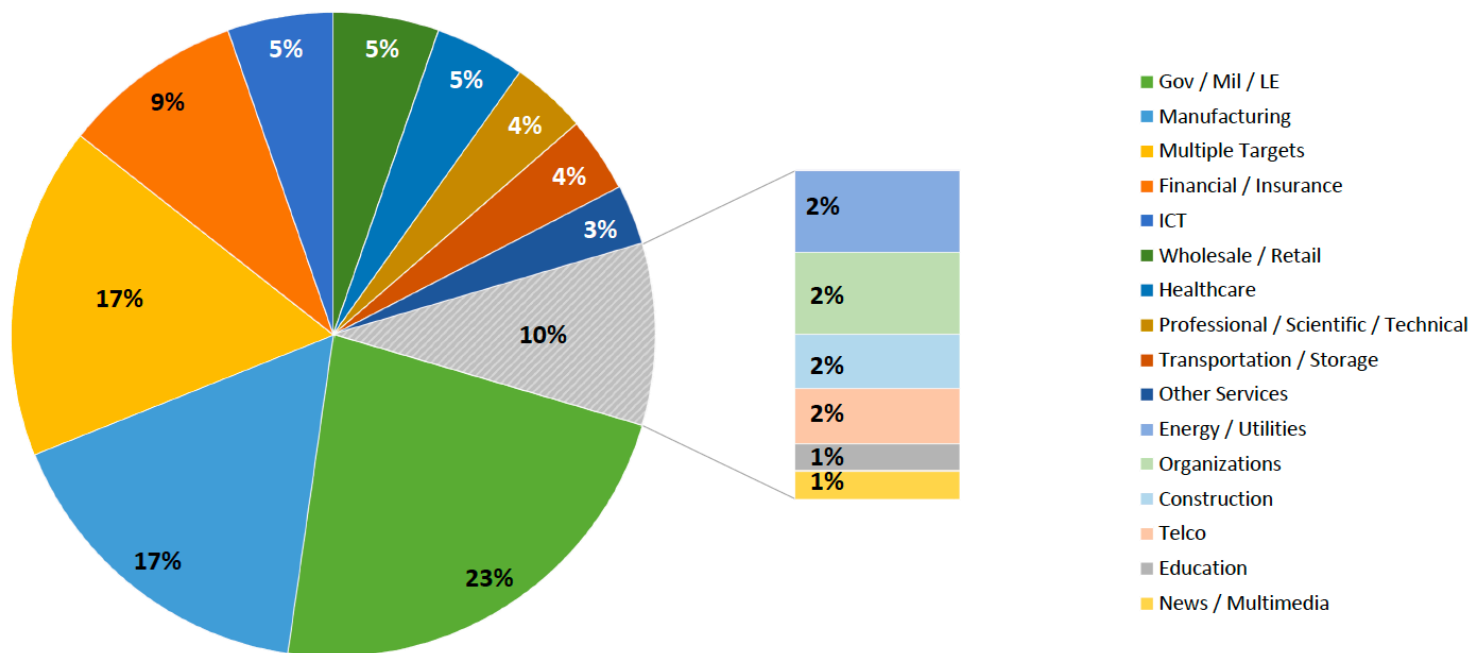
Hacktivism.
Hacktivists-motivated cyberattacks have been linked to conflicts and social and human rights disputes.

Crime as a service.
The price of malicious services offered on the dark web has fallen, due to increased competition.

ENISA Threat Landscape, 2022

Università Bocconi MILANO

Target

© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2023

Rapporto Clusit Primo Semestre 2023

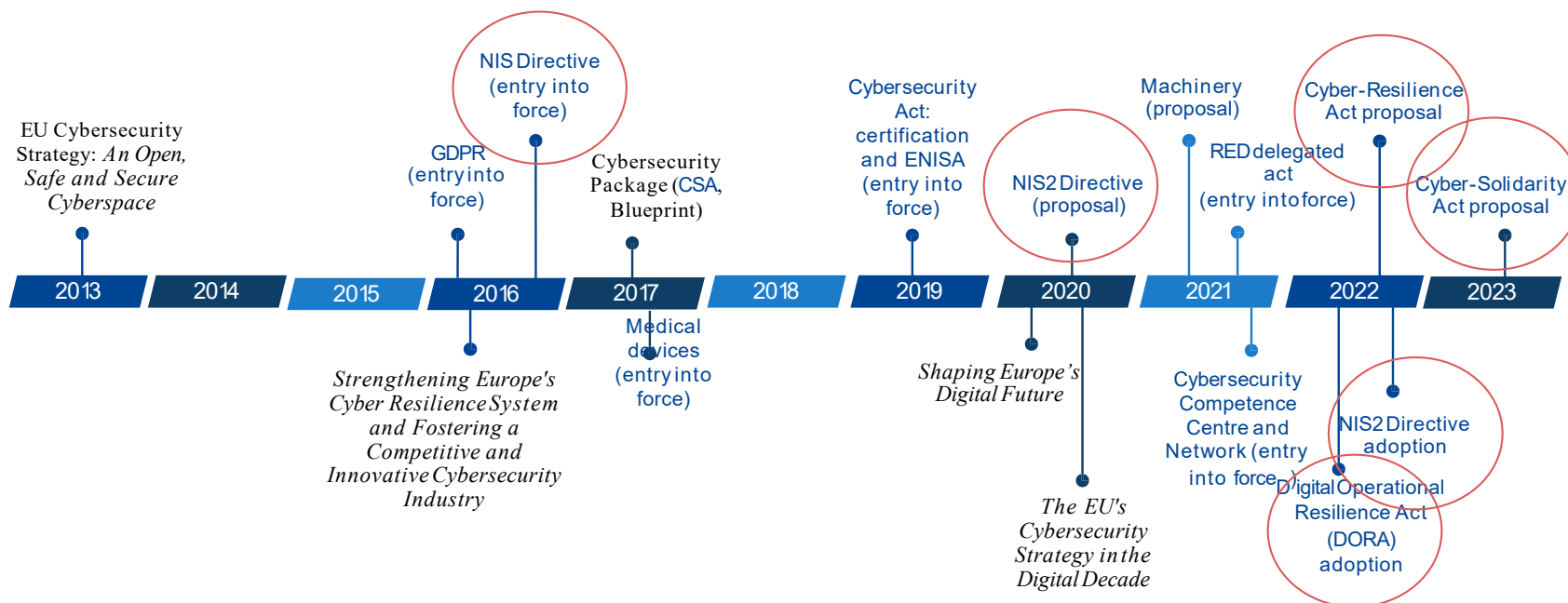# Il problema a livello organizzativo

Persone e capacità amministrativa
350,000 unfilled jobs in cybersecurity in the EU in 2022
Source: Cybersecurity Ventures

Cultura cyber
85% degli attacchi si poteva evitare
Data Breach investigation Verizon

Il decennio di policy EU

EU Cybersecurity
Strategy: *An Open,
Safe and Secure
Cyberspace*

NIS Directive
(entry into
force)

GDPR
(entry into
force)

Cybersecurity
Package (CSA,
Blueprint)

Cybersecurity
Act:
certification
and ENISA
(entry into
force)

Machinery
(proposal)

Cyber-Resilience
Act proposal

NIS2 Directive
(proposal)

RED delegated
act
(entry into force)

Cyber-Solidarity
Act proposal

| 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 |

Medical
devices
(entry into
force)

*Strengthening Europe's
Cyber Resilience System
and Fostering a
Competitive and
Innovative Cybersecurity
Industry*

*Shaping Europe's
Digital Future*

Cybersecurity
Competence
Centre and
Network (entry
into force)

NIS2 Directive
adoption

Digital Operational
Resilience Act
(DORA)
adoption

*The EU's
Cybersecurity
Strategy in the
Digital Decade*

Un contesto complesso dove prendere decisioni

ANSA.it › English › General News › **Alarm after pro-Russian hackers attack Italian institutions**

Alarm after pro-Russian hackers attack Italian institutions

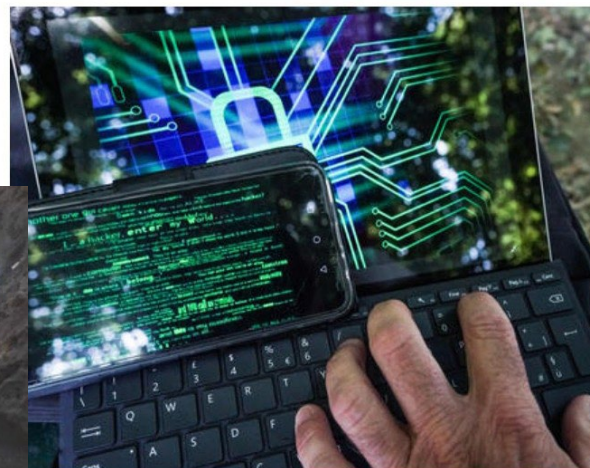'Killnet' claims responsibility, Senate, defence min sites hit

Redazione ANSA

 ROME

12 May 2022
10:17

NEWS

Suggerisci

REGIONE LAZIO

A causa di un attacco hacker il sito non è momentaneamente raggiungibile.
Ci scusiamo per il disagio, stiamo lavorando per ripristinare tutte le funzioni nel più breve tempo possibile.

Università Bocconi
MILANO

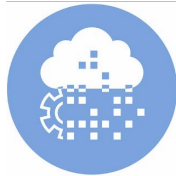## Woman dies during a ransomware attack on a German hospital

It could be the first death directly linked to a cybersecurity attack

By Nicole Wetsman | Sep 17, 2020, 3:11pm EDT

Prospettive di analisi differenti

Legal studies
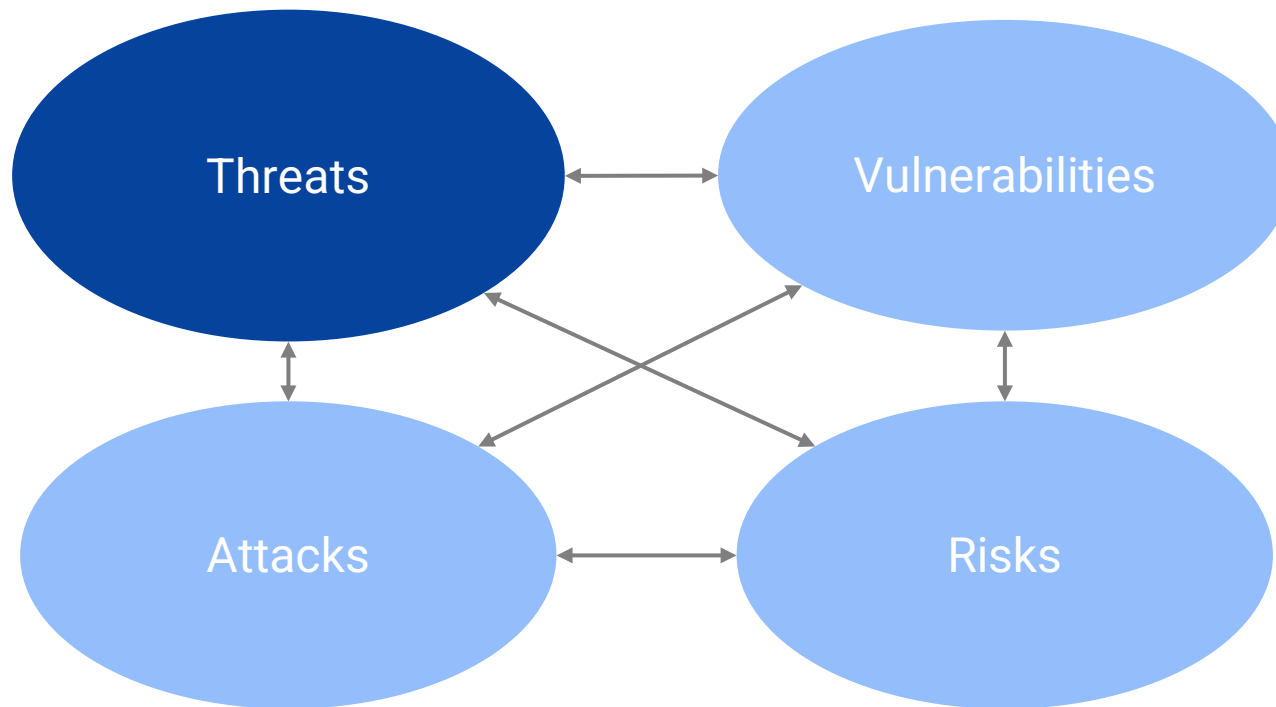
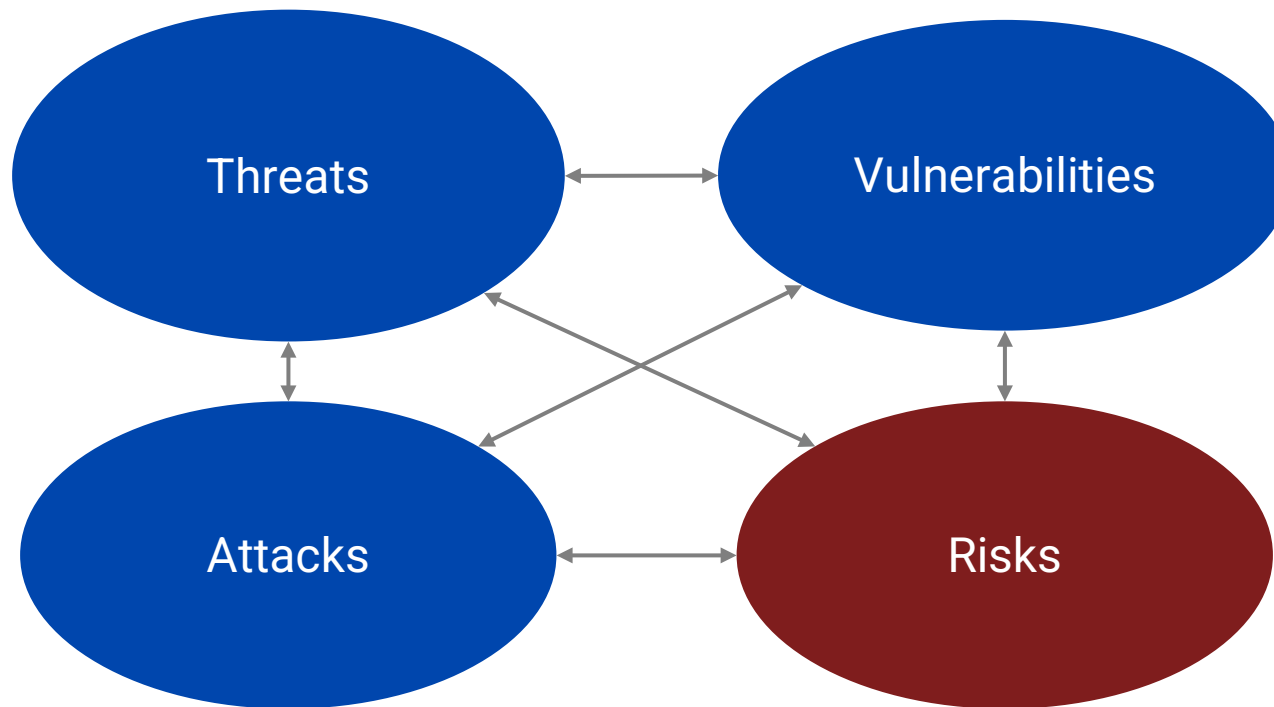**Science & technology**

Sicurezza nazionale

Economia

Scienze sociali

Università Bocconi
MILANO

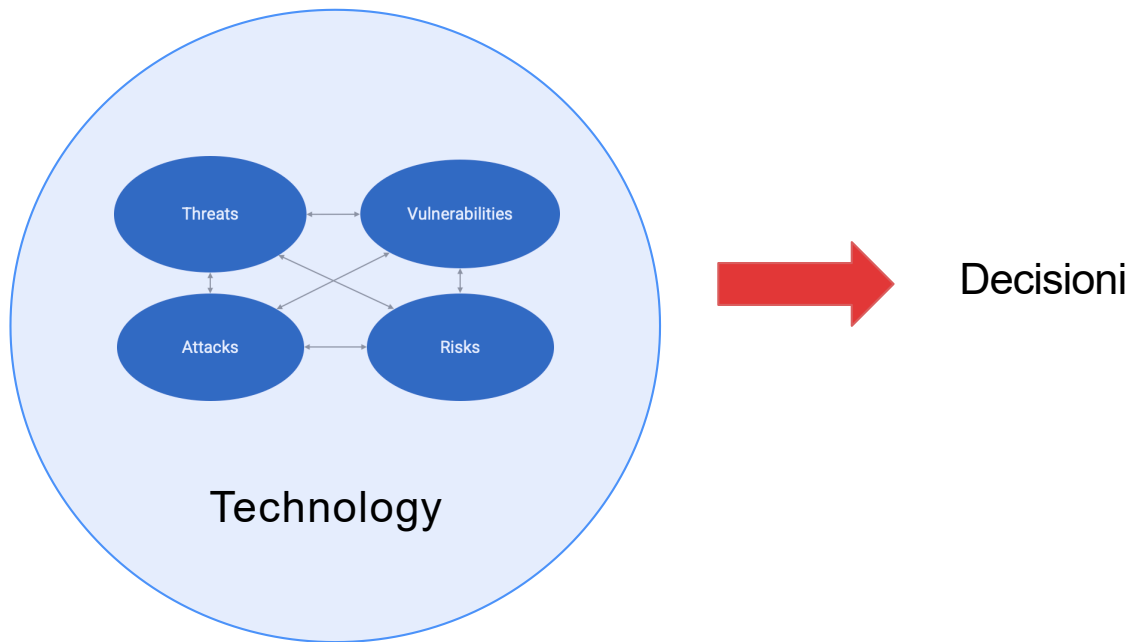# I modelli di cybersecurity: threat-based approach

Reduce the number of:

Threats

Vulnerabilities

Attacks

Risks

Agrafiotis, I., et al. (2018)

Università Bocconi MILANO

I modelli decisionali: risk management approach

Threats ⟷ **Vulnerabilities**

Attacks ⟷ **Risks**

Reduce the risks

Agrafiotis, I., et al. (2018)

I modelli decisionali attuali

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

Che impatto reale ha avuto l'attacco?

The New York Times

## Gas Pipeline Hack Leads to Panic Buying in the Southeast

The national average for a gallon of regular gasoline rose 2 cents on Tuesday, and some airlines began to take small measures in response to the shutdown.

Give this article 9

Rick Rouan
USA TODAY
Published 4:34 p.m. ET May 12, 2021 | Updated 11:05 p.m. ET May 12, 2021

Lines are **wrapping around** gas pumps in the Southeast U.S.

▶ ◀× 0:02 | 0:53
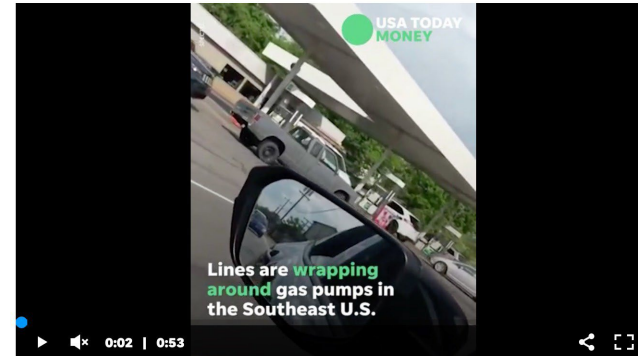
People speed to the gas pump after Colonial Pipeline cyber attack
The disruption of the Colonial Pipeline, which runs over 5,500 miles, is threatening to leave Southeast gas stations with little to no gasoline. *Staff video, USA TODAY*

AIRLINES

Pipeline outage forces American Airlines to add stops to some long-haul flights, Southwest flies in fuel

PUBLISHED MON, MAY 10 2021•9:11 PM EDT | UPDATED TUE, MAY 11 2021•9:25 AM EDT
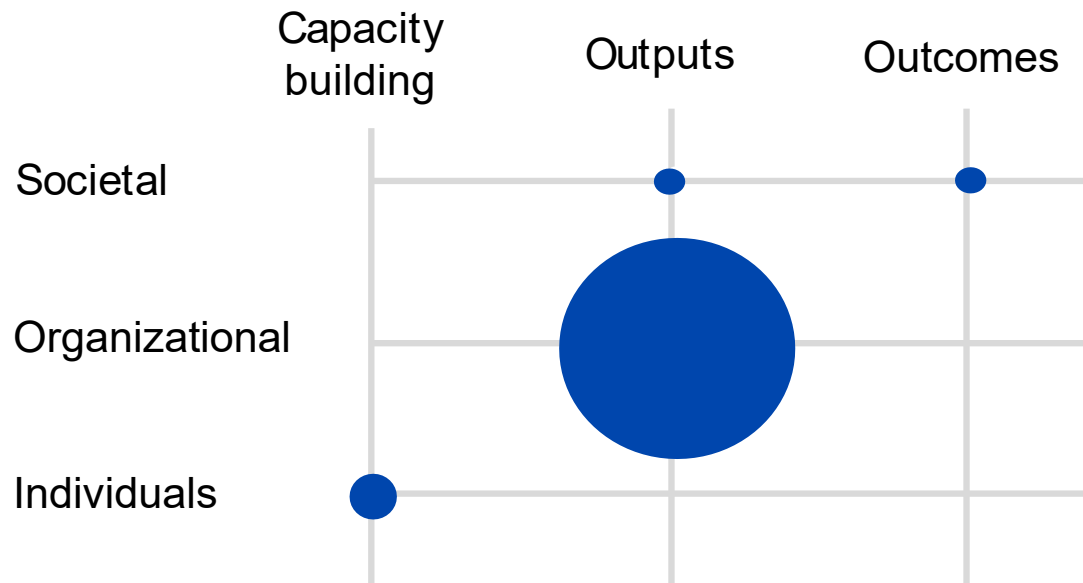
Leslie Josephs
@LESLIEJOSEPHS   SHARE

Università
Bocconi
MILANO

Servizi essenziali e valore a rischio

Starting point over = N. 17378
Subset of the papers reviewed with information about value at risk N=77

Re-framing del problema

Without a holistic understanding of all possible impacts, making good decision-making and policy choices about the possible risks or harms is impossible.

Agrafiotis, I., et al. (2018)

"Disruption of essential services is also expanding as a problem area to a multitude of additional policy domains not traditionally within the narrow purview of security."

CYBER RISK

Cyber risk research impeded by disciplinary barriers

Security progress requires cross-disciplinary collaboration

By **Gregory Falco**[1,2,3], **Martin Eling**[4], **Danielle Jablanski**[5], **Matthias Weber**[6,7], **Virginia Miller**[8], **Lawrence A. Gordon**[9,10], **Shaun Shuxun Wang**[11], **Joan Schmit**[12], **Russell Thomas**[13,14], **Mauro Elvedi**[15], **Thomas Maillart**[16], **Emy Donavan**[17], **Simon Dejung**[18], **Eric Durand**[19], **Franklin Nutter**[20], **Uzi Scheffer**[21], **Gil Arazi**[22], **Gilbert Ohana**[23], **Herbert Lin**[24,25,26,27,28,29]

Cyber risk encompasses a broad spectrum of risks to digital systems, such as data breaches or full-fledged cyber attacks on the electric grid. Efforts to systematically advance the science of cyber risk must draw on not only computer science but also fields such as behavioral science, economics, law, management science, and political science. Yet, many scholars believe that they have sufficient understanding of other fields to comprehensively address the inherently cross-disciplinary nature of cyber risk. For example, a statistician might apply Bayesian modeling to predict future cyber events, even though it is not entirely clear what bearing historical cyber events have on future ones. Computer scientists might write on data protection laws, yet with little knowledge of legal jurisdiction issues. Such questions of disciplinary ownership, the inability to coordinate across disciplines, and the undefined scope of the problem domain have thus plagued inherently cross-disciplinary cyber risk research. Drawing on global expertise and challenges from industry, academia, nonprofit organizations, and governments, we adapted the classical risk-management process to identify core research questions for cyber risk, gaps in knowledge that need to be addressed for advances in security, and opportunities for cross-disciplinary collaboration for each area. Although we mention specific disciplines reflective of our backgrounds, these are not the only ones that should be conducting cyber risk research.

CYBER RISK TRADECRAFT

We consider cyber risks to include "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (*1*). But the scope of cyber risk has nonetheless been difficult to characterize because there

Università Bocconi MILANO

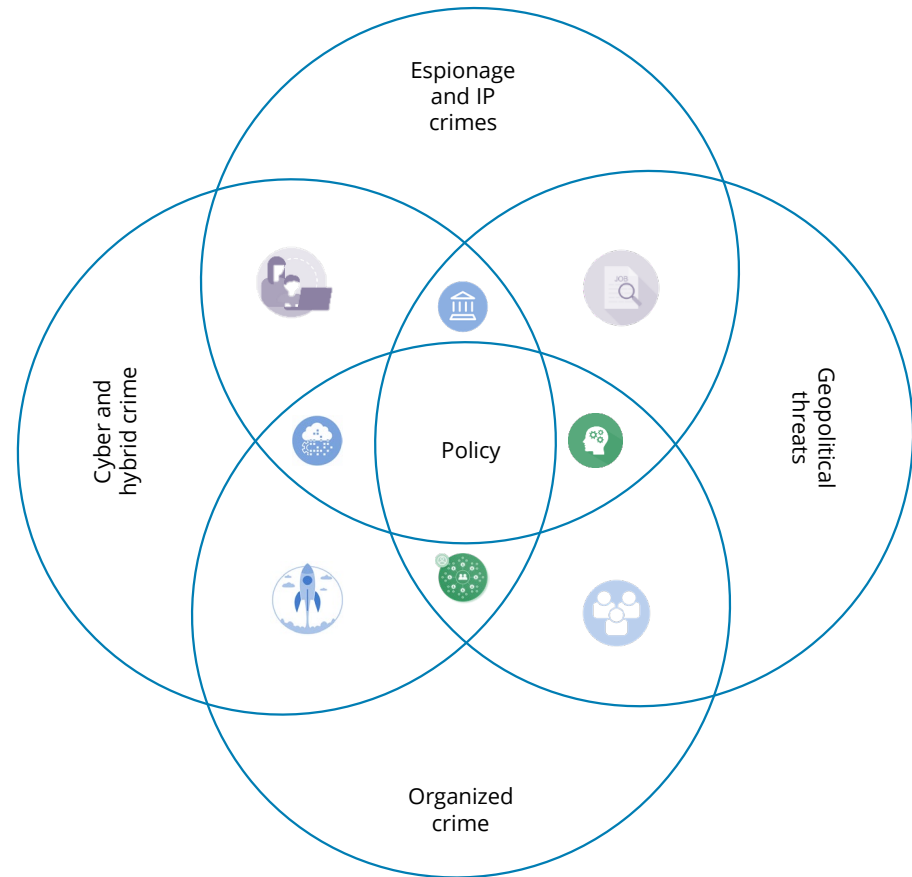# I gap nei modelli decisionali attuali

- I modelli decisionali attuali riguardano la protezione dell'infrastruttura, anziché la sicurezza dei servizi essenziali;

- Il focus di strategie e politiche è a livello organizzativo, e si considerano prevalentemente elementi di previsione e mitigazione del rischio, anziché gli effetti a cascata;

- I modelli attuali, non tengono conto delle interconnessioni tra servizi essenziali né tra gli asset di organizzazioni diverse che contribuiscono all'erogazione del servizio, generando il "siloed problem framing"

- Gli effetti della discontinuità di servizi essenziali riguardano gli output, come la continuità del sistema e la performance organizzativa. Non tengono in considerazione in modo sistematico il valore a rischio che riguarda gli individui e la società

Università
Bocconi
MILANO

Il missing link: il valore a rischio

1	Energetic crisis & self-sufficiency	9	Economic and financial sustainability
2	Glocal supply chains	10	Digital awareness
3	Misinformation	11	Logistics and infrastructures
4	Lifesciences	12	Start-up ecosystem
5	Public health	13	Resource-dependency
6	Climate change	14	Essential services
7	Terrorism	15	Urban platforms
8	Connected government	16	Citizenship

Espionage and IP crimes

Cyber and hybrid crime

Geopolitical threats

Policy

Organized crime

Università Bocconi
MILANO

La nostra serie podcast

GRAZIE

greta.nasi@unibocconi.it