Obiectivo
Thinking outside the box

CyberSecurity
perché è un problema che ci riguarda tutti

Alessio L.R. Pennasilico
apennasilico@obiectivo.it

Alessio L.R. Pennasilico, aka mayhem

Cyber Security Advisor

Objectivo

Membro del Comitato Direttivo e del Comitato Tecnico Scientifico

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità

Presidente dell'Associazione Informatici Professionisti (AIP)

Membro del Comitato di Schema UNI 11506 Informatico Professionista

#iosonopreoccupato

Quali sono gli asset più preziosi?

Provocazione:

Se sono le informazioni, perché non esiste una apposita voce di bilancio?

L’informazione è Patrimonio aziendale!

#iosonopreoccupato

Quanto valgono i nostri dati?

Home | Hacking | Tech | Cyber Attacks | Vulnerabilities | Malware | Spying

The Hacker News™
Security in a serious way

Hackers Are Offering Apple Employees $23,000 for Corporate Login Details

Tuesday, February 09, 2016 Rakesh Krishnan

An unsatisfied Employee may turn into a Nightmare for you and your organization.

http://thehackernews.com/2016/02/hacking-apple-id.html

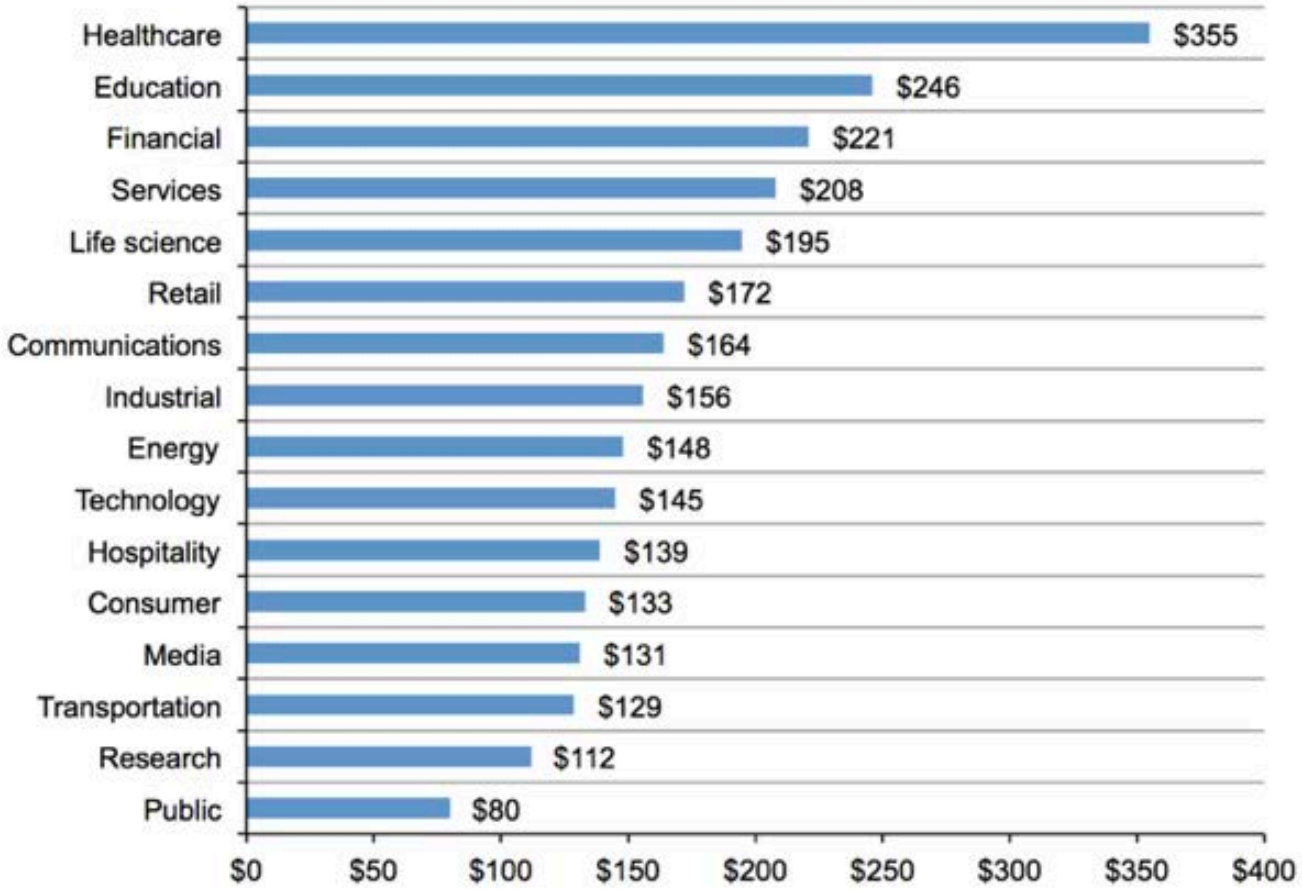
Cosa significa “garantire la sicurezza”?

Quel che succede

“su Internet”

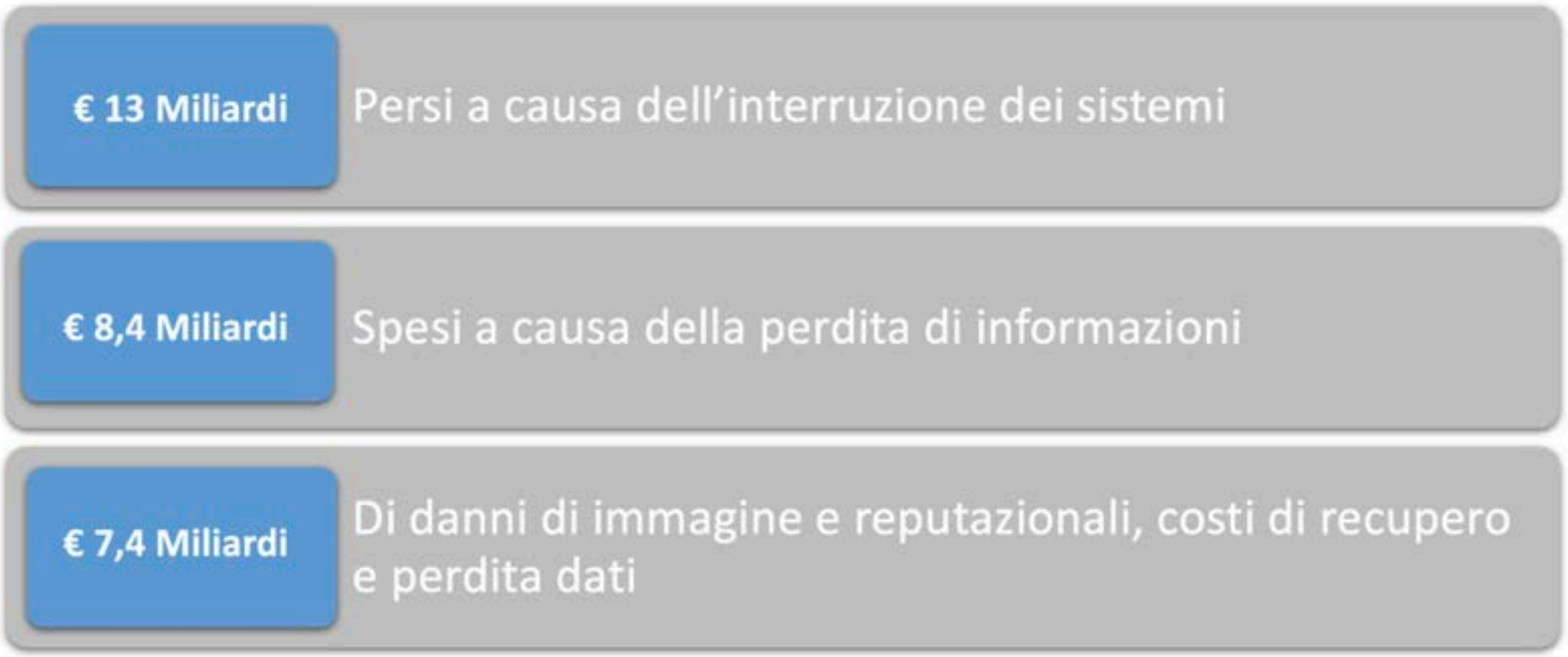
influenza la realtà

Quanto costa “perdere” una informazione?



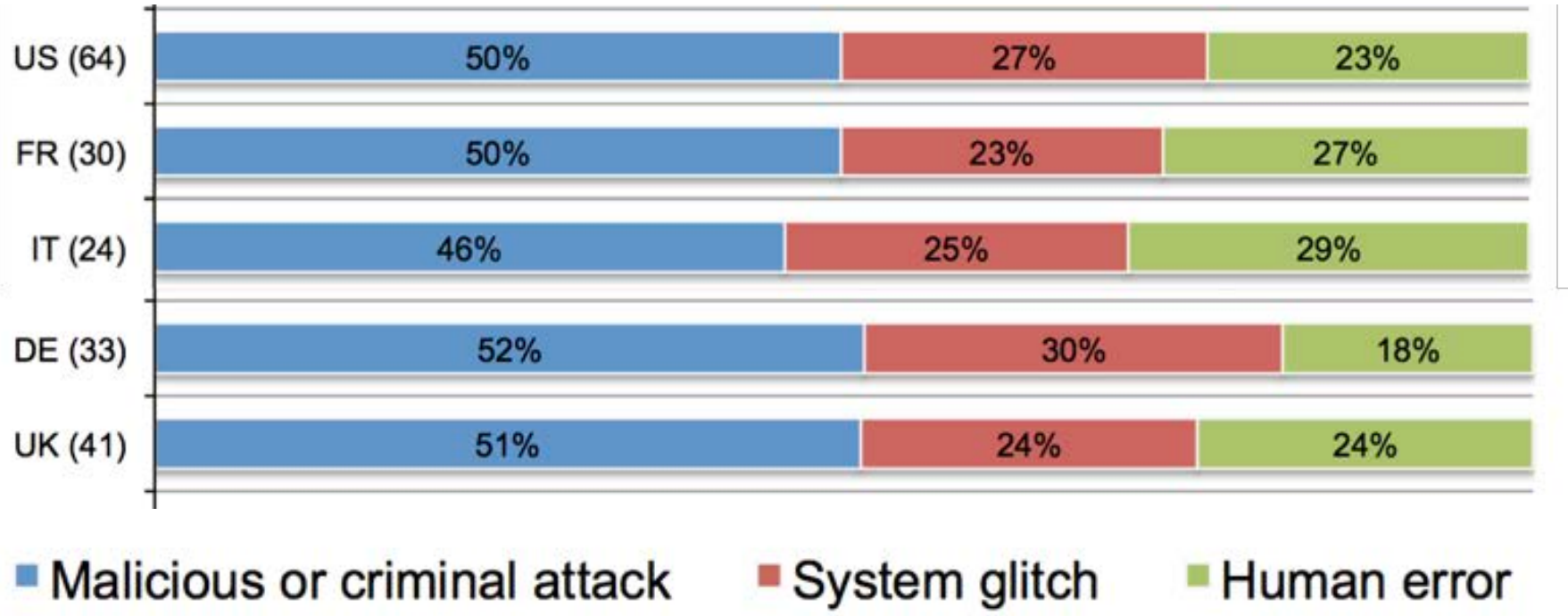
Fonte: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute (Dati 2015)

Quanto ci costano questi incidenti?



Fonte: Criminalità Informatica e Rischi per L'economia e le Imprese a Livello Italiano ed Europeo, UNICRI (Dati Italia 2014)

Quanto incidono le diverse cause?



Fonte: 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute (Dati 2015)

Quale é lo scenario rispetto ai Cyber Attack?

Ogni anno

durante il Security Summit di Marzo a Milano

Clusit presenta un rapporto

su cosa è accaduto nell'anno precedente

e cosa ci si aspetta dall'anno in corso

#iosonopreoccupato

Riassunto del Rapporto Clusit:

Non importa chi sei

Non importa cosa fai

Non importa con cosa lo fai

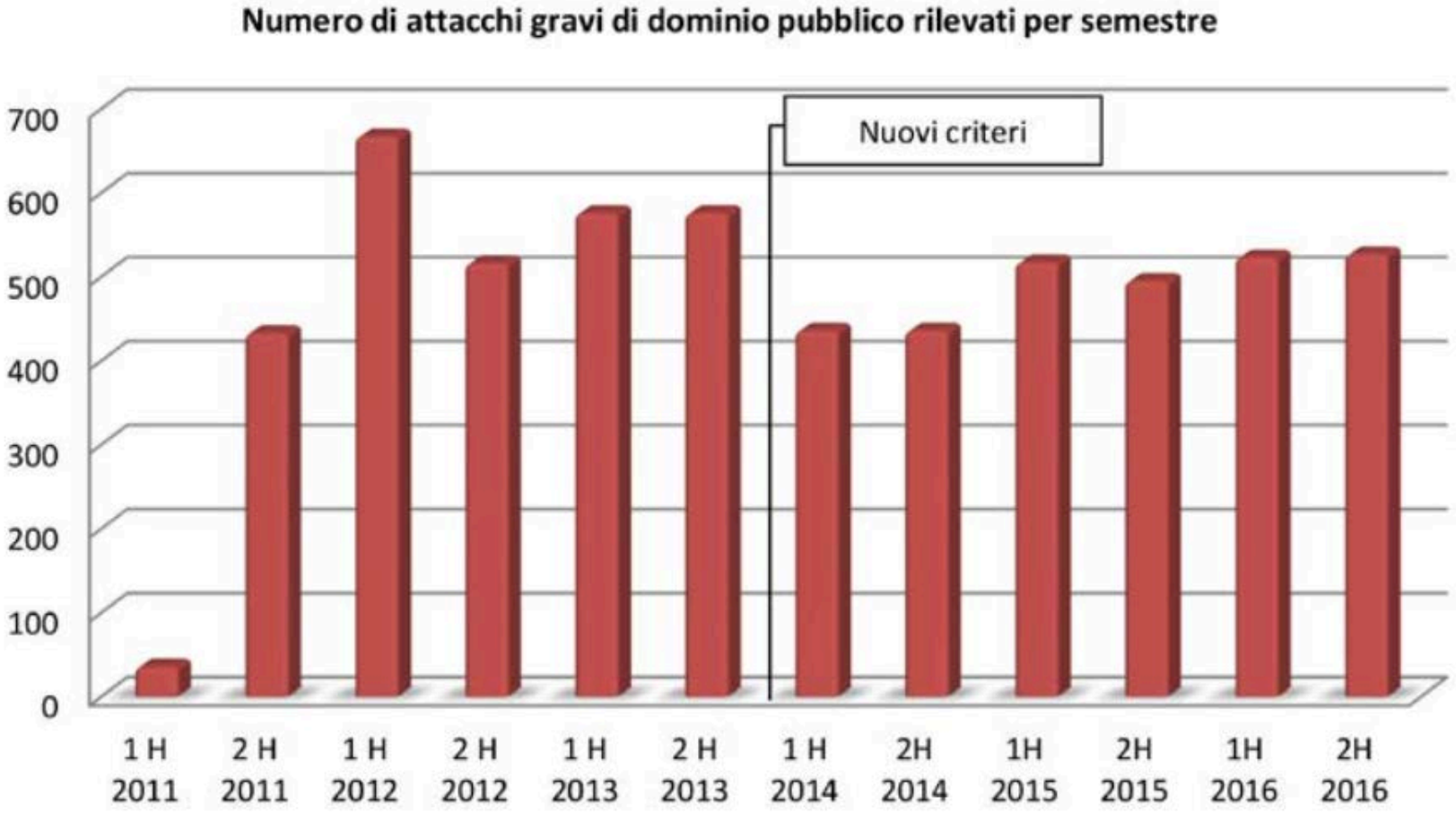
Ti attaccheranno

E se non ti sarai protetto in modo adeguato

subirai dei danni

#iosonopreoccupato

Abbiamo dovuto riclassificare gli incidenti, poiché la gravità aumenta!



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Chi può resistere ad un attacco da 45 Gb/s?

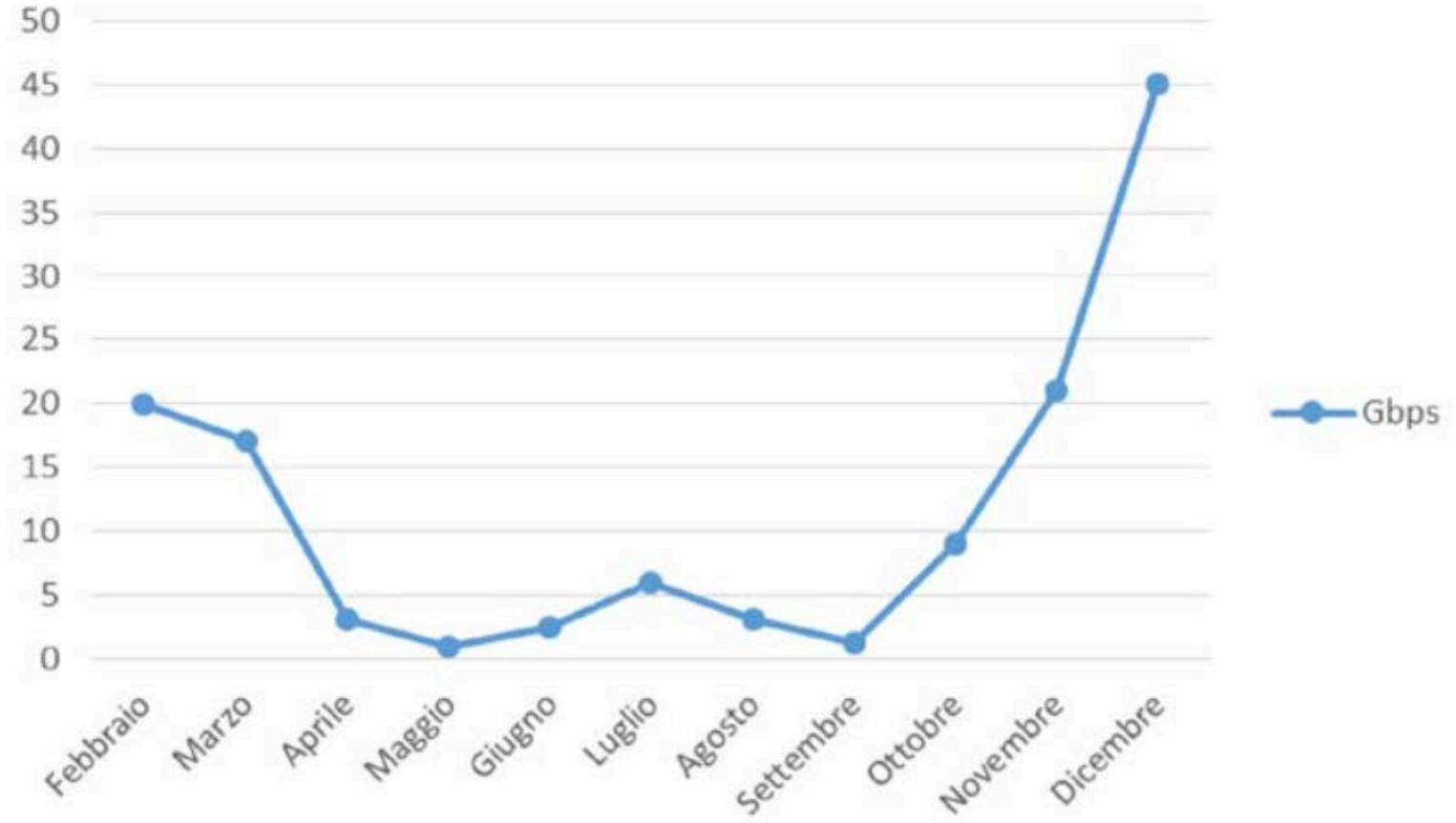
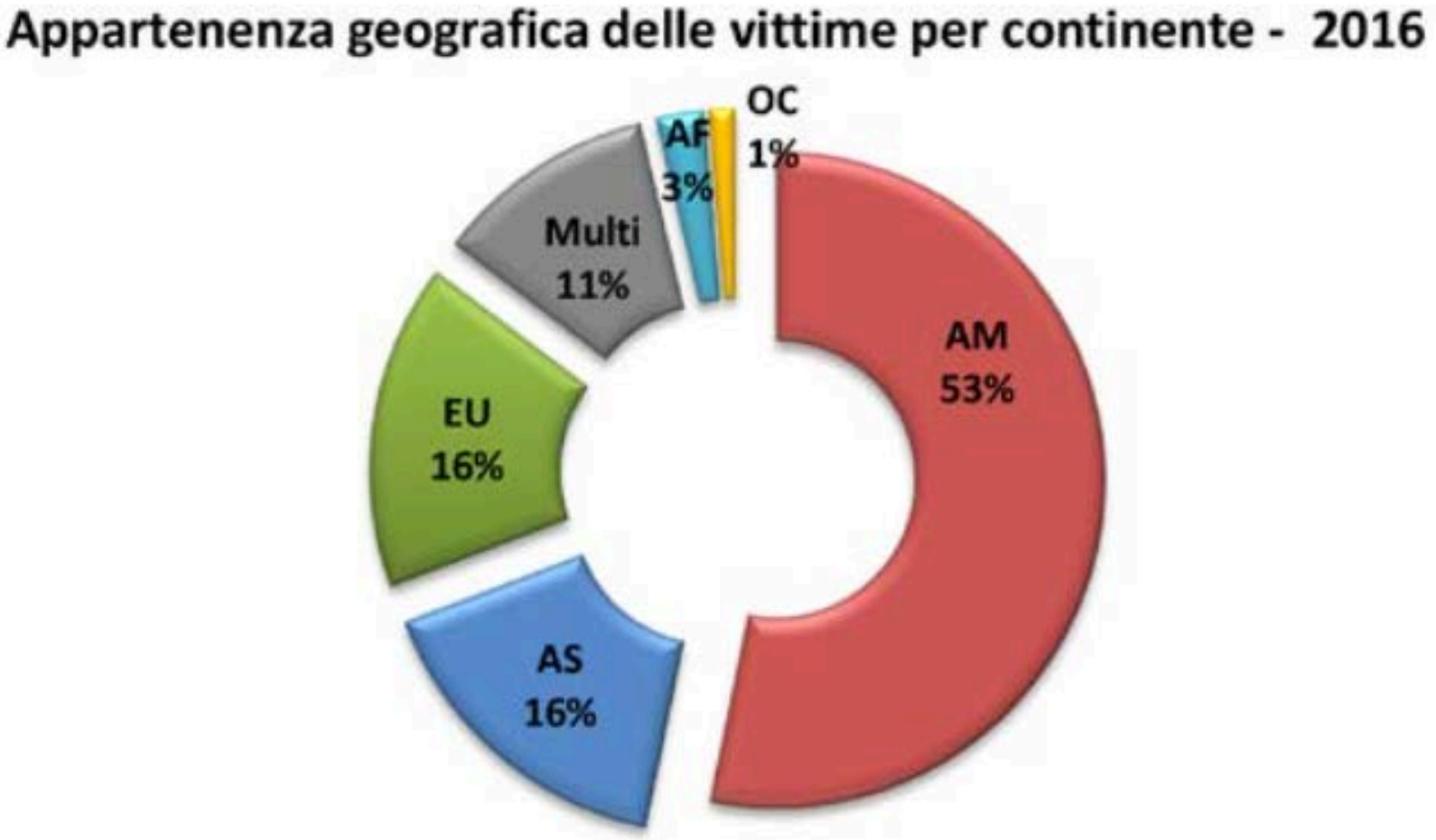


Figura 11 - *Picchi di traffico relativi ad attacchi DDoS mitigati*[2] *(DATI Fastweb, anno 2016)*

Sono davvero gli USA lo stato più colpito?

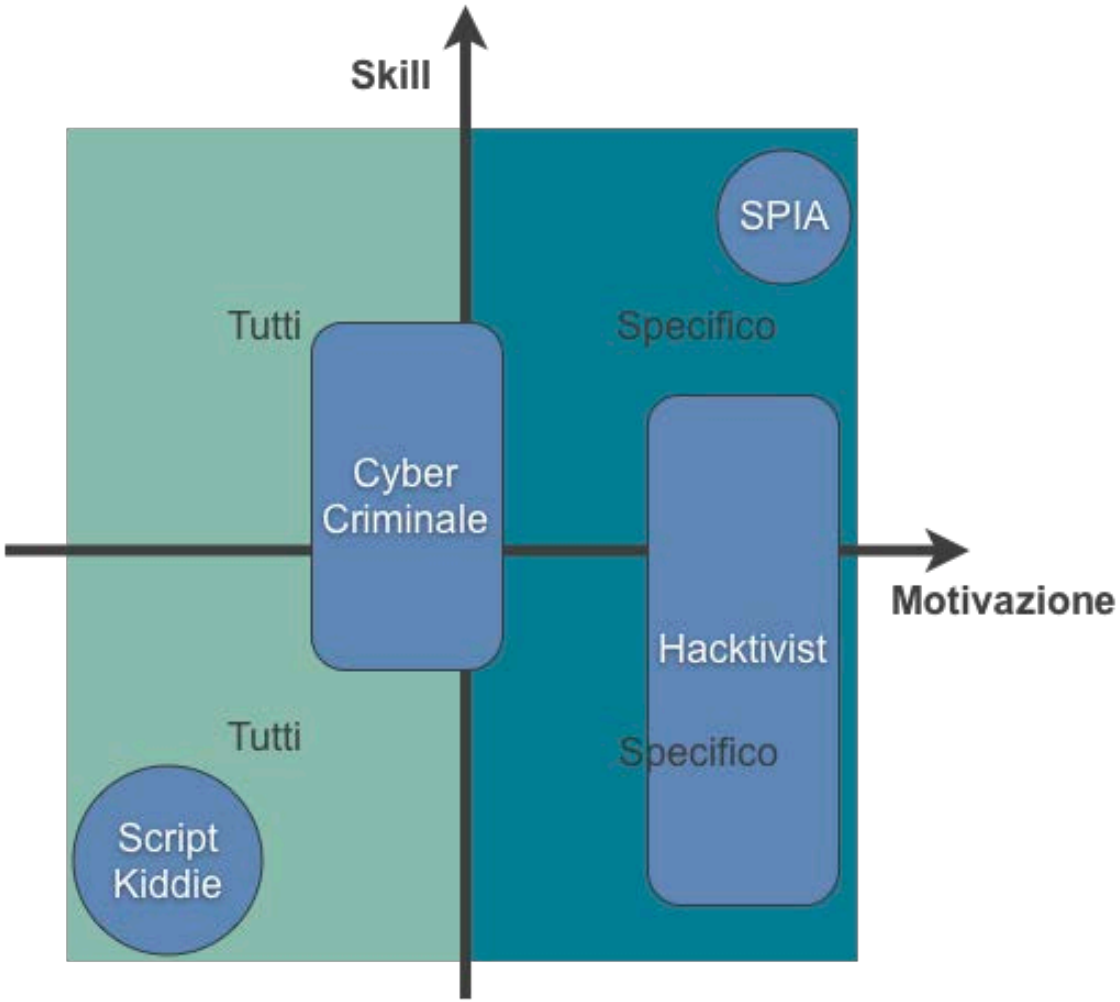


Classificare gli attaccanti: un progetto a cui ho partecipato…

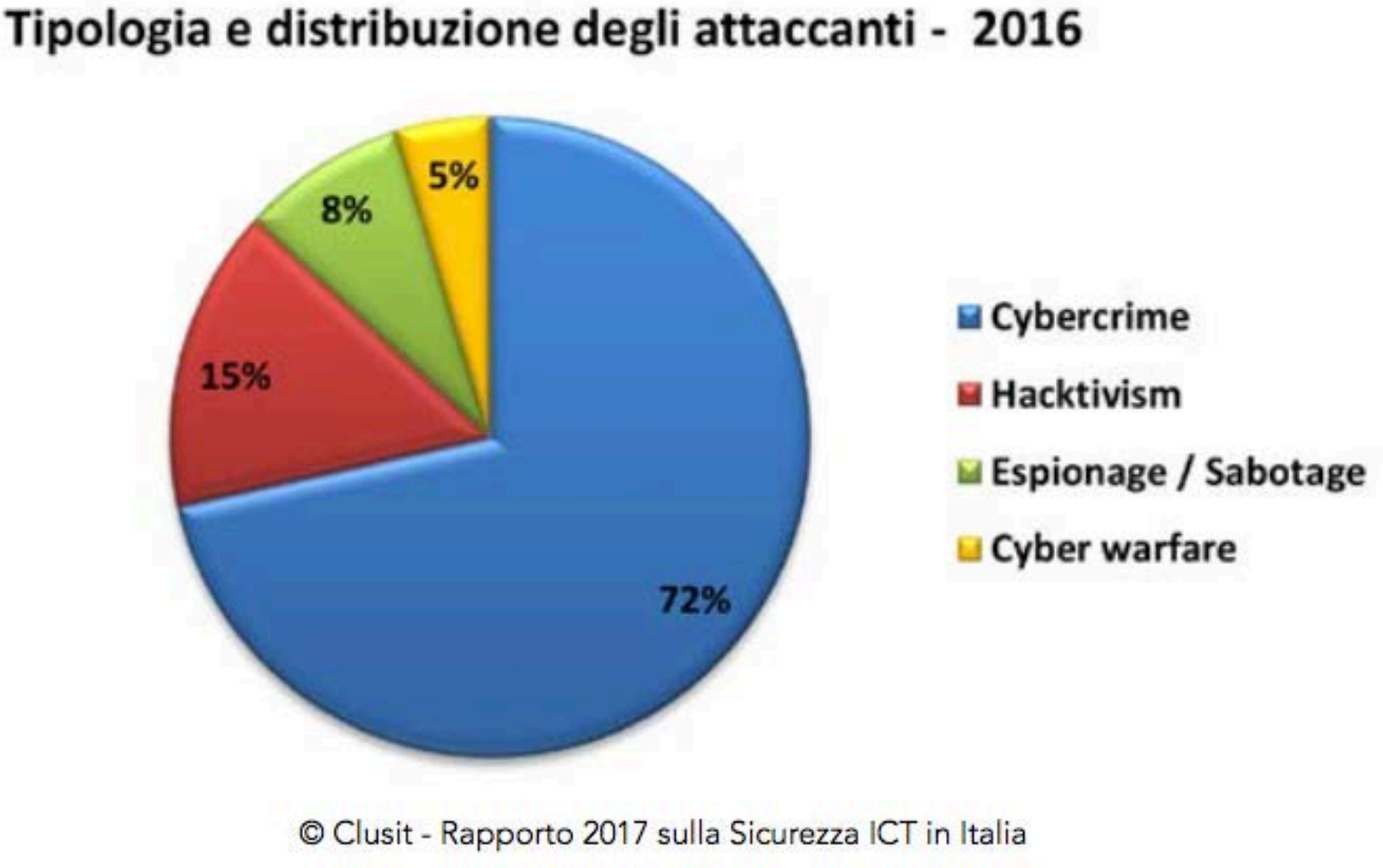
Chi ci attacca e per quale ragione?

Come mi difendo?

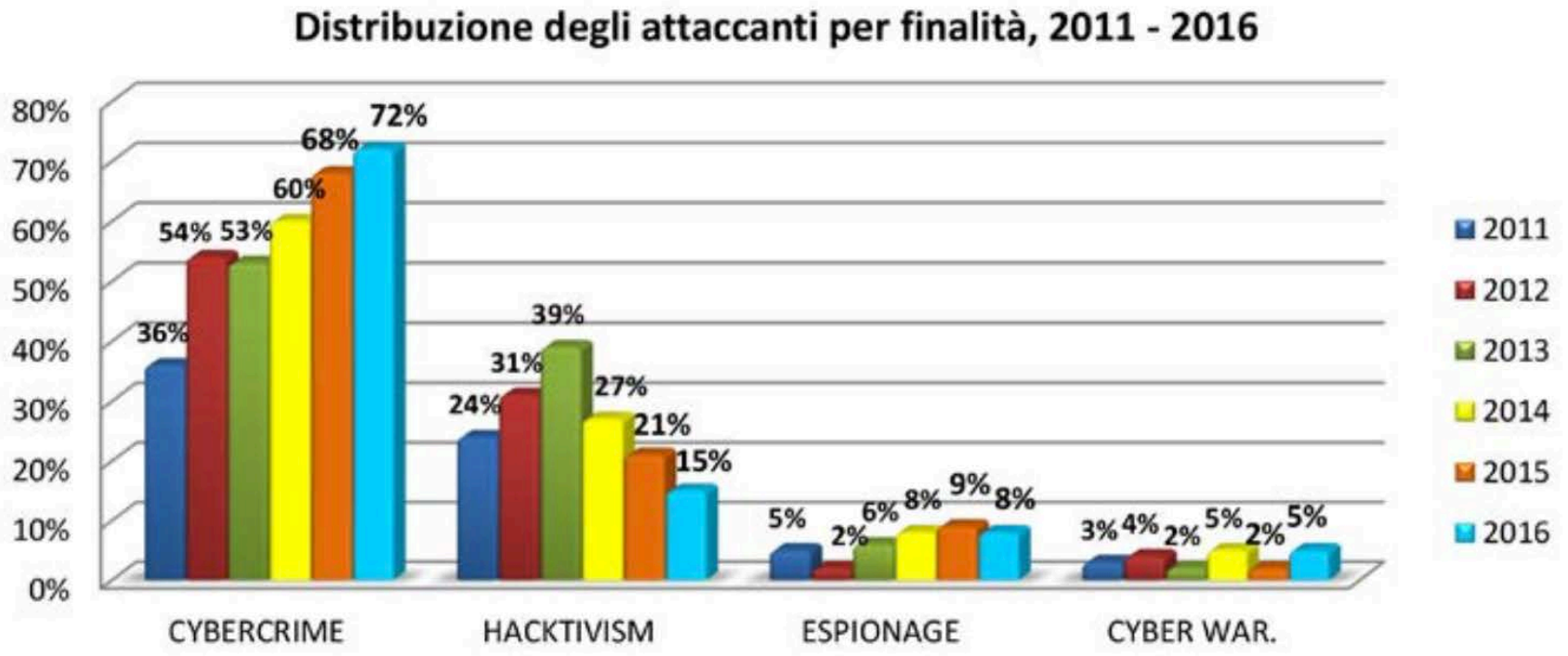
Chi ci attacca e perché?



Di chi ci dovremmo preoccupare?



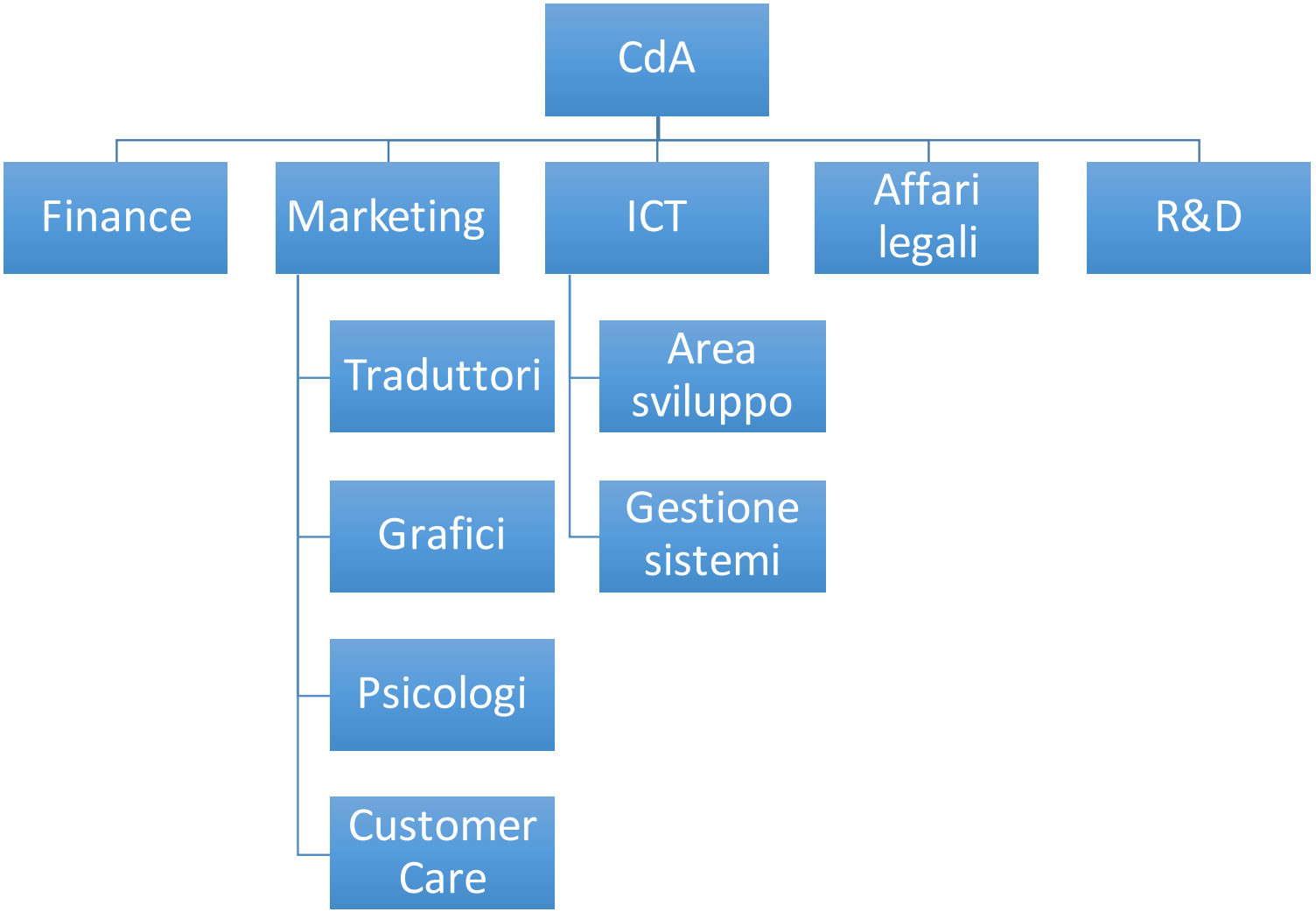
L’utilizzo di Internet potrebbe diventare anti-economico!



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

#iosonopreoccupato

L’organizzazione dei cyber criminali



#iosonopreoccupato

Ci attaccano con tecniche banali!

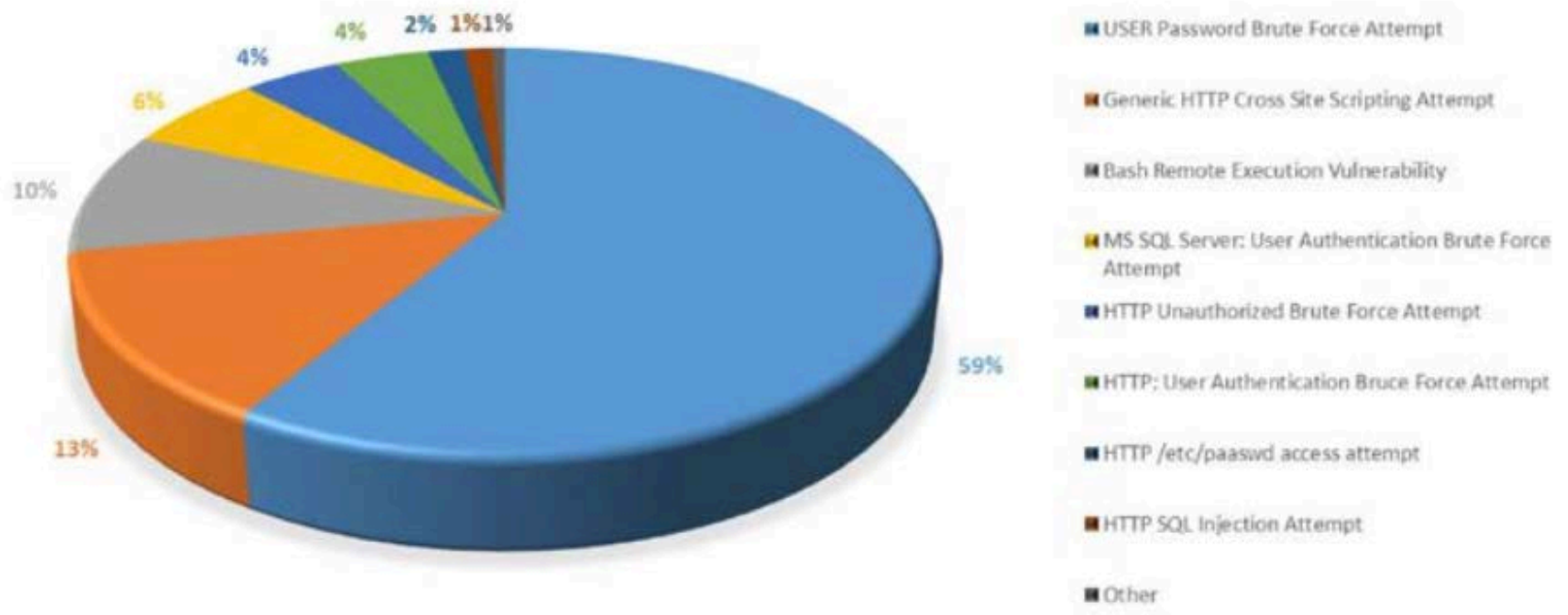
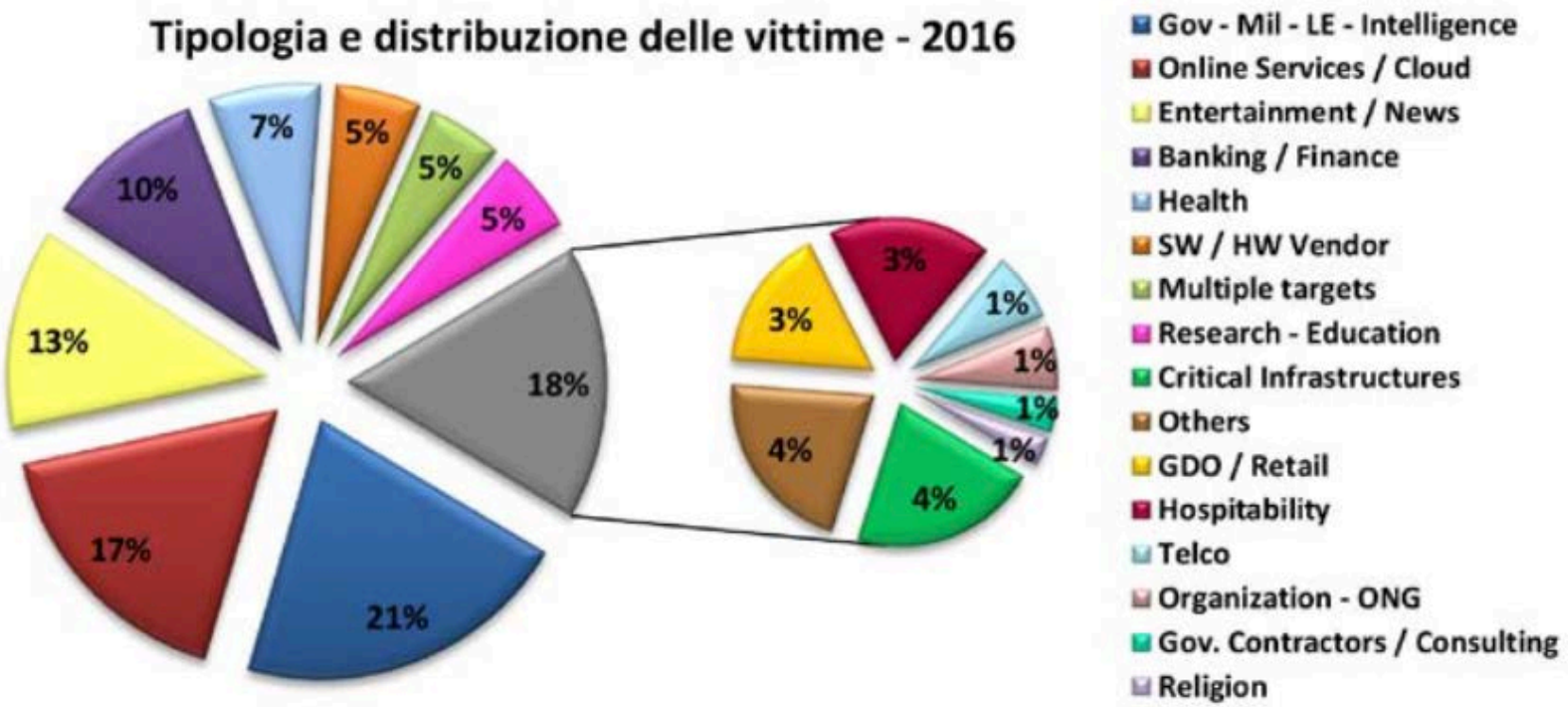


Figura 21 - *Analisi dei principali tentativi di exploit rilevati (DATI Fastweb relativi all'anno 2016)*

E’ un problema che riguarda tutte le organizzazioni!



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

Su ogni tecnologia usata (es. VoIP)

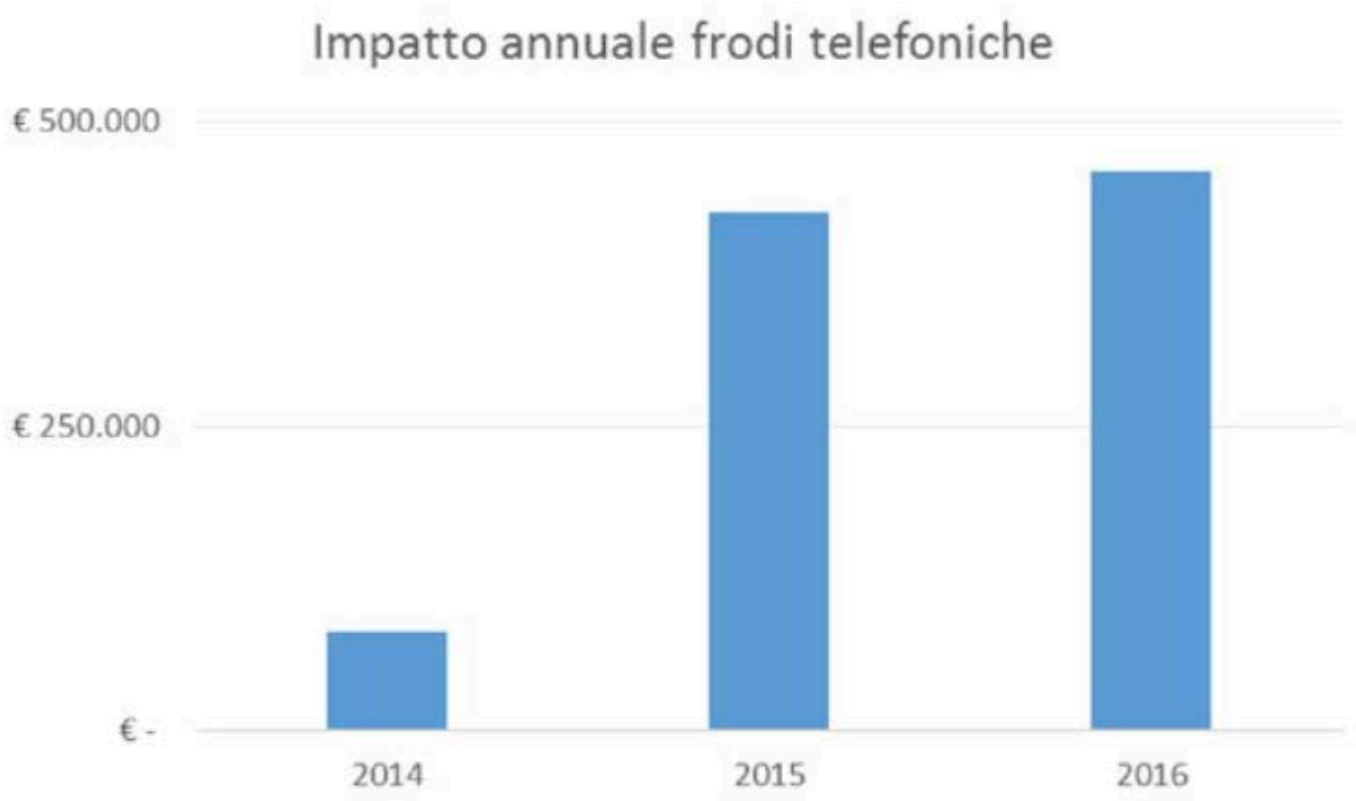


Figura 14 - *Valore delle frodi (DATI Fastweb relativi all'anno 2016)*

Trend

Aumentano i tentativi di intrusione

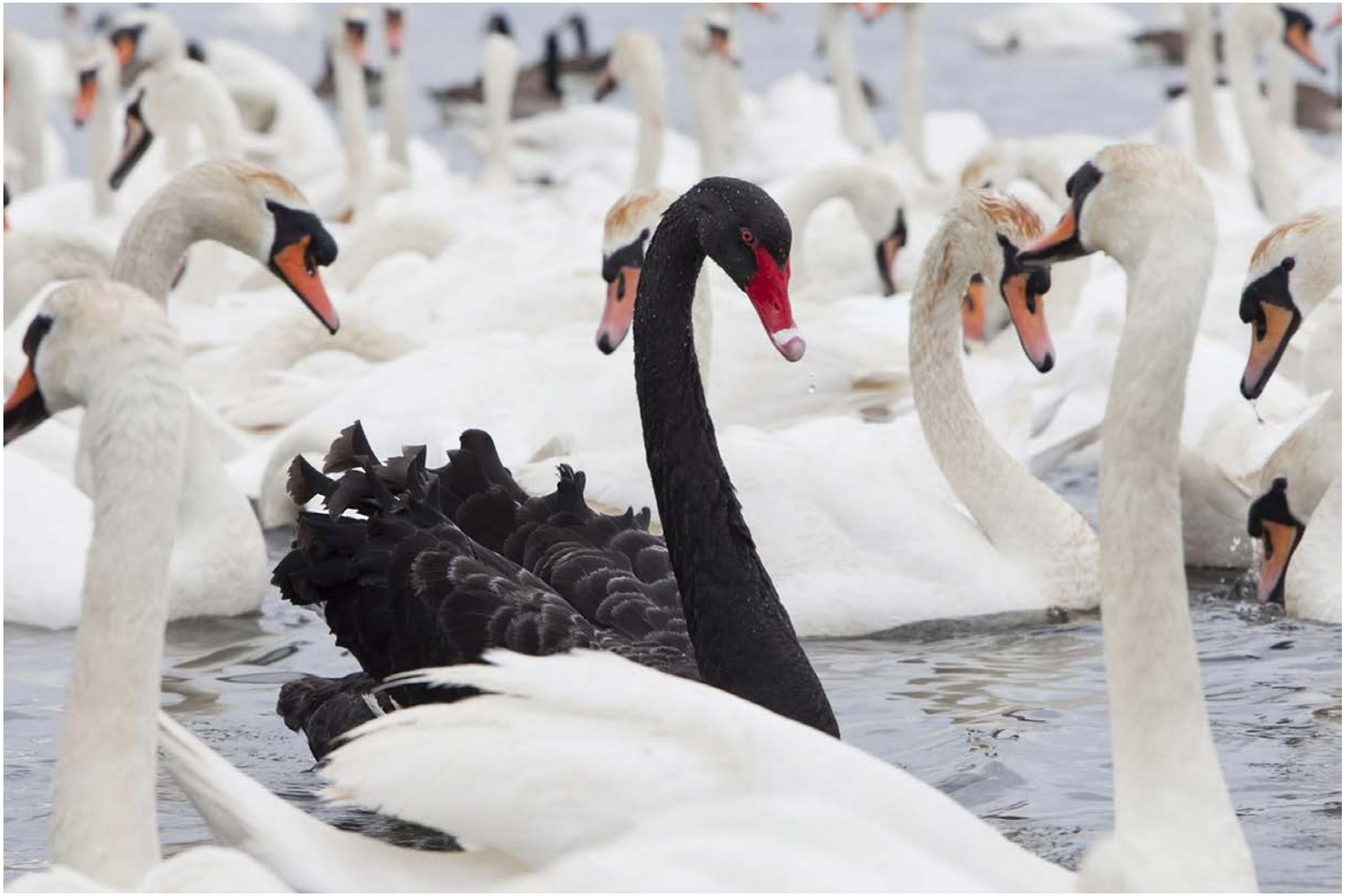
Tra i tentativi aumentano quelli andati a buon fine

Ad ogni intrusione perdiamo sempre più denaro

I CyberCriminali colpiscono dove fa più male: il patrimonio aziendale!

#iosonopreoccupato

... ed il patrimonio intaccato può portare a ...



Quel che succede

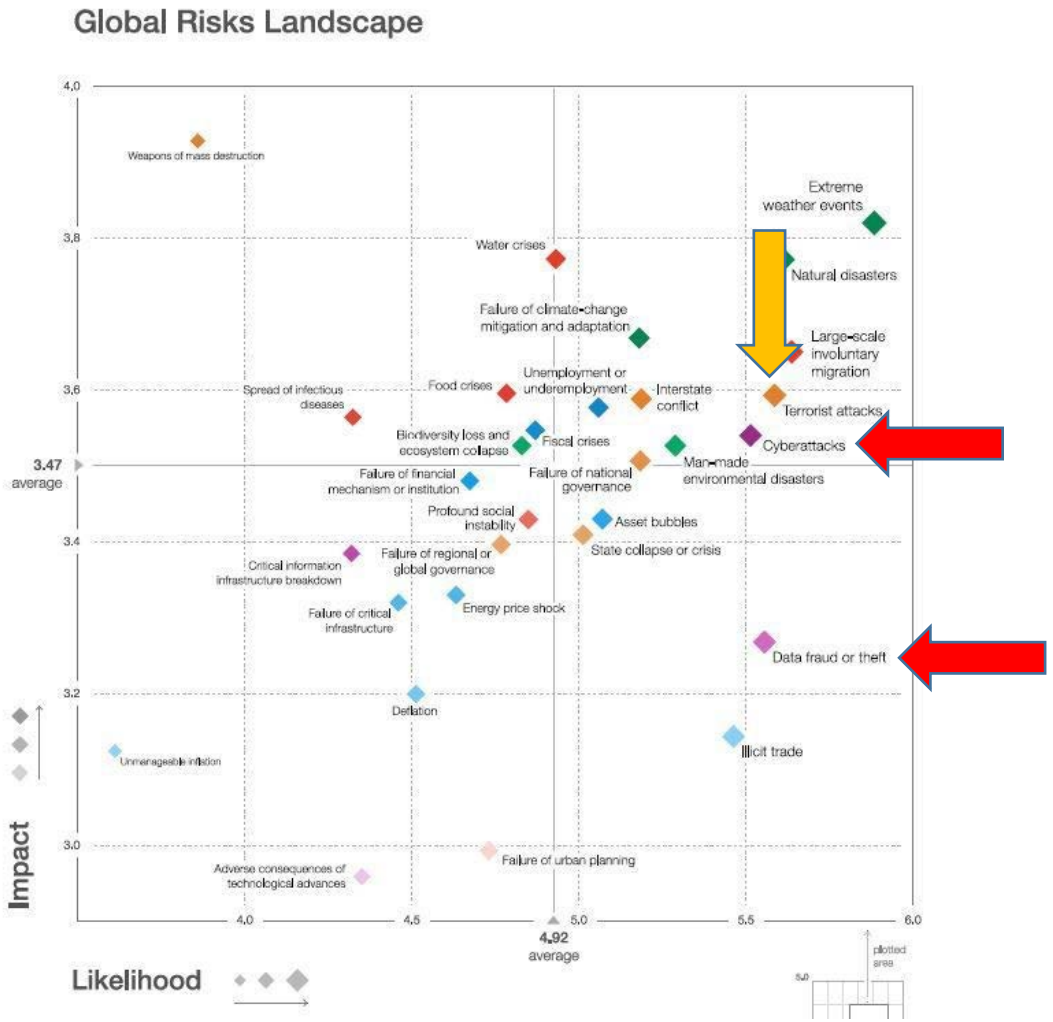
“su Internet”

influenza la realtà

Quanto il problema preoccupa le Aziende

Fonte: Allianz Risk Barometer, 2016

Quanto il problema preoccupa gli esperti



Fonte: World Economic Forum Risk map, 2017

GDPR: non potremo più nascondere la polvere sotto al tappeto!

Il GDPR: obbligo di notifica e sanzioni

stabilisce che il titolare del trattamento (da Maggio 2018)

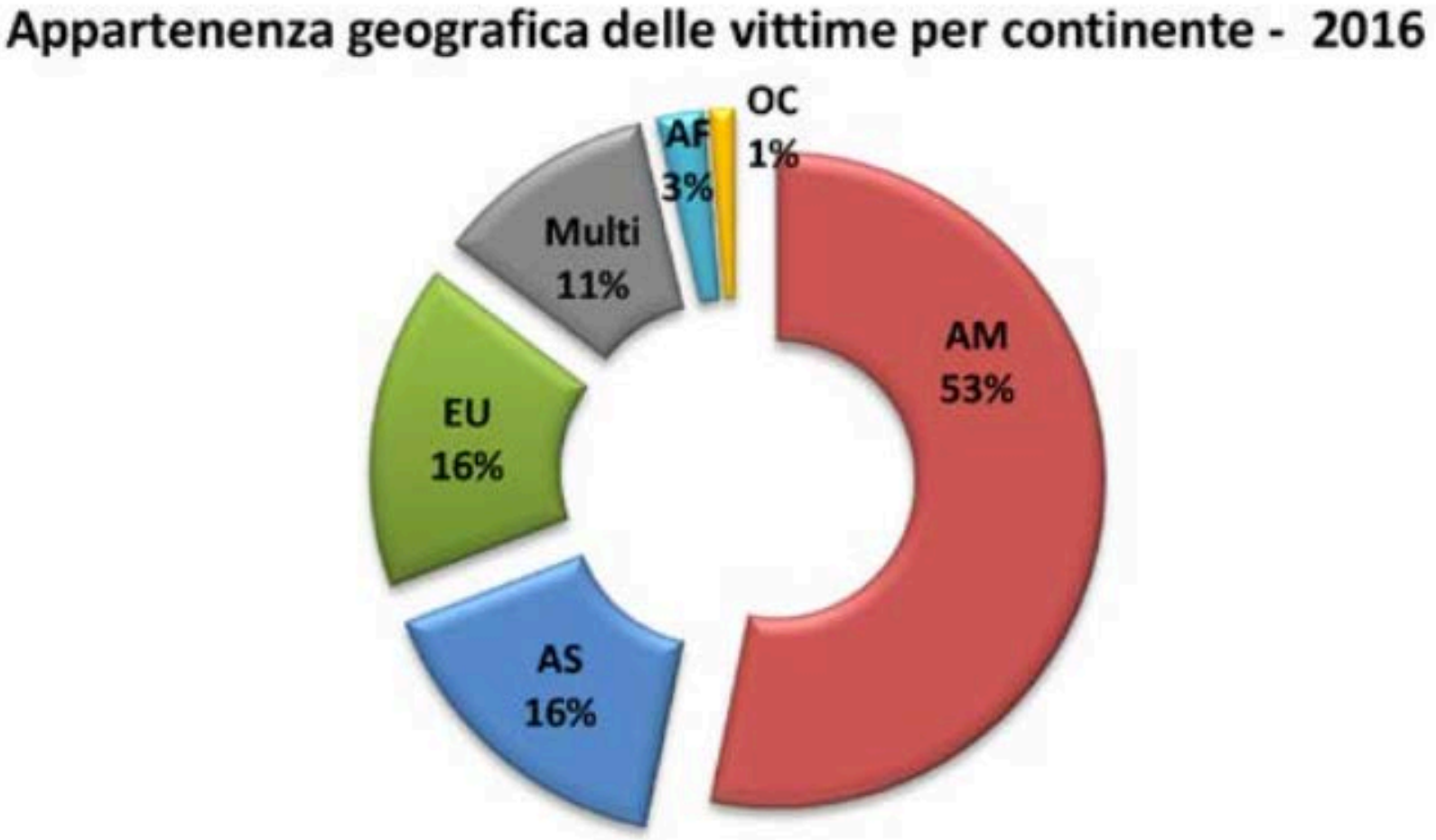
notifichi la violazione dei dati personali

sia (i) all'autorità di controllo competente (art. 33)

sia (ii) all'interessato, a meno che il titolare abbia adottato misure atte a prevenire la violazione stessa (art. 34).

Per le imprese le **sanzioni** amministrative pecuniarie possono arrivare fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente (art. 83)

Sono davvero gli USA lo stato più colpito?



Alcuni esempi…

Ho capito bene?

I criminali attaccano indistintamente **chiunque**

e possono **guadagnare** soldi

anche prendendo il controllo del PC

della massaia mia vicina di casa?

Si, grazie alle Botnet!

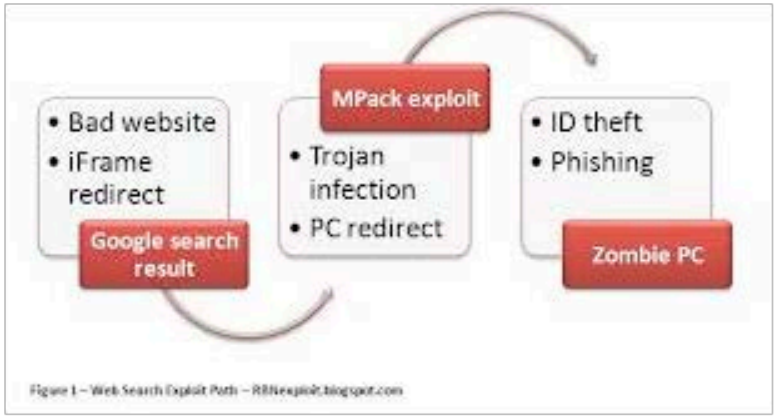
Infetto il maggior numero possibile di host

Li uso per fare spam, phishing, spit, vishing, DDoS

Le affitto a chi vuole gestire da se le stesse attività

Avendo il controllo del dispositivo non mi costa nulla cercare al suo interno dati personali

Un esempio: RBN



#iosonopreoccupato

Sfruttare la “fiducia” ed il cambio di scenario

Incremento dell'uso di Social Engineering

"... the social engineer is able to take advantage of people to obtain information with or without the use of technology."

Kevin Mitnick, The Art of Deception

"Social engineering, the process of deceiving people into giving away access or confidential information, is a formidable threat to most secured networks. While there is plenty of information on social engineering, the threat is considered very real and not easily defended."

David Gragg, A Multi-Level Defense Against Social Engineering

In una nota banca italiana…

from: CEO

to: CFO

Ciao Marco,

per favore fai questo bonifico con urgenza!

> from DG to CEO

> In merito al caso che abbiamo discusso prima, ritengo che la

> soluzione migliore sia accogliere la loro richiesta e bonificare l'importo

> pattuito all'iban indicato nel documento allegato

Aziende “mediamente” fortunate

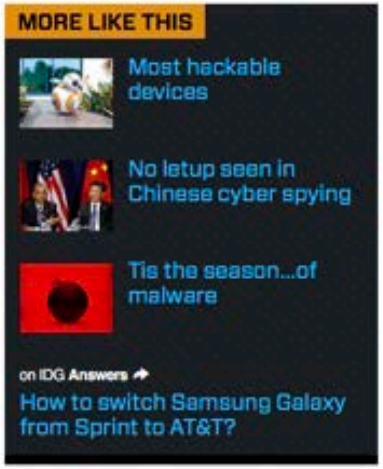
NEWS

Chinese scammers take Mattel to the bank, Phishing them for $3 million

Mattel's Hello Barbie doll is a virtual personality and another step in the future of people talking with their computers. *Credit: Mattel*

Thieves took advantage of a recent company shakeup and corporate policy regarding payments

CSO | Mar 29, 2016 2:14 PM PT



http://www.csoonline.com/article/3049392/security/chinese-scammers-take-mattel-to-the-bank-phishing-them-for-3-million.html

Aziende “sfortunate”

THE WALL STREET JOURNAL.

CFO Journal

Exclusive reporting and analysis for corporate-finance executives.

DATA DASHBOARD | DEALS DASHBOARD | CFO REPORT | COMPLIANC

6:24 pm ET
Aug 7, 2015 CYBERSECURITY

CFO-Less Ubiquiti Tricked Into Wiring Hackers Large Sums

ARTICLE | COMMENTS (2)

CYBERSECURITY FRAUD THEFT UBIQUITI NETWORKS

By MAXWELL MURPHY CONNECT

Ubiquiti Networks in June discovered it was the victim of a roughly $47 million "business email fraud," where cybercriminals tricked employees into wiring money out of its Hong Kong-incorporated subsidiary. The FBI said companies around the globe lost more than $1 billion from October 2013 through June 2015 as a result of such schemes. — Associated Press

http://blogs.wsj.com/cfo/2015/08/07/cfo-less-ubiquiti-tricked-into-wiring-hackers-large-sums/

Truffa ai Clienti

From: Produttore

To: Cliente

Spet.le Cliente,

Abbiamo cambiato banca!

Vi preghiamo di bonificare l'acconto per l'ordine eseguito sul nuovo IBAN XYZ

Esempio di cash-out

“Guadagna da casa, diventa il ns. responsabile commerciale,
comunicaci il tuo IBAN
e dovrai solo incassare le fatture dei ns. clienti Italiani.
Le ragioni sono meramente fiscali.
Una percentuale del pagamento resta a te.”

#iosonopreoccupato

Quel che succede

“su Internet”

influenza la realtà

Malware

Parlare di virus è oramai obsoleto

Le minacce sono molte e diversificate

Lo scopo è nascondersi...

Spyware, Worm, Trojan, Backdoor, Key Logger

Ransomware

Ti cripto tutti i dati
e chiedo il riscatto per darti la chiave
per poterli consultare di nuovo

Social Engineering & Ransomware

A natale 2014:

[spedizioniere] “c’è un pacco in giacenza per te!”

A settembre 2015:

[utility] “hai dimenticato di pagare la bolletta!”

Il ransomware targato “ENEL”

From: Enel Servizio Elettrico
Sent: Thursday, July 02, 2015 3:41 AM
To: [redacted]
Subject: bolletta per la fornitura di energia elettrica

AVANTI

Enel
L'ENERGIA CHE TI ASCOLTA.

Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 85 388 448 [redacted] Codice Fiscale: SXXDOX7070NXI

BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura **610640108** del 30/06/2015 Bimestre maggio - giugno 2015
Totale da pagare entro il 05/07/2015: euro 553,87

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 67923577579
Clicca qui per scaricare

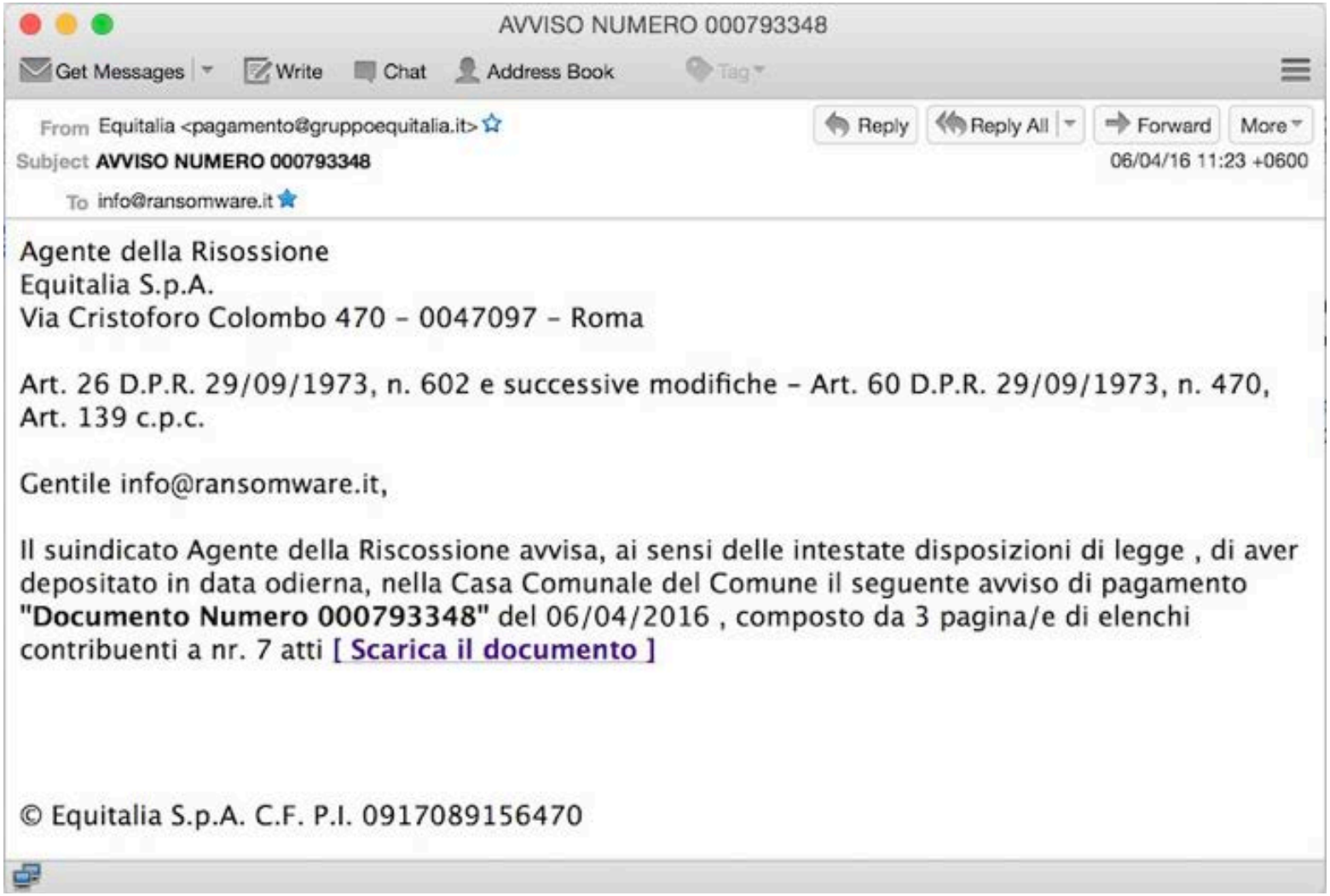
DATI FORNITURARIEPILOGO IMPORTI FATTURATI

Politica sulla privacy

Enel tratta tutti i dati personali dei propri clienti fruitori dei servizi offerti nel portale nel pieno rispetto di quanto previsto dalla normativa nazionale italiana in materia di privacy e, in particolare del D. Lgs. 196/03. Ove l'accesso a particolari servizi venga subordinato alla registrazione previa comunicazione di dati personali, secondo quanto comunicato con l'informativa data al momento della sottoscrizione del servizio. L'acquisizione dei dati che potranno essere richiesti `e il presupposto indispensabile per la stipulazione e la gestione del contratto di erogazione dei Servizi indicati nelle condizioni generali di contratto e per tutte le conseguenti operazioni di interesse del cliente;

clicca qui per cancellare l'iscrizione (unsubscribe)

Il ransomware targato Equitalia



17 Novembre 2013

The UK's National Crime Agency has given out an urgent national alert that a mass spamming event targeting 10 million UK based email users with a piece of malware called **CryptoLocker** that encrypts your files and then demands a ransom money to restore access.

http://thehackernews.com/2013/11/Cryptolocker-Ransomware-spam-emails-campaign-ten-million-users.html

22 Novembre

The CryptoLocker Malware continues to spread, infected more than 12,000 U.S computers in one week and threatening millions of computers in the UK.

Just last week, The UK National Crime Agency urge people afflicted by CryptoLocker not to pay ransom, not least because there is no guarantee that they will even receive an unlock key.

http://thehackernews.com/2013/11/us-police-department-pays-750-ransom-to.html

12.000 device infetti x $ 750 = $ 9.000.000

5% di 10.000.000 x $ 750 = $ 375.000.000

Domande…

E’ una tecnica nuova?

Quanto costa organizzare una campagna di ransomware?

Chi sceglie l’importo del riscatto e rispetto e rispetto a quale principio?

E’ economicamente conveniente pagare il riscatto?

Se pago mi daranno davvero la password?

Chi sceglie ed in base a cosa la modalità di pagamento del riscatto?

Quale può essere il massimo impatto di un attacco ransomware?

#wannacry

Per tutti i sistemi operativi

1 INFORMATICA

Mac a rischio riscatto: Transmission integra il primo ransomware per OS X

CONDIVIDI SU FACEBOOK

60 TOTAL SHARE

Cosimo Alfredo Pina • 7 marzo 2016

I **ransomware** arrivano sui **Mac**. **KeRanger** è il primo malware capace di **sequestrare i file su OS X**, criptandoli e richiedendo un riscatto per poter tornare ad utilizzarli. A portare questo tipo di software malevolo sui computer **Apple** è **Transmission 2.90**.

Ad annunciarlo è *Palo Alto Network* che ha scoperto come alcune copie di **Transmission 2.90**, popolare client per la rete BitTorrent, integrano **KeRanger**, un **malware** capace di rende inaccessibili i file, permettendo la **decriptazione** solo dopo aver pagato.

http://www.smartworld.it/informatica/verificare-keranger-ransomware-mac-os-x.html

Vuoi accedere di nuovo ai tuoi dati?

#1bitcoin

Cryptolocker Mobile?

The Andr/Koler-A ransomware falsely claimed to have encrypted your files

https://nakedsecurity.sophos.com/2014/06/06/cryptolocker-wannabe-simplelocker-android/

Vuoi accedere di nuovo a rubrica, sms, foto?

#1bitcoin

Un problema di percezione

SmartPhone o IdiotPC?

Più potente del mio “vecchio” PC

Più banda di Seabone 20 anni fa

#iosonopreoccupato

SmartTV = StupidPC

Proofpoint Uncovers Internet of Things (IoT) Cyberattack

More than 750,000 Phishing and SPAM emails Launched from "Thingbots" Including Televisions, Fridge

SUNNYVALE, Calif. – January 16, 2014. Proofpoint, Inc., (NASDAQ: PFPT), a leading security-as-a-service provider, has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used to launch attacks. As the number of such connected devices is expected to grow to times the number of connected computers in the next few years according to an IoT-based attack has significant security implications for device owners ar

http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

Vuoi guardare la partita ora?

#1bitcoin

Una “curiosa” TV

BBC News Sport Weather Earth Future Shop TV Radio More... Search

NEWS TECHNOLOGY

Home UK Africa Asia Australia Europe Latin America Mid-East US & Canada Business Health Sci/Environment Tech Entertainment Video

9 February 2015 Last updated at 11:20 GMT

Share

Not in front of the telly: Warning over 'listening' TV

Samsung said personal information could be scooped up by the Smart TV

Samsung is warning customers about discussing personal information in front of their smart television set.

Related Stories

Top Stories

US warns Russia on Ukraine violence

Greece 'to request loan extension'

Lunar New Year celebrations begin

Everest climbing route to be changed

Syria 'agrees to halt' Aleppo raids

Features & Analysis

Creating Cold

The men who made the world a cooler place to live

What the A-listers see

Take a trip down the Oscars' red carpet

Stop wasting time

Top bosses share their secrets on how to get things done

http://www.bbc.com/news/technology-31296188

Elettrodomestici 2.0

TM5

BIMBY

VS

TM31

Vuoi cucinare ora?

#1bitcoin

Serrature “intelligenti”

http://ces.schlage.com/

Vuoi entrare in casa ora?

#1bitcoin

CyberCriminali e nuove tecniche…

SECTIONS HOME SEARCH

The New York Times

SUBSCRIBE NOW LOG IN

245 Migrants Feared Dead in Mediterranean Shipwrecks

The Bloomsbury Bohemians in the British Countryside

Right and Left React to France's Election

Heinz Kessler, Who Led East Germany's Military, Dies at 97

EUROPE

Hackers Use New Tactic at Austrian Hotel: Locking the Doors

By DAN BILEFSKY JAN. 30, 2017

The ransom demand arrived one recent morning by email, after about a dozen guests were locked out of their rooms at the lakeside Alpine hotel in Austria.

The electronic key system at the picturesque Romantik Seehotel Jaegerwirt had been infiltrated, and the hotel was locked out of its own computer system, leaving guests stranded in the lobby, causing confusion and panic.

https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0

Automobili connesse

TRANSPORT IT

Ford Lincoln announces remote-control car app as BMW issues security patch

Monday 02 February 2015
10:15

Share 39 8+1 12 Tweet 63

Ford Motor Company's Lincoln luxury brand is to announce an app to enable users to control their cars remotely as BMW issues a security patch for a flaw affecting 2.2 million vehicles.

The MyLincoln smartphone app – developed with Google – will allow users to schedule remote starts as well as lock and unlock their cars, reports *The Detroit News*.

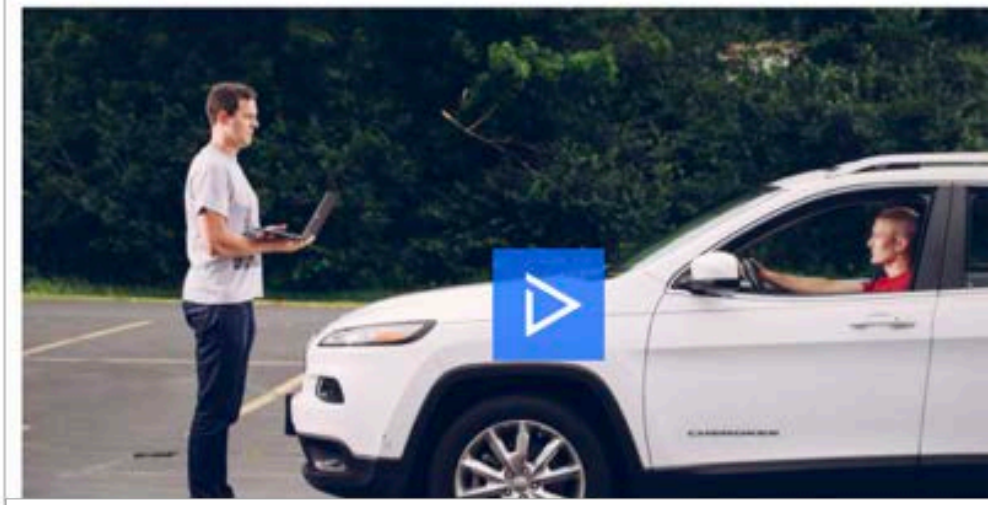
MyLincoln is the first app of its kind to be integrated with the Android organiser app Google Now, and is likely to raise concerns with privacy watchdogs and cyber security professionals.

But users may disregard the risks to benefit from remote start functionality that will ensure the vehicle is cooled off or warmed up by the time they are ready to drive.

"Delivering unique experiences for the luxury client throughout ownership is fundamental to Lincoln," Matt VanDyke, director, global Lincoln, said in a statement.

https://www.computerweekly.com/news/2240239247/Ford-Lincoln-announces-remote-control-car-app-as-BMW-issues-security-patch

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Vuoi andare in ufficio oggi?

#1bitcoin

#iosonopreoccupato

Pacemacker / Pompe di insulina “intelligenti”

http://www.theregister.co.uk/2012/10/17/pacemakers_open_to_wireless_attack/

Vuoi che il tuo cuore
non si fermi ora?

#1bitcoin

Capacità negoziale di rifiutare il pagamento?

http://www.usatoday.com/story/news/2016/02/17/l-hospital-ceo-says-he-paid-17k-ransom-hackers/80530752/

“Smart” Industry?

Quel che succede

"su Internet"

influenza la realtà

#iosonopreoccupato

FBI vs MegaVideo

LA STAMPA.it TECNOLOGIA a cura di Anna Masera

NEWS

19/1/2012 - IL CASO

Oscurato Megaupload, il gigante della condivisione di file in Rete

Sigilli al sito. "Viola il copyright, danni per 500 milioni alle compagnie" Arrestato il fondatore Kim Schmitz. Su Twitter è partita la rivolta degli utenti. Sul fronte pro-copyright in Italia l'intervento del presidente Anica

G. BOT.

Megaupload, il popolare sito per la condivisione in rete, è stato oscurato dall'Fbi. I fondatori del servizio di sharing, uno dei più conosciuti e

http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=9998

Kim *Kimble* ~~Schmitz~~ Dotcom

Mega*: solo film ed MP3?

Dove sono conservati da chi i nostri dati?

Chi li può visionare?

Saranno sempre nella mia disponibilità?

Quel che succede

“su Internet”

influenza la realtà

#iosonopreoccupato

Cyber Risk

è un problema economico, sociale, politico, personale

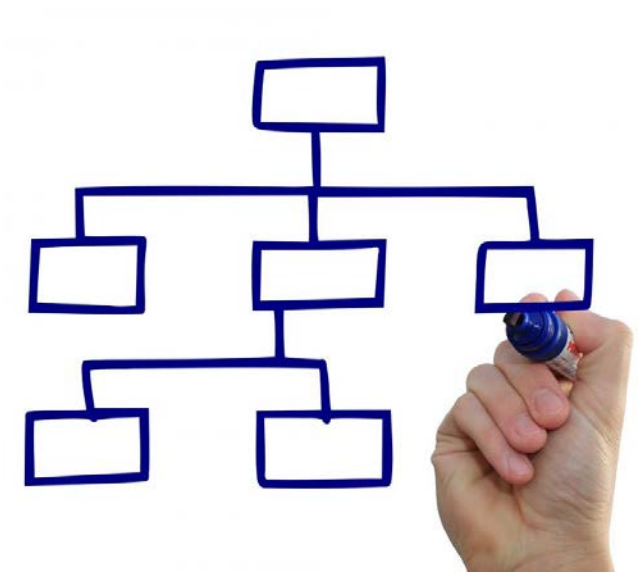
colpisce al cuore della società civile e non risparmia niente e nessuno

in primis nelle nostre aziende

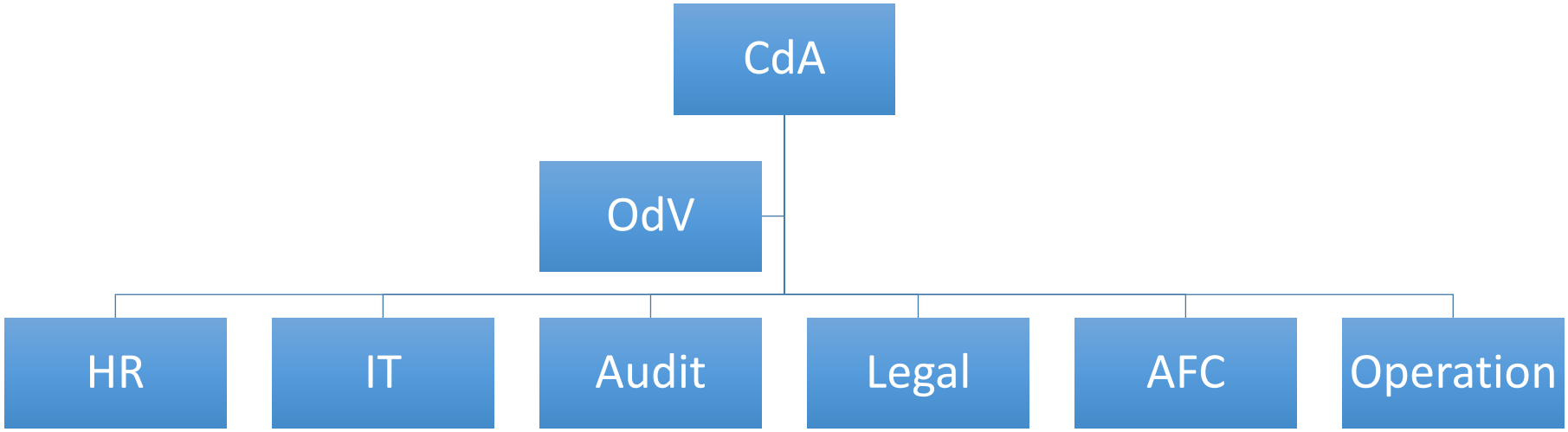
centro nevralgico della sussistenza della nostra società

Cosa fare?

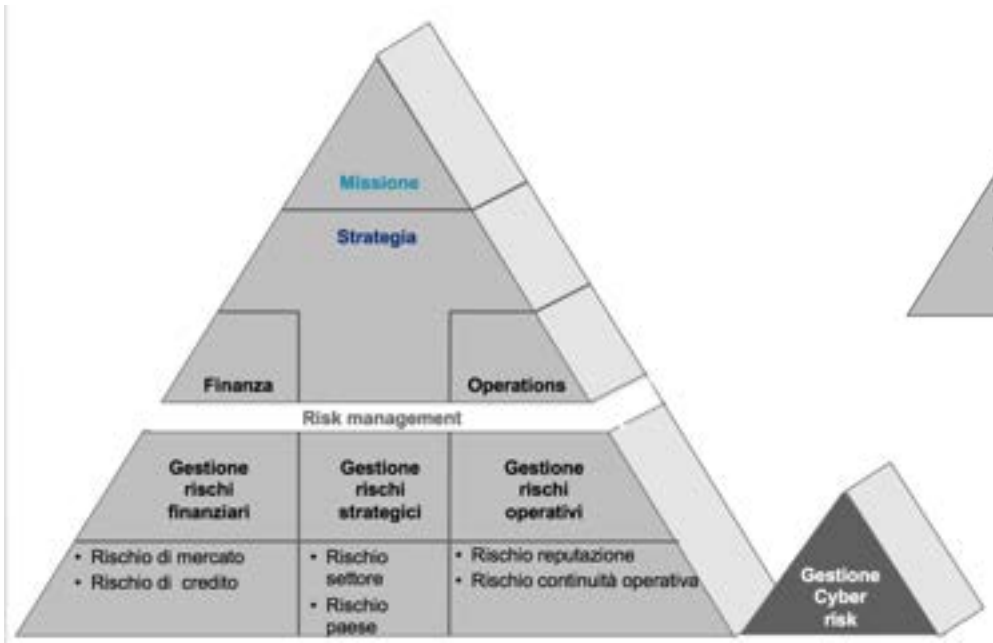
La soluzione deve essere *organizzativa* e solo di conseguenza tecnica

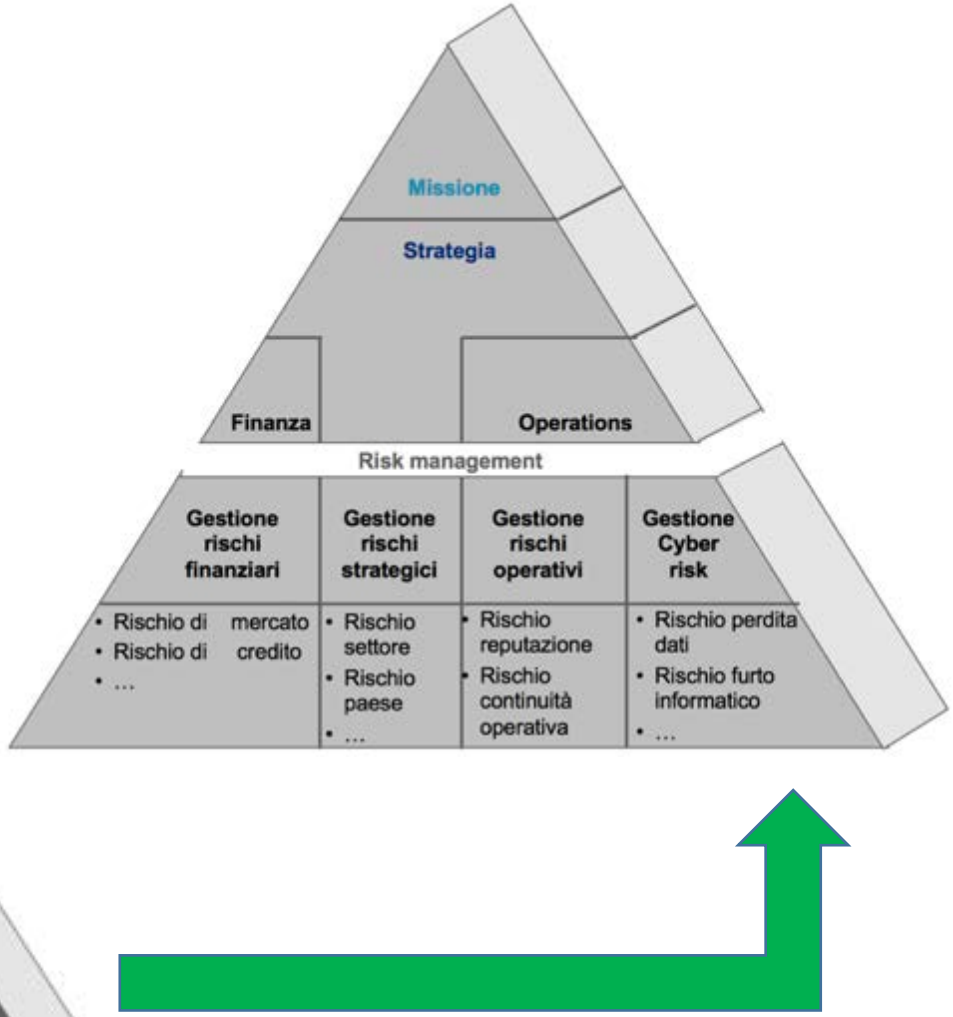


Tutta l'organizzazione è coinvolta!



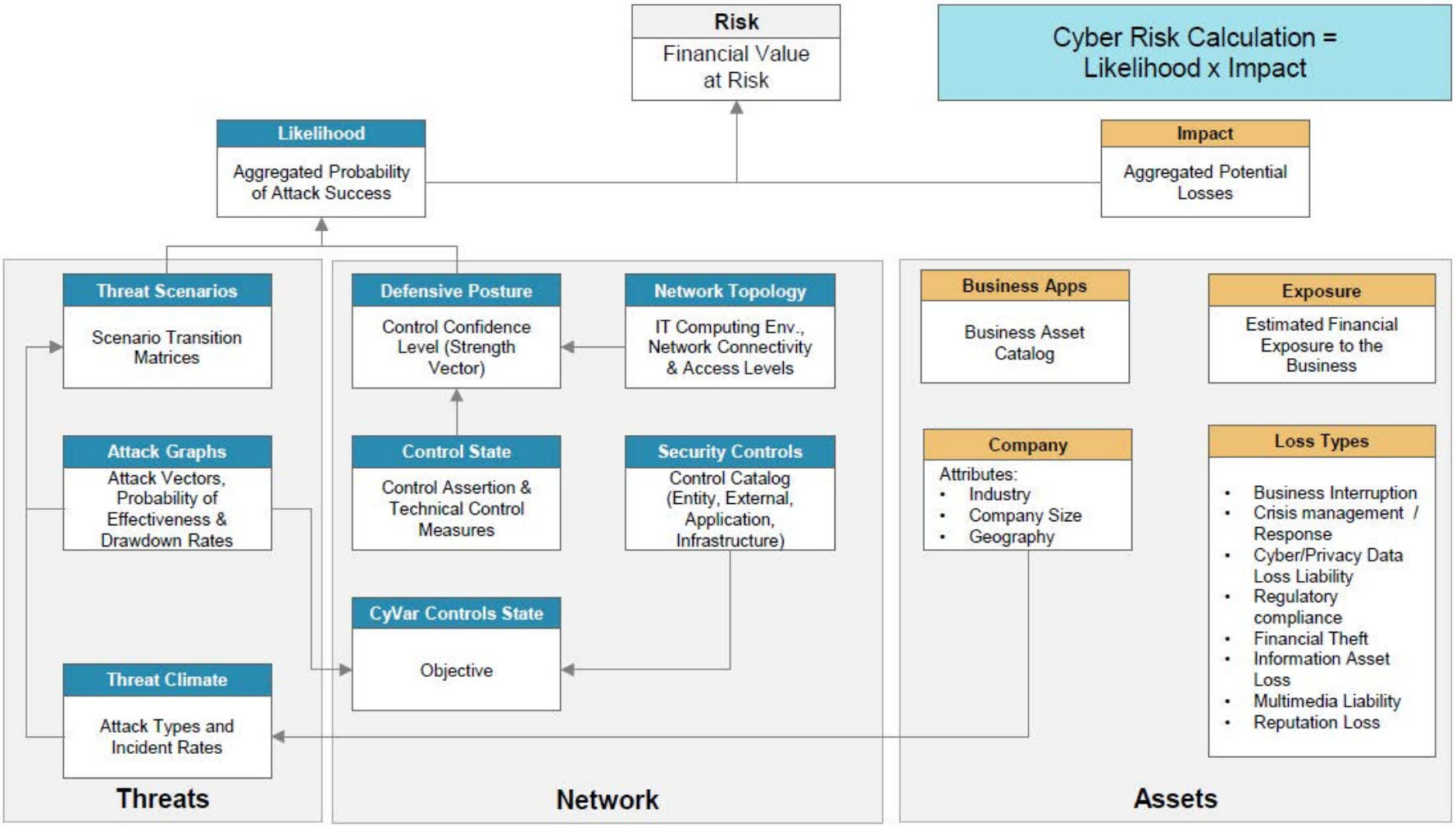
La gestione del Cyber Risk deve essere integrata nella gestione dei rischi aziendali



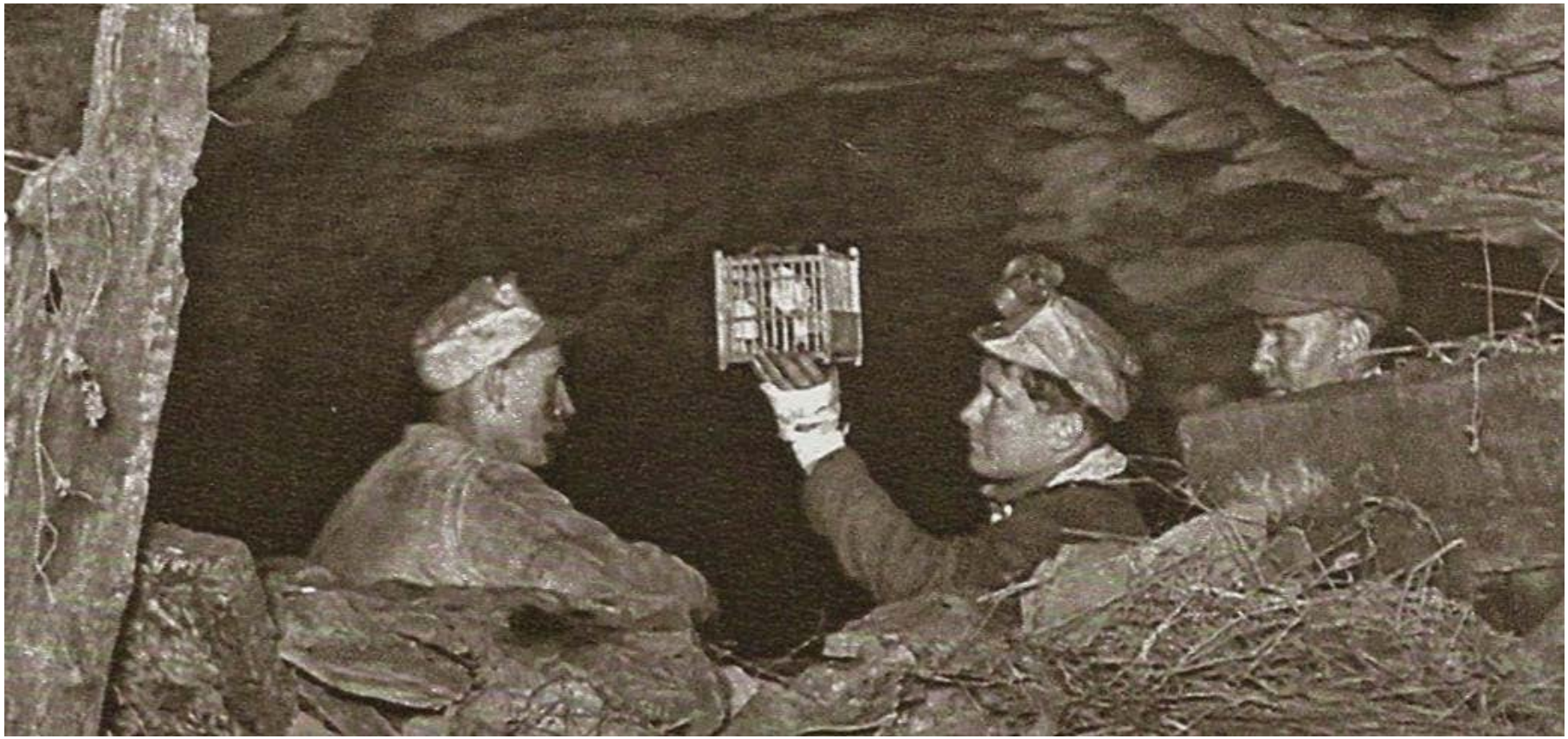


Adozione di un Framework di Corporate Cyber Risk Governance

Possiamo abbassare la probabilità, non l'impatto!



Non possiamo azzerare la probabilità di un incidente
Possiamo rendere il suo impatto *accettabile*



Le persone

Informate, consapevoli, attente

sono il moderno cardine

della sicurezza delle informazioni

Cyber Security Posture

Per disinnescare molti rischi è necessario che i **collaboratori** ed il **Top Management** siano consci di:

Attuale scenario di riferimento

Comportamenti rischiosi

Chi potrebbe attaccare

Sulla base di quali informazioni

Con che tecniche?

Quali situazioni dovrebbero far “suonare un allarme”

#iosonopreoccupato

Perché occuparsi di Cyber Security?

Rischi reali e concreti

attacchi semplici da trasformare in incidenti

grande impatto sul business

facili da prevenire

difficili da mitigare a posteriori

Conclusioni

Il **Cyber Risk** rischia di compromettere

il patrimonio informativo aziendale

non può essere percepito come un “problema tecnico”

Deve essere parte di una gestione organica che integri

persone, organizzazione, processi, strumenti

Deve essere inserito nel framework di **Enterprise Risk Management**

ed all’attenzione del Board Aziendale

Conclusioni

E’ necessaria una evoluzione

Organizzativa – Tecnologica – Legale - **Culturale**

Obiectivo
Thinking outside the box

Grazie!

CyberSecurity: perché è un problema che ci riguarda tutti

Alessio L.R. Pennasilico
apennasilico@obiectivo.it