




Workshop ARIOSTEA - 10 maggio 2018

Cyber Risk e Cyber Crime



Relatore: Dott. Cesare Burei
Docente e formatore – Cyber Risk



“Il mondo digitale si divide in due:
chi ha perso i dati e chi li perderà”



“Fra tutte le conquiste tecnologiche conseguite dall'uomo in epoca moderna, il computer sembra l'invenzione più rivoluzionaria, destinata com'è a modificare radicalmente la nostra esistenza.

I futuri ladri cercheranno di farla in barba ai computer. Anzi, è quello che già fanno. Rubando i codici o ricorrendo ai più vari imbrogli, di cui lo stupido computer non si accorge, alcuni delinquenti riescono a far finire enormi somme di danaro in mani non autorizzate.

Naturalmente, il computer può venire dotato di programmi sempre più sofisticati con i quali ovviare alle manipolazioni che vengono via via scoperte, ma ogni volta l'uomo si ingegnerà a inventare qualche trucco ancora più elaborato.

E, con ogni probabilità, ci riuscirà.”



Isaac Asimov
“Crimini e misfatti al computer”
1983



Rudimenti di lessico

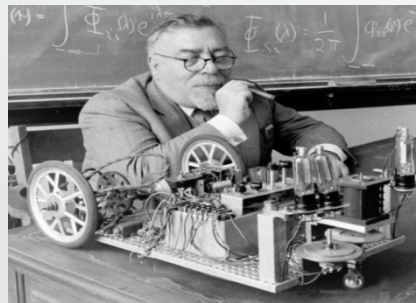
Ovvero

Come non essere completamente sprovveduti
nel mondo IT

“CYBER”

Cybernetic

Scienza che studia e realizza macchine ad alto grado di automatismo, atte a sostituire l'uomo nella sua funzione di controllore e di pilota di macchine e di impianti e dall'altro lato, inversamente, di servirsi delle macchine anzidette per studiare determinate funzioni fisiologiche e dell'intelligenza.



(Norbert Wiener – 1947)



“RISK”



“Se ci sono due o più modi
di fare una cosa,
e uno di questi modi
può condurre a una catastrofe,
allora qualcuno la farà in quel modo.”

(Ing. Edward Murphy – 1949)

“La probabilità che la tua connessione ad Internet non funzioni
è direttamente proporzionale alla necessità di usufruirne.”



ADSL	WAN	Fibra
Ethernet	LAN	Wireless
SSD	Hard Disk	Memoria USB/SD
Bluetooth	Zigbee	WiFi
Software	Licenza	EULA
Virus	Malware	Ransomware
Dropbox	Cloud	Private Cloud
Hacker	Black Hat	White Hat
IT	IoT	SCADA
Cyber Risk	Cyber Crime	



“Device”

apparecchio (meccanico od elettronico)
che svolge una determinata funzione





Collegamento di rete cablato

Linea analogica	fino a 7 KB/s
ISDN	fino a 144KB/s
ADSL	fino a 3.0Mb/s
FIBRA	fino a 125Mb/s



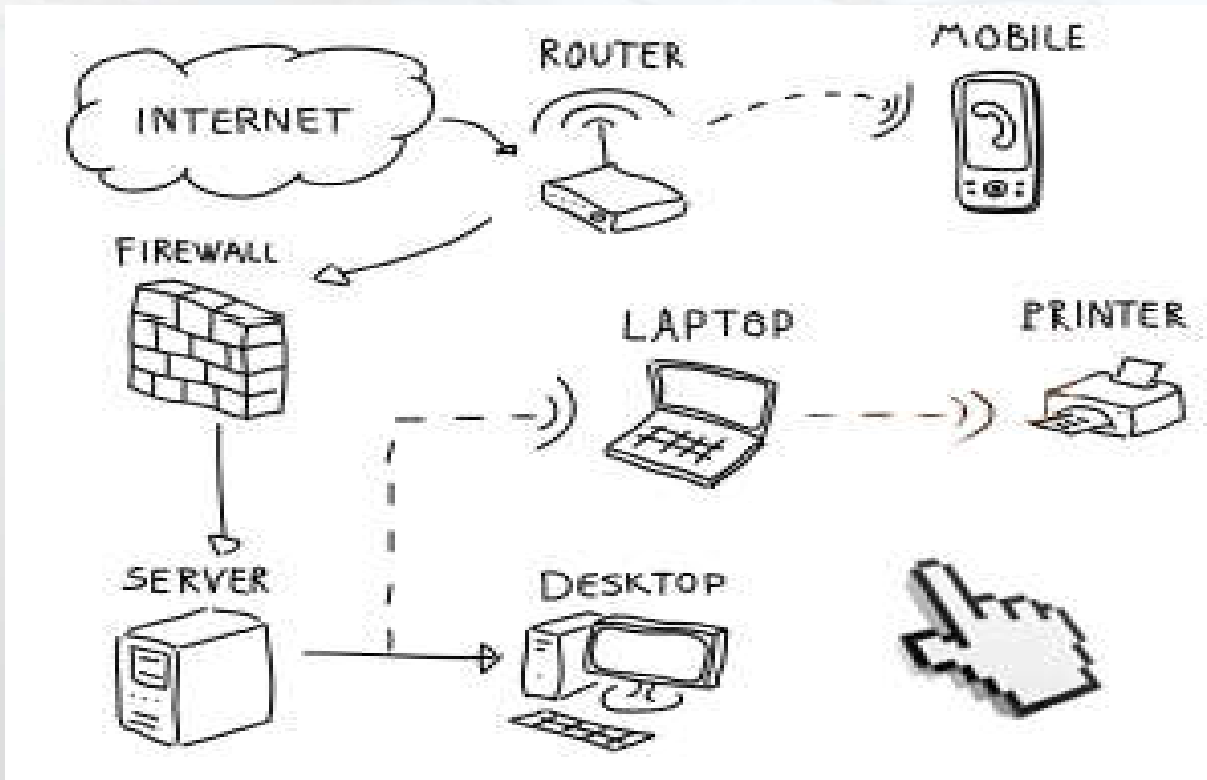
Quanto tempo ci vuole per scaricare 1Gb di informazioni?

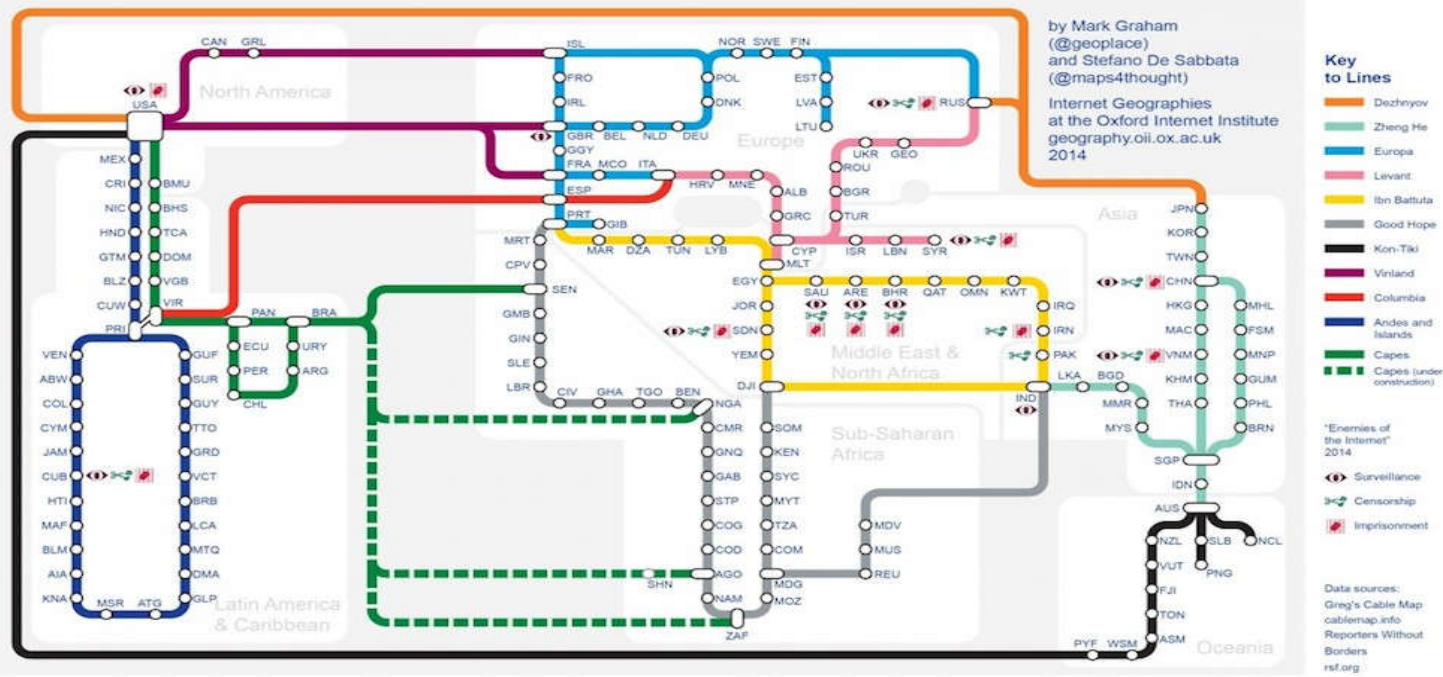
Linea analogica 39 ore

ISDN 2 ore

ADSL 6 minuti

FIBRA 8 secondi

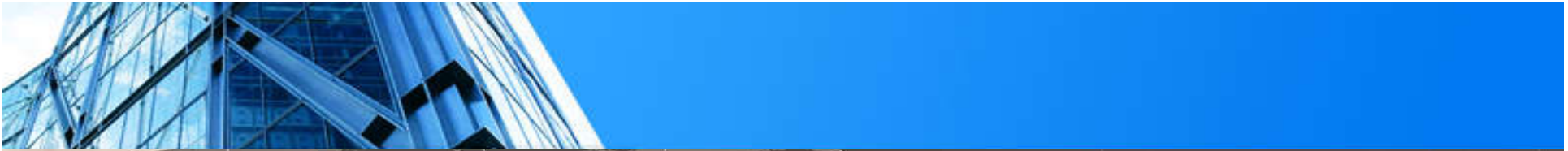




Internet Tube

An abstraction of the global submarine fibre-optic cable network







Cloud Computing



“There’s no cloud. There is someone else computer.”



Cloud Computing

Condivisione, tramite un accesso di rete fissa o mobile, di un insieme di risorse cibernetiche (reti, servers, storage, applicazioni o servizi) che possono essere rapidamente configurate e rese disponibili su richiesta.



Cloud Computing

Caratteristiche

- On demand, in maniera automatica
- Disponibilità “device independent”
- Allocazione flessibile di risorse
- Elasticità immediata
- Servizio misurabile tramite “benchmarks”.



Cloud Computing Servizi

- SaaS: Software as a service
- PaaS: Platform as a service
- IaaS: Infrastructure as a Service



FOG COMPUTING



A.I.

Artificial Intelligence



IoT

Internet of things

**Investimenti stimati tra i
40 ed i 70Mld USD
All'anno**



Cyber Risk

Criticità interne:

Know How a disposizione di tutti

Gestione delle risorse

Continuità del servizio

Simulazioni/esercitazioni

Numero di sedi

Uso di device mobili

...



Criticità esterne:

Vicinanze

Disponibilità delle connessioni fisiche

Rischi correlati

Interesse nel nostro Know How

Minacce informatiche

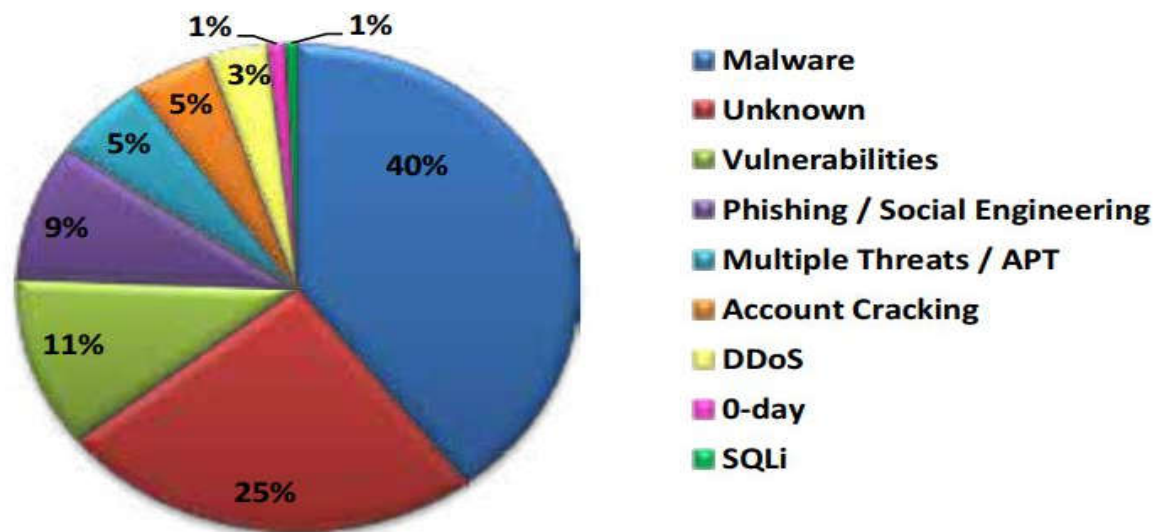
Preparazione informatica

(Carenza di) coordinamento nazionale


...

Conosci il tuo nemico?

Tipologia e distribuzione delle tecniche d'attacco nel 2017



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia




Ma cosa succede intorno a noi?

Una visione su Internet



Ma cosa succede intorno a noi?

Una visione DENTRO casa di qualcuno....



Ma cosa succede intorno a noi?

Una visione DENTRO al telefono di qualcuno....

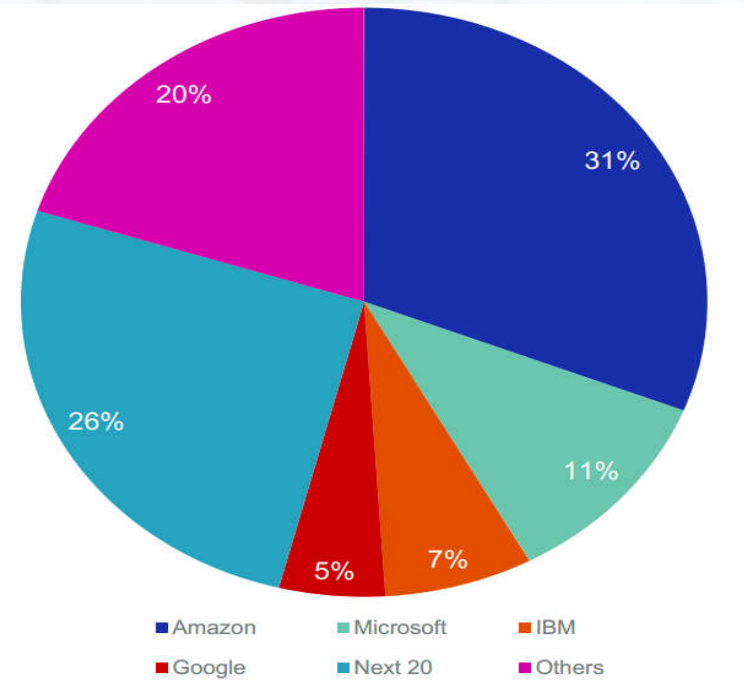


Scenari di rischio secondo i Lloyd's

“Counting the Cost 2017”

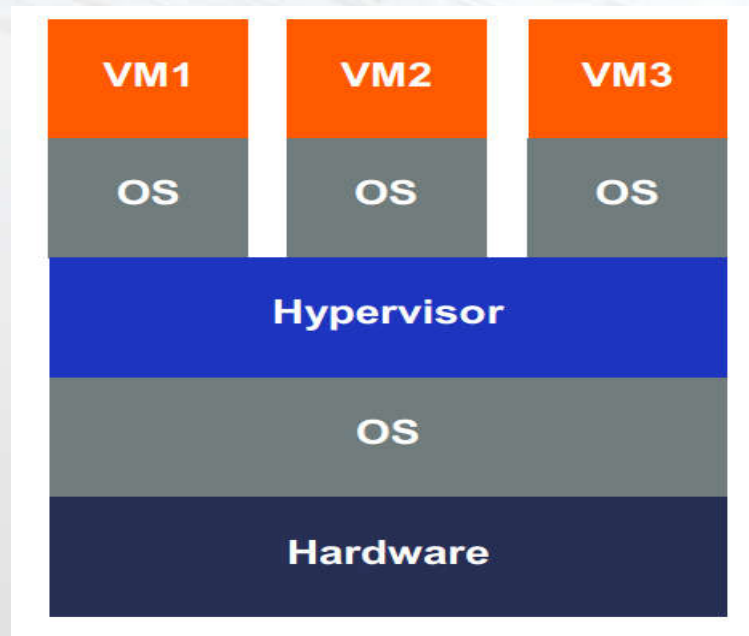
1. Cloud Service Provider

Maggiori provider cloud



Source: Forbes, 2016

Struttura di un Cloud Service Provider



Hack di un Cloud Service Provider



Day 1

Code inserted in a feature update of a particular version of ABC



Day 185

Feature widely used and integrated into ABC at update



Days 185 – 250

Other CSP's running slightly differing versions of ABC integrate feature



Day 365

Timer goes off, Malicious code enters hypervisor and triggers persistent shut down command



Day 366

Forensics and security researchers identify vulnerability



Day 367

Tier 1 CSP's start to deploy patch



Day 368

Tier 2 CSP's receive patch and begin deployment

Ramp up

CSP and server restoration takes place over the following days

Conseguenze

- Fermo di attività (diretta ed indiretta)
- Danni materiali
- Immagine e reputazione
- Contenziosi legali

Conseguenze economiche (danni)

Da \$4.6bn (fermo < 18 ore)

A \$53bn (fermo fino a 3 giorni)



Scenari di rischio secondo i Lloyd's

2. Vulnerabilità di massa

Potenziali fonti di rischio

- Vulnerabilità non (ancora) pubblicate
- Il Dark Web
- Le comunità online

Vulnerabilità di massa



Week -23

Report found on train



Week -20

First attack begins
vulnerability exposure



Week -2

Breaches detected



Week 0

Zero-day vulnerability
identified



Week 1

First patch created



Week 3

Full patch created



Week 11

Patch remediation tail



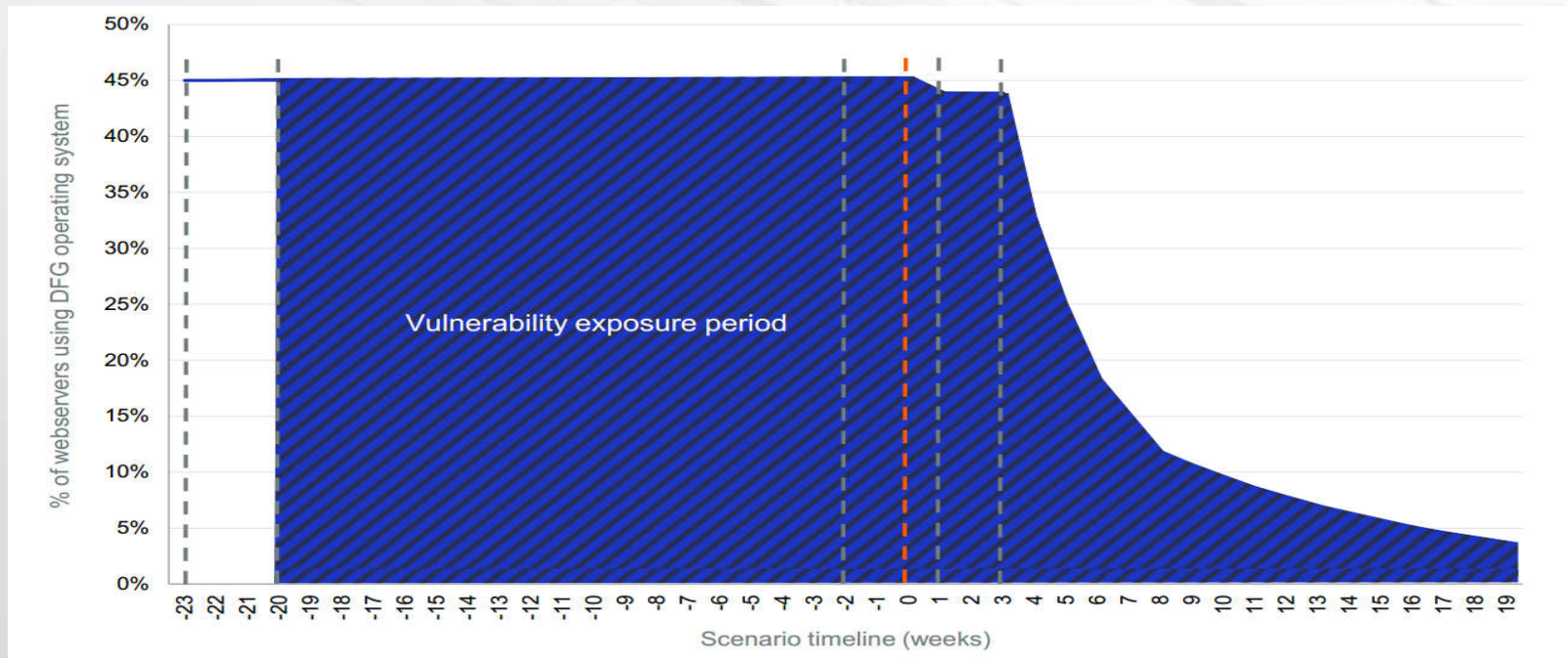
Scenari di rischio secondo i Lloyd's

Vulnerabilità Zero Day

Tempi di reazione

Da 160 a 248 giorni

Vulnerabilità di massa



Conseguenze

- Fermo di attività (diretta ed indiretta)
- Danni materiali
- Data Forensics e Remediation
- Costi di notifica
- Immagine e reputazione
- Monitoraggio del credito
- Risorse IT aggiuntive
- Contenziosi legali

Conseguenze economiche (danni)

Da \$9.68bn

A \$28.72bn



Sinistro “digitale” - 1

- Sviluppo di siti di e-commerce con subappalto
- Ottobre 2016 – code injection su 6 siti
- Conseguenze: pagamenti non pervenuti ai vendors
- Remediation: attività di forensic by Visa

- Risultato: fattura del gestore dei pagamenti a dicembre 2016 di Eur 80.000.



Sinistro “analogico” - 2

- Gestionale con backup locale e remoto
- Luglio 2017: Fenomeno Elettrico (fulmine)
- Conseguenze: distruzione locale totale
- Remediation: recupero da backup remoto



Sinistro “analogico” - 3

- Imprevisto: backup remoto fermo ad aprile 2016
- Risultato: reimputazione manuale
- Probabile rivalsa nei confronti dell’MSP
- Danno ad oggi di circa



Sinistro “analogico” - 3

Risorse utilizzate:

1. Quattro interne per 36 giorni
2. Quattro interinali per 111 giorni
3. Quattro interne per 36 giorni

Costo azienda 1. = $4 \times 8 \times 35 \times 36 = 40.320\text{€}$

Costo azienda 2. = $4 \times 8 \times 18 \times 111 = 63.936\text{€}$

Costo azienda 3. = $4 \times 8 \times 35 \times 36 = 40.320\text{€}$



Sinistro “digitale” - 4

- Ubicazione: tutto il mondo (06/2017)
- Attacco tramite codice “Mirai”
- Fermo di tutti i sistemi aziendali



Sinistro “digitale” - 4

- Fermo di attività
- Sanificazione e ripristino dei sistemi



Sinistro “digitale” - 4

Danni patrimoniali puri

Cause “seriali”

Class-action

Danno reputazionale

Compromissione di dati soggetti a privacy

Furto di informazioni riservate

Ambiti aziendali interessati

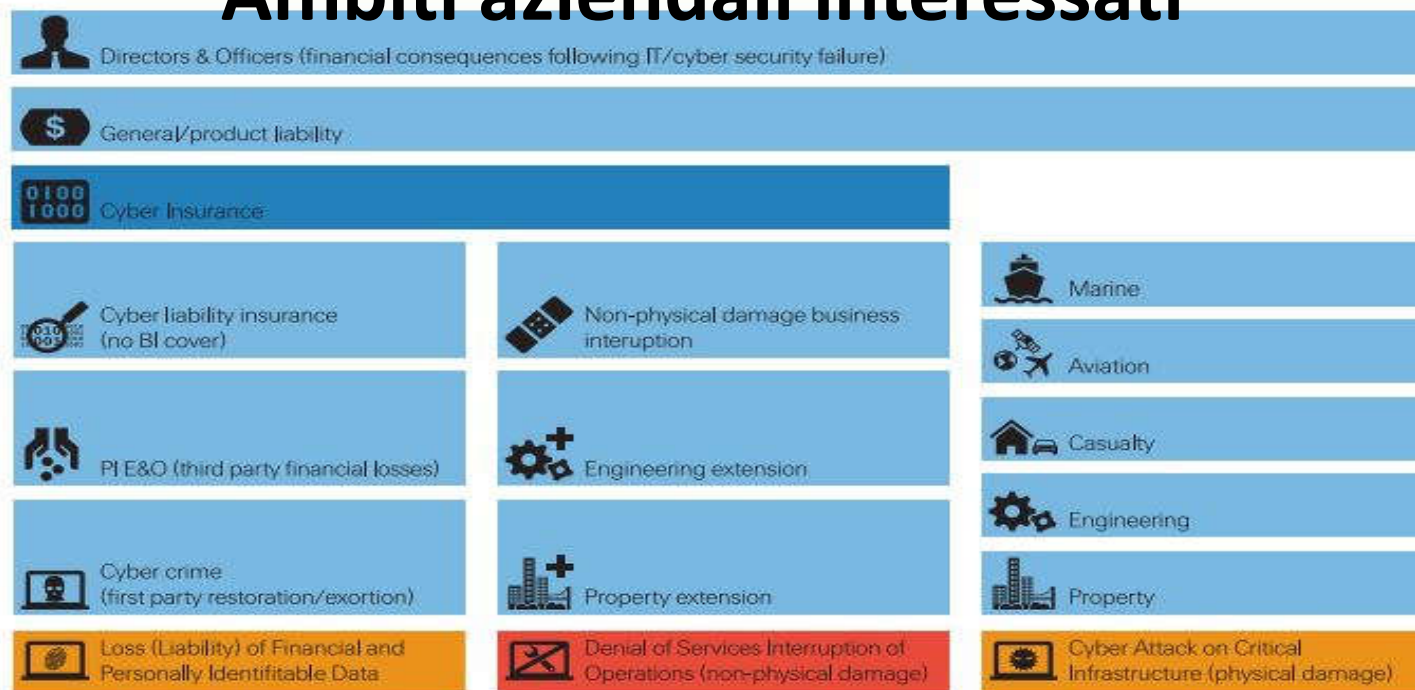
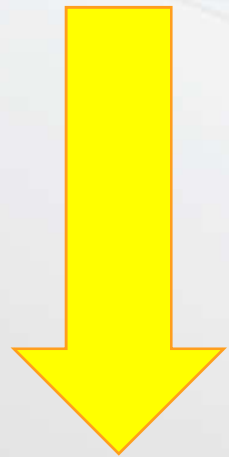


Figure 8: Example of potentially exposed insurance products.

Gestione della Crisi - Quanto deve durare?



Attività normale

Sinistro

Emergenza

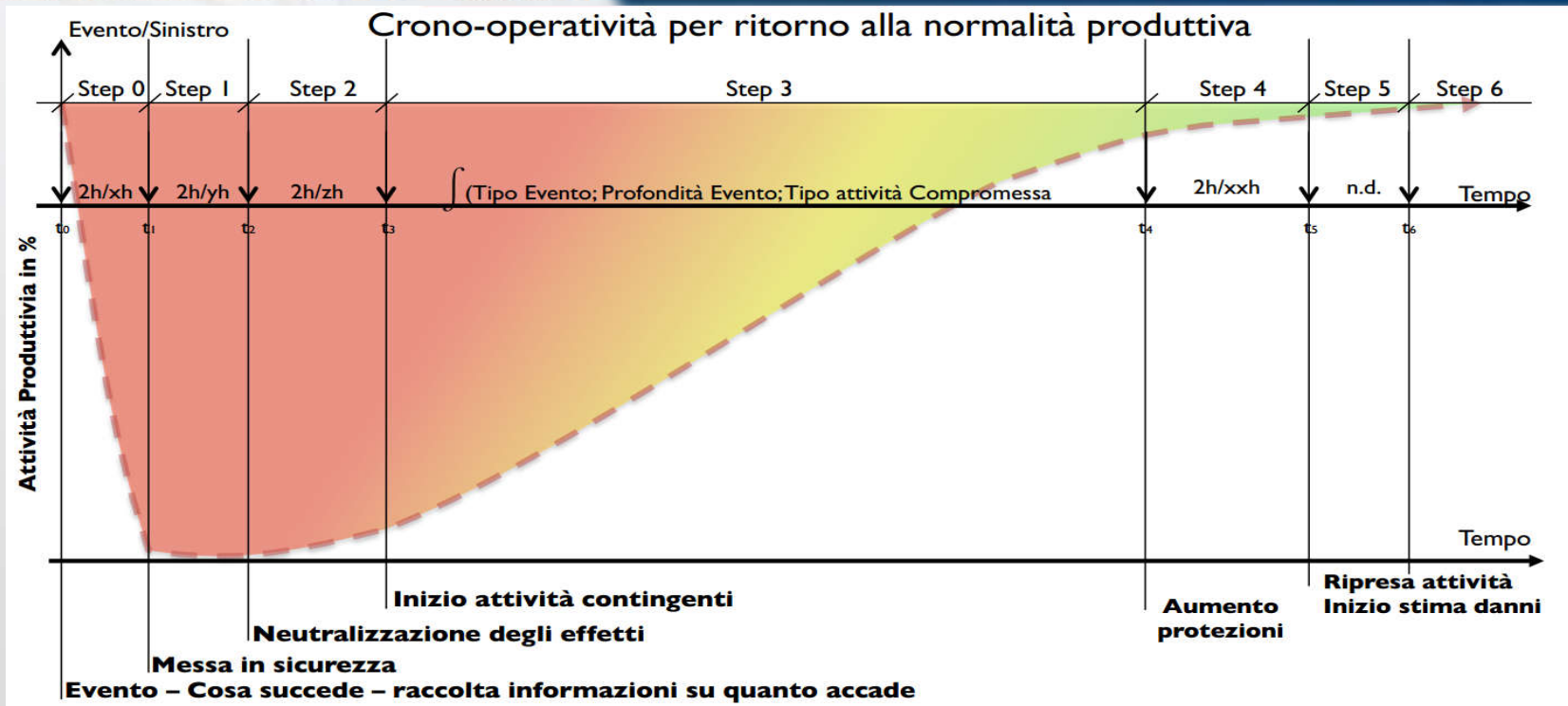
Crisi

Continuità

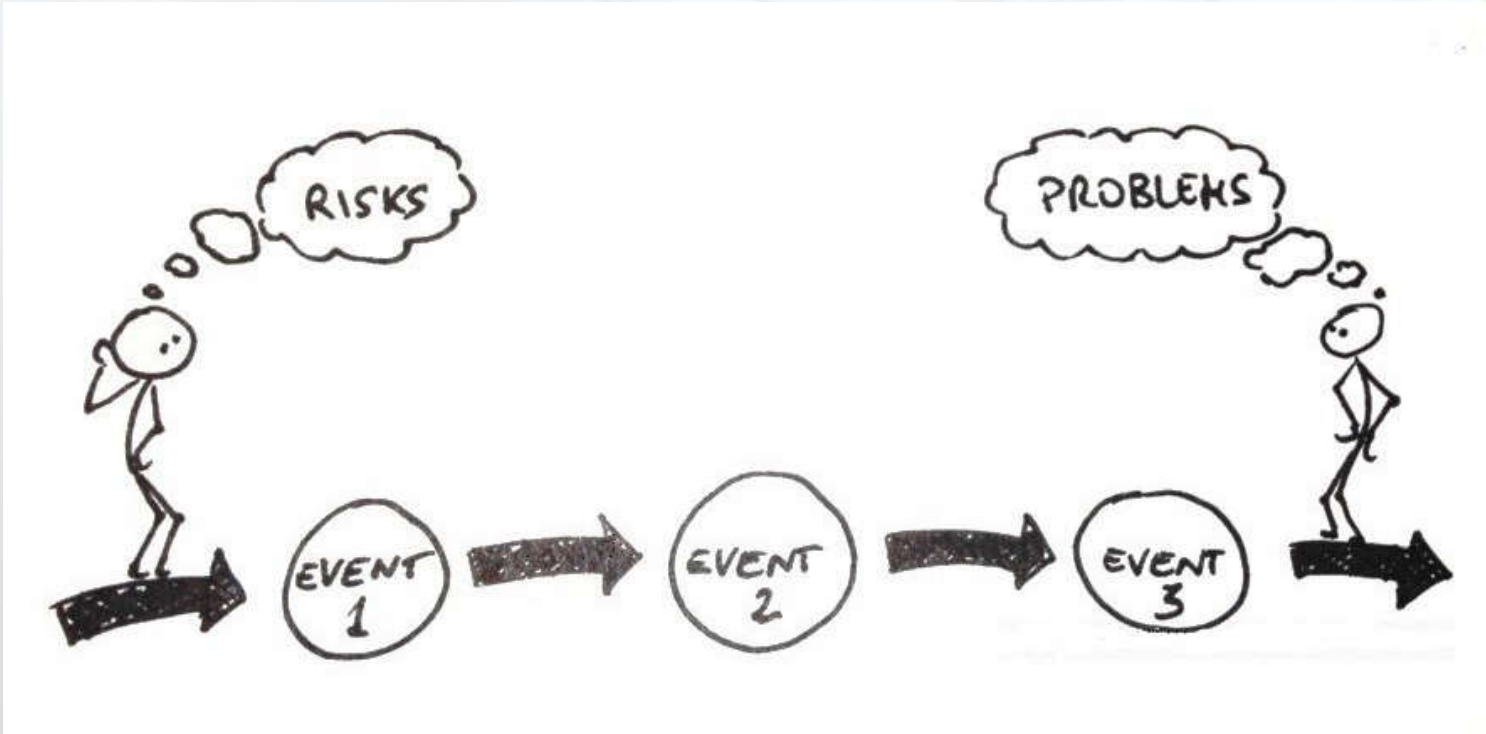
Recovery

Attività normale

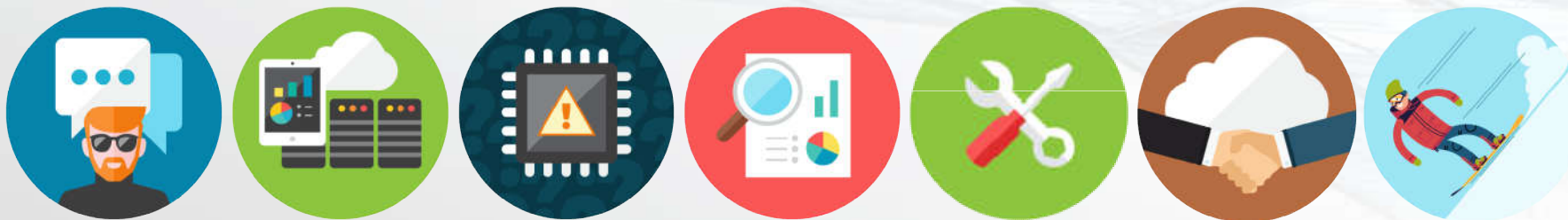
Il meno possibile...



Courtesy of Gianluigi Lucietto - UniVR



Dal Cyber Risk al Cyber Risk Management

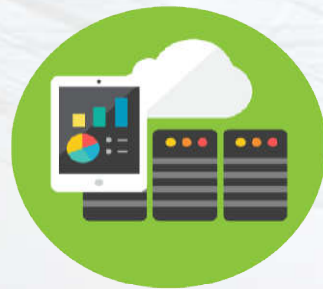


Per arrivare ad una “resilienza” cyber.



Tavolo di lavoro aziendale

Gruppo di lavoro periodico



Inventario degli asset digitali



Mappatura dei rischi esogeni ed endogeni



Stima delle conseguenze economiche

Fermo di esercizio, perdita di reputazione, costi propri di emergenza, danni a terzi



Investimenti in mitigazione del rischio, formazione e compliance



Trasferimento del rischio Assicurazione Cyber



State sereni (?)



Grazie per l'attenzione e... fate i backup!



Workshop ARIOSTEA CIIP - maggio 2018