Analisi e gestione del rischio cyber

Vincenzo Calabrò

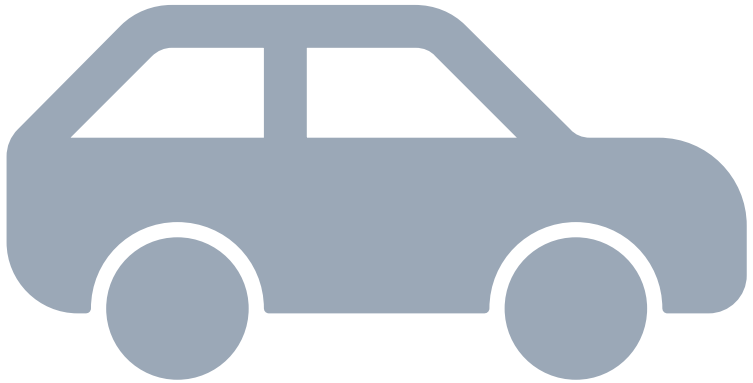
PARTE 1 –
SCALDIAMO
I MOTORI

PARTE 2 –
E' TEMPO
DI 31000

PARTE 3 –
INFORMATION
SECURITY

PARTE 4 –IL
CISO (CHIEF INFORMATION
SECURITY MANAGER)

PARTE 1 – SCALDIAMO I MOTORI



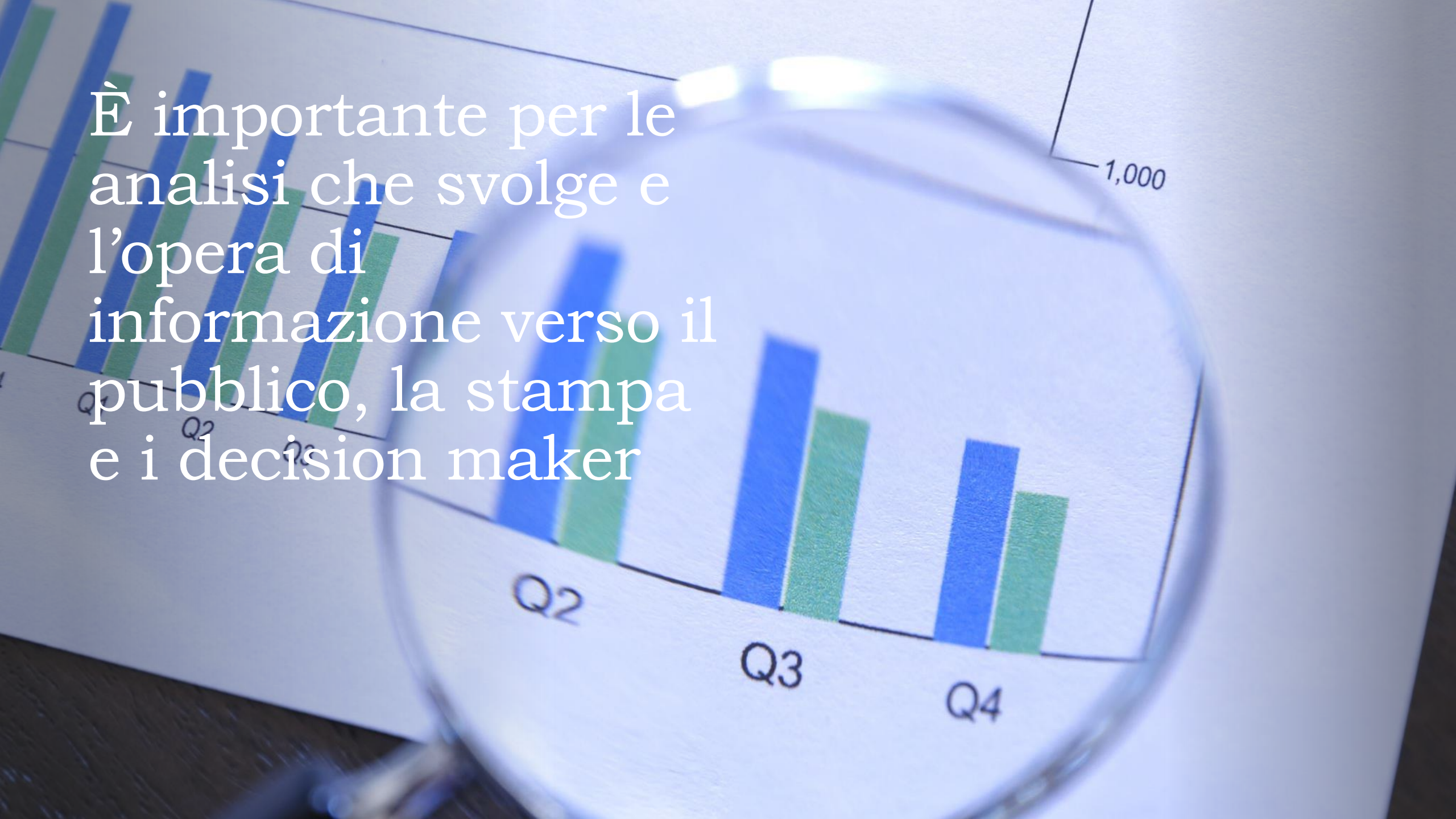
Cosa significa

PxI

Indice

Rapporto Clusit

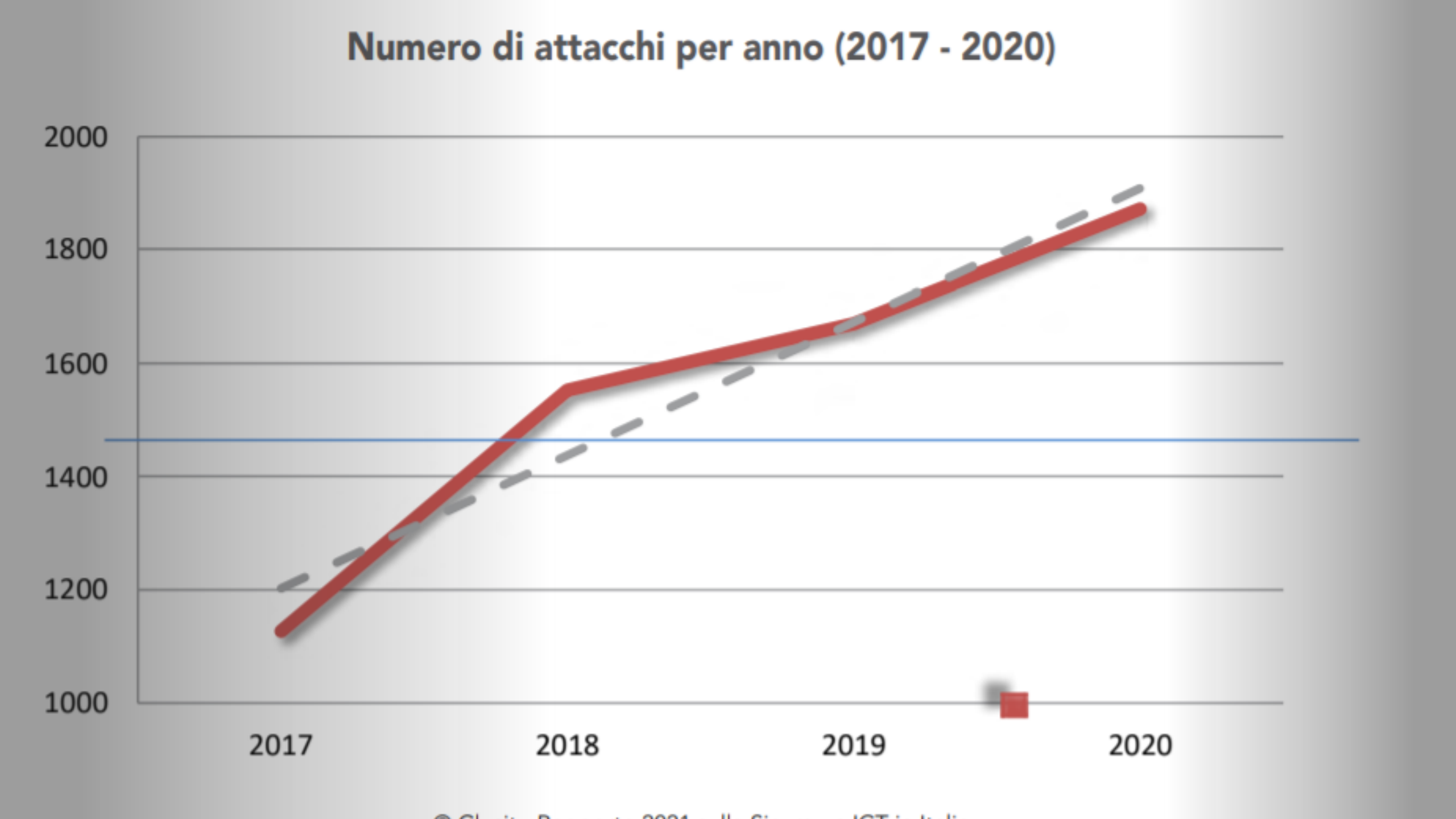
https://clusit.it/rapporto-clusit/



È importante per le analisi che svolge e l’opera di informazione verso il pubblico, la stampa e i decision maker

Analisi dei principali cyber attacchi noti a livello globale del 2020

In questa prima sezione del Rapporto CLUSIT 2021, come di consueto, proponiamo una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel 2020, confrontandoli con i dati raccolti nei 3 anni precedenti[12].
Lo studio si basa su un campione che al 31 dicembre 2020 è costituito da **11.959** attacchi noti di particolare gravità avvenuti nel mondo (inclusa l'Italia) dal primo gennaio 2011 (di cui **5.093** dal 2017), ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti. Di questi **1.871** sono avvenuti nel 2020 (**+12%** rispetto al 2019, **+ 20%** rispetto al 2017). Il numero di attacchi rilevati nel 2020 segna una differenza del **+29%** rispetto alla media degli attacchi per anno del triennio precedente (1.449), visualizzata con una linea blu orizzontale nel grafico seguente.


Numero di attacchi per anno (2017 - 2020)
2000
1800
1600
1400
1200
1000
2017
2018
2019
2020

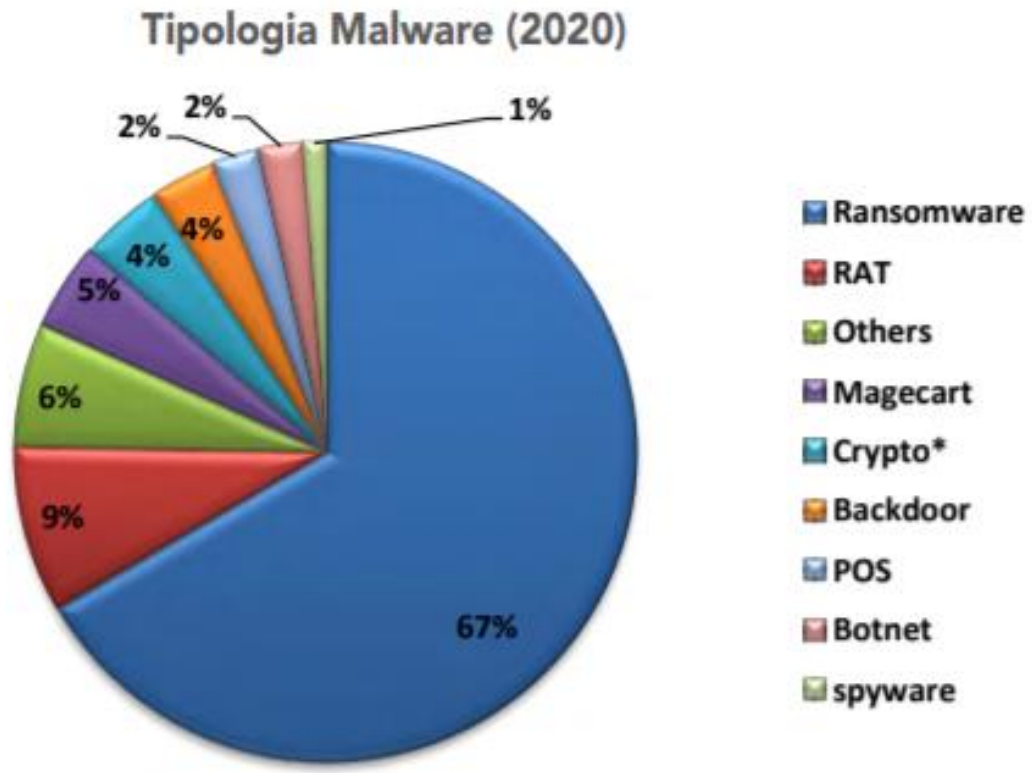
Distribuzione degli attaccanti

ATTACCANTI PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Cybercrime	857	1232	1383	1517	9.7%	↗
Hacktivism	79	61	48	47	-2.1%	↗
Espionage / Sabotage	129	203	204	266	30.4%	↑
Cyber warfare	62	56	35	41	17.1%	↑
Espionage / Sabotage + Cyber Warfare	191	259	239	307	28.5%	↑
TOTALE	**1127**	**1552**	**1670**	**1871**	**+12%**	

Distribuzione delle tecniche di attacco

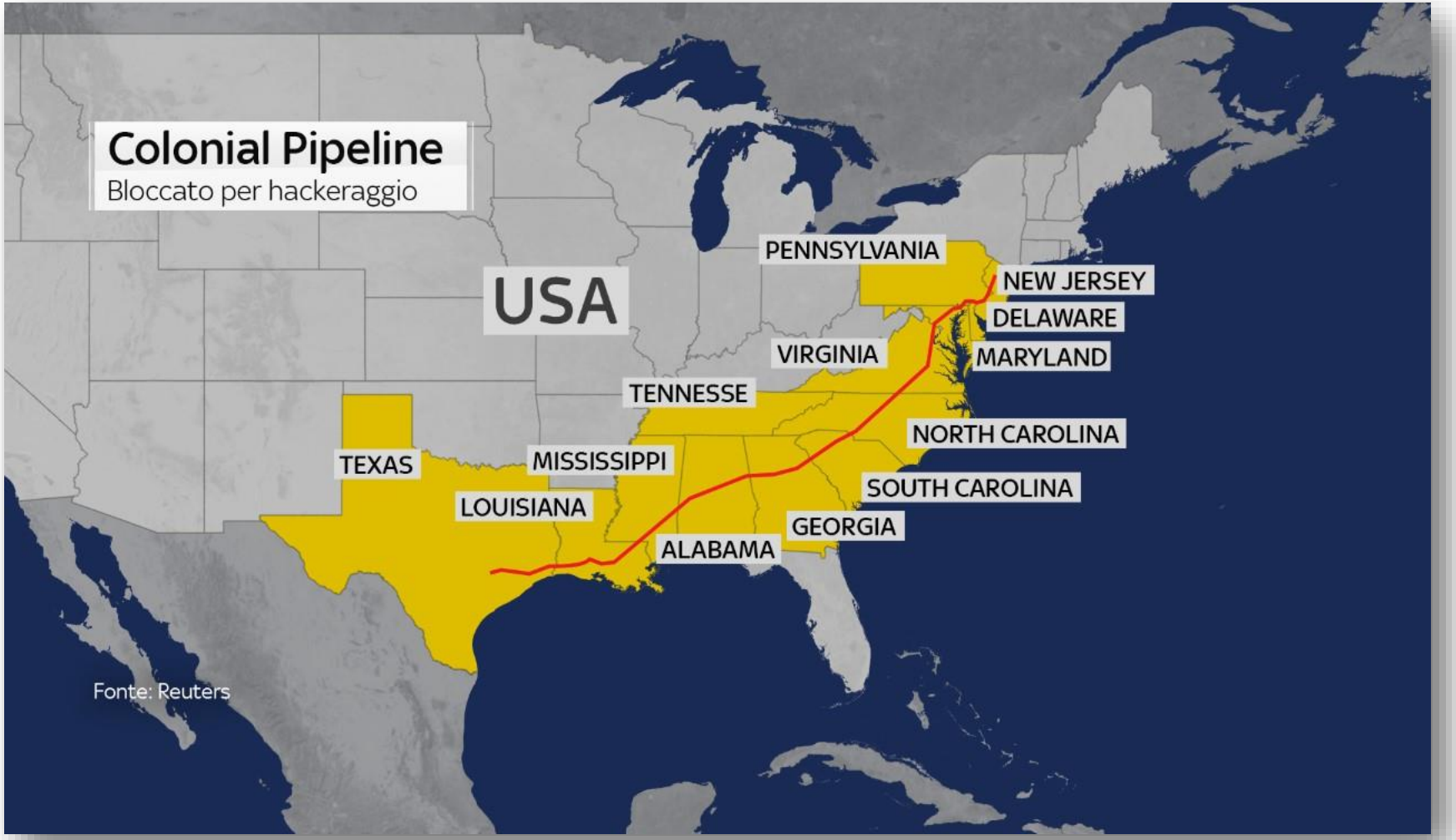
TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	↗
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	↗
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

VITTIME PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Institutions: Gov - Mil - LEAs - Intelligence	179	252	247	258	4.5%	↗
Multiple targets	222	304	395	374	-5.3%	↗
Health	80	159	203	215	5.9%	↗
Banking / Finance	117	157	100	97	-3.0%	↗
Online Services / Cloud	95	129	186	177	-4.8%	↗
Research - Education	71	109	141	207	46.8%	↑
Software / Hardware Vendor	68	109	70	113	61.4%	↑
Entertainment / News	115	102	83	69	-16.9%	↓
Critical Infrastructures	40	57	50	70	40.0%	↑
Hospitability	34	45	27	22	-18.5%	↓
GDO / Retail	24	39	37	35	-5.4%	↗
Others	40	30	53	140	164.2%	↑
Org / ONG	8	18	17	26	52.9%	↑
Gov. Contractors / Consulting	6	14	11	16	45.5%	↑
Telco	13	11	18	25	38.9%	↑
Automotive	4	9	10	8	-20.0%	↓
Security Industry	11	4	17	12	-29.4%	↓
Religion	0	3	2	5	150.0%	↑
Chemical / Medical	0	1	3	2	-33.3%	↓
TOTALE	**1127**	**1552**	**1670**	**1871**	**+12%**	



Colonial pipeline cyberattack

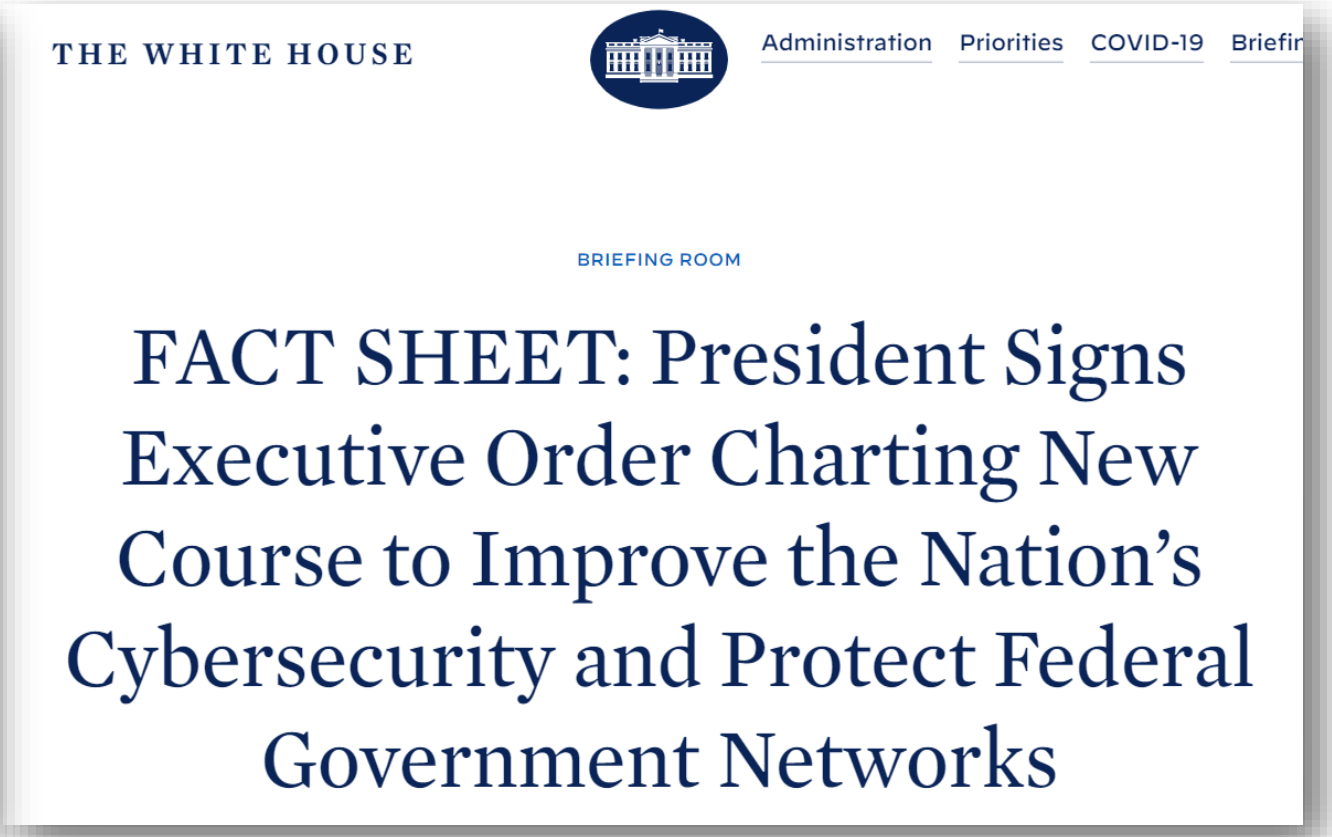
- Il più grande oleodotto americano (8850 chilometri di condotte)
- Fornisce il 45% del carburante della East Coast



FONTE: SKY TG24

6 giorni di stop – 5 milioni di riscatto

FONTE: https://seekingalpha.com/news/3693634-biden-turns-to-emergency-powers-to-counter-colonial-pipeline-disruption



FONTE: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

Obiettivi del Presidential Executive Order

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
- Improve Software Supply Chain Security
- Establish a Cybersecurity Safety Review Board
- Create a Standard Playbook for Responding to Cyber Incidents
- Improve Detection of Cybersecurity Incidents on Federal Government Networks
- Improve Investigative and Remediation Capabilities

FBI & CISA sul caso Colonial Pipeline

Cybersecurity and Infrastructure Security Agency

From Wikipedia, the free encyclopedia

The **Cybersecurity and Infrastructure Security Agency** (**CISA**) is a standalone United States federal agency, an operational component under Department of Homeland Security (DHS) oversight.[3] Its activities are a continuation of the National Protection and Programs Directorate (NPPD). CISA was established on November 16, 2018 when President Donald Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018.[4][3]

Former NPPD Under-Secretary Christopher Krebs was CISA's first Director, and former Deputy Under-Secretary Matthew Travis was its first Deputy Director.[5][6] The expected role of CISA is to improve cybersecurity across all levels of government, coordinate cybersecurity programs with U.S. states, and improve the government's cybersecurity protections against private and nation-state hackers.[3]

Contents [hide]

History [edit]

Cybersecurity and Infrastructure Security Agency

Agency overview

Formed	2018
Jurisdiction	United States
Headquarters	Rosslyn, Arlington, Virginia
Employees	3,374 (2017)[a]
Annual budget	$3.16 billion (2020)
Agency executives	Brandon Wales, Director (acting)[1]

FONTE: https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency

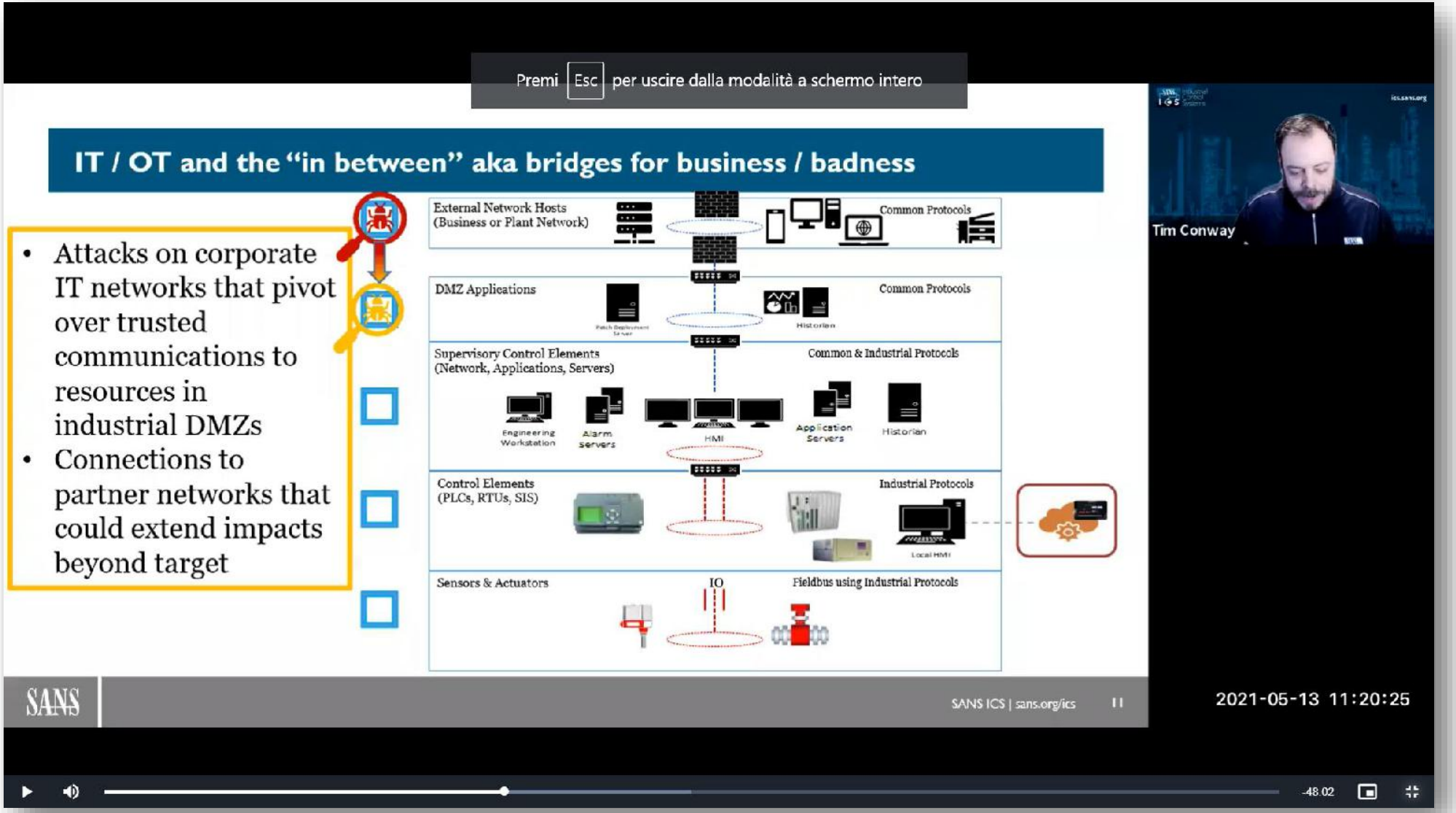
Un secondo commento

280 stazioni pompaggio e controllo

“Many believe that this attack was a result of more engineers remotely accessing control systems for the pipeline from home using a remote desktop software such as TeamViewer and Microsoft Remote Desktop," said Troy Gill, manager of security research at security provider Zix. "The pandemic forces more employees to work from home, and unfortunately, many organizations are still trying to secure their devices, remote access points and overall networks."

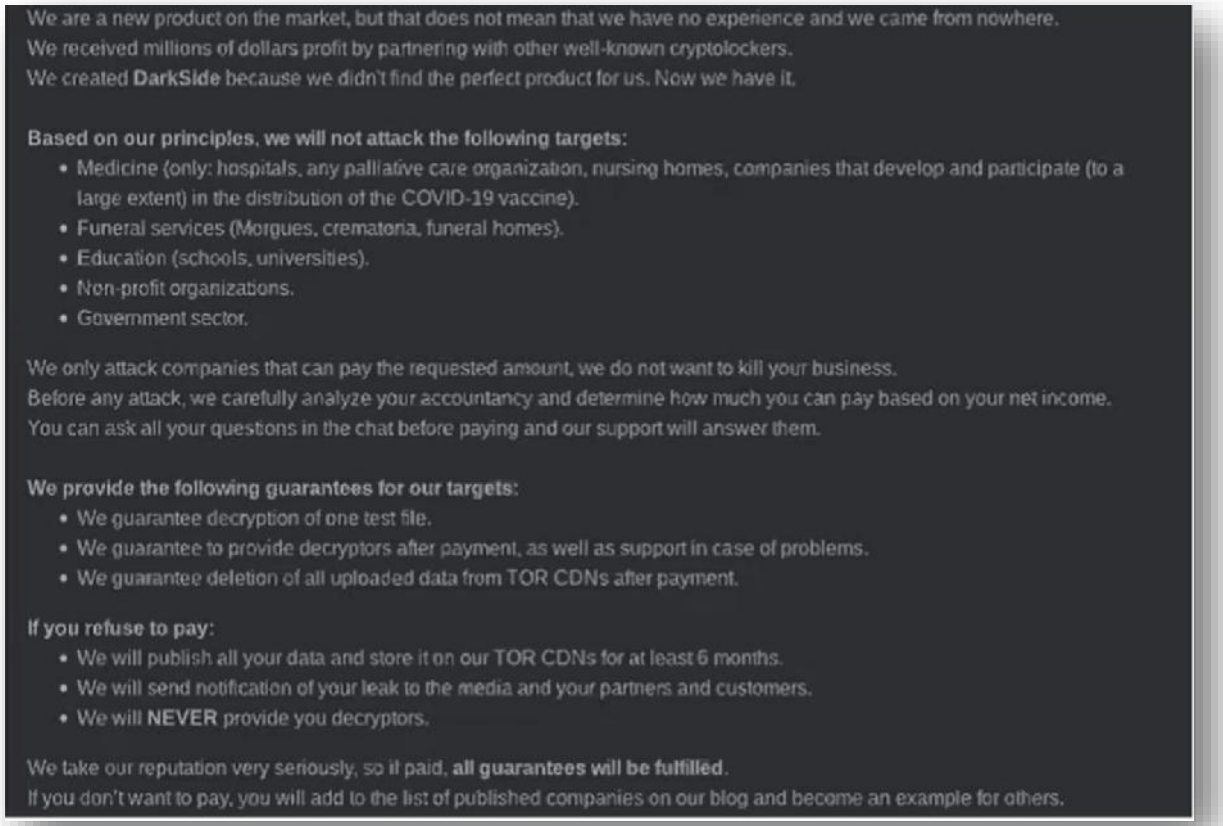
FONTE: https://www.techrepublic.com/article/how-to-prevent-another-colonial-pipeline-ransomware-attack/

Osmosi di IT / OT. Due mondi sempre più uniti



FONTE: https://www.sans.org/services/video-player/?key=iwNOQX8XM1h2

Darkside



We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

FONTE: Dark web; pagina del gruppo criminale

CYBERSECURITY360 Ransomware Darkside, organizza

Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo

La variante 2.0 del ransomware Darkside è l'occasione per analizzare l'evoluzione delle attività di organizzazione e affiliazione del malware, alla luce del core business dei nuovi attacchi informatici basato sul modello Ransomware-as-a-Service. Ecco il modus operandi e le soluzioni di mitigazione

13 Apr 2021

B Giorgia Benatti
Focus team Legal Tech SC Avvocati Associati e team Compliance di SCnet Compliance&Corporate

C Vittorio Colomba
Avvocato esperto di diritto delle nuove tecnologie

FONTE: https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-darkside-organizzazione-e-affiliazione-il-core-business-dei-nuovi-attacchi-informatici/

Organizzazione criminale; Malware as a Service

‘Majority’ of ransom paid by Colonial Pipeline seized and returned by DOJ

Of the $4.4 million the company paid, $2.3 million was returned.

By Jonathan Greig | June 7, 2021 -- 20:29 GMT (21:29 BST) | Topic: Government : US

The Department of Justice announced on Monday that it managed to recover some of the ransom that was paid by Colonial Pipeline to the cybercriminals behind the DarkSide ransomware last month.

While this is not the first time the government has been able to get some money back to victims, Deputy Attorney General Lisa Monaco said during a press conference that this was a first for the new Ransomware and Digital Extortion Task Force that was created in April to address the growing number of cyberattacks.

FONTE: https://www.zdnet.com/article/majority-of-ransom-paid-by-colonial-pipeline-seized-and-returned-by-doj/

Colonial Pipeline sends breach letters to more than 5,000 after ransomware group accessed SSNs, more

Colonial Pipeline said the leaks involved the personal information of current and former employees.

By Jonathan Greig | August 16, 2021 -- 20:46 GMT (21:46 BST) | Topic: Security

Colonial Pipeline is sending out breach notification letters to 5,810 current and former employees whose personal information was accessed by the DarkSide ransomware group during an attack in May.

The company admitted in an August 13 letter that on May 6, the ransomware group "acquired certain records" stored in their systems.

FONTE: https://www.zdnet.com/article/colonial-pipeline-sends-breach-letters-to-more-than-5000-after-ransomware-group-accessed-ssns-more/

E poi?

Attacco al sistema di prenotazione vaccinale della regione Lazio

CORRIERE DELLA SERA

ROMA / CRONACA

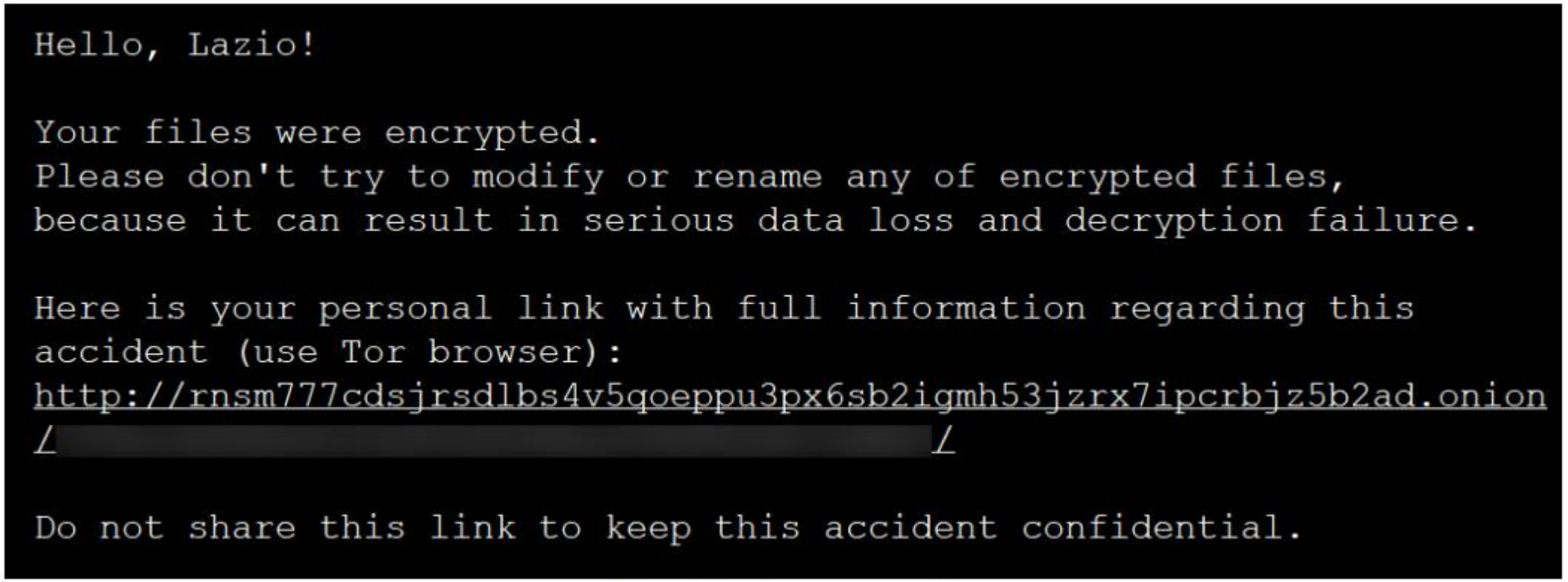
REGIONE LAZIO

Attacco hacker, ecco come sono stati «bucati» i sistemi della regione Lazio

Per l'attacco hacker che ha colpito la regione Lazio sono state usate le credenziali di un dipendente di Frosinone. Criptati milioni di dati dal ransomware. Gli esperti: «Senza chiave andrà tutto perso»

di Alessio Lana e Fiorenza Sarzanini

Il governatore Nicola Zingaretti



Alleged Lazio ransom note

FONTE: https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/

Conseguenze

- Chiesto un riscatto di 5 milioni di euro in cryptovalute
- Sistemi regionali (in particolare quelli vaccinali e sanitari) bloccati dal primo al sei agosto
- Fortissimo interessamento dei media e grande confusione nella comunicazione

Venerdì 6 Agosto 2021, 13:36 - Ultimo aggiornamento: 15:05

293

1

E' uscito poco fa dalla questura di **Frosinone** N. B., 61 anni, impiegato presso la Regione (Enti Locali) che è stato sentito in merito all'**attacco hacker** del sito regionale. Ai poliziotti ha detto che, stando a casa, in smart working, lavora spesso di sera per ultimare le pratiche a lui assegnate. Ha aggiunto anche di non essersi «accorto di nulla» nella notte in cui il sito è stato attaccato (si presume) attraverso il suo computer.

FONTE: https://www.ilmessaggero.it/roma/news/attacco_hacker_regione_lazio_interrogatorio_impiegato-6124289.html

1. Furto delle credenziali VPN

Cos'è Emotet?

Emotet è un programma malware originariamente sviluppato sotto forma di trojan bancario. L'obiettivo era quello di accedere a dispositivi stranieri e spiare i dati privati sensibili. Emotet ha ingannato i programmi anti-virus di base nascondendosi da essi. Una volta infettati i sistemi, il malware si diffonde come un worm cerando di infiltrarsi in altri computer nella rete.

Emotet si diffonde principalmente attraverso e-mail di spam. L'e-mail contiene un collegamento dannoso o un documento infetto. Scaricando il documento o aprendo il collegamento, vengono automaticamente scaricati altri malware nel computer. Le e-mail sono state create per sembrare molto autentiche e molte persone sono rimaste vittime di Emotet.

FONTE: https://www.kaspersky.it/resource-center/threats/emotet

2. Installazione di Emotet

A

questo punto tutto era pronto per il terzo passaggio, il clou dell'operazione, **l'inserimento del ransomware**, il programma che ha criptato i dati e chiesto il riscatto. Insomma, u na procedura che ricalca un copione già letto favorita però dall'assenza di una procedura di autenticazione a due fattori da parte del dipendente, quella misura che oltre a username e password chiede un secondo modo per confermare la propria identità come per esempio un sms sul telefono o un'app che rilascia un codice.

FONTE: https://www.corriere.it/cronache/21_agosto_03/attacco-hacker-lazio-vpn-5d4eb07e-f420-11eb-9680-9b12a81aa8eb.shtml

3. Inserimento del ransomware

chiave che ti do io dietro pagamento. Per fare questa cosa hanno cercato di eliminare tutte le copie di salvataggio, proprio per evitare che la vittima recuperasse i dati. In questo caso i dati di salvataggio non sono stati cifrati perchè anche questa sarebbe un'operazione troppo onerosa, ma sono stati cancellati con una tecnica sofisticata sovrascrivendo nuovi dati e cifrando i dati primari". "Peccato- ha proseguito- che questa operazione sia stata sventata dal sistema che gestiva questi dati di salvataggio, che non è un disco normale ma un'attrezzatura per data center che emula le vecchie librerie robotizzate a nastro e quindi ha un disaccoppiamento molto importante tra le funzioni di alto livello e lo strato fisico. Le cancellazioni sono state soltanto logiche: i dati sono rimasti nel substrato delle memorie e con operazioni tecniche piuttosto sofisticate è stato possibile recuperarli" ha concluso Giustozzi. (Fde/ Dire) 17:51 06-08-21 NNNN

14.4K 18:11

FONTE: Account ufficiale regione Lazio, 9 agosto. Attribuito a Corrado Giustozzi

Storia plausibile, dice **Paolo dal Checco, ingegnere forense e tra i massimi esperti del tema**: "Può succedere che i dati siano solo cancellati, anche se di solito i ransomware riescono a criptare anche i backup".

Plausibile, ma che lascia perplessi numerosi tecnici, in particolare su **Twitter** e su chat dedicate alla security su **Telegram**: Matteo Flora si è per esempio detto scettico rispetto all'annuncio del ritrovamento dei dati (presentato per la prima volta ieri sera da Corrado Giustozzi, che lavora sul caso e finora avrebbe sempre parlato autorizzato dalla Regione), ma "**sarà facile vedere se hanno pagato o meno** il riscatto. Se non escono i dati, hanno pagato".

Insomma, il sospetto è che i dati siano stati recuperati perché la Regione ha pagato il riscatto, **ipotesi fin dall'inizio scartata anche dal governo**. Comunque, la piattaforma vaccinale è già

FONTE: https://www.repubblica.it/tecnologia/2021/08/06/news/l_attacco_alla_regione_lazio_il_backup_che_salva_e_i_dubbi_sul_riscatto-313139323/

Risoluzione

Hard National Security Choices

LAWFARE

SUPPORT

Sunday, September 26, 2021

TOPICS | HOME | REVIEWS AND ESSAYS | FOB BLOG | AEGIS | RESOURCE PAGES | SPECIAL FEATURES | MORE

CYBERSECURITY

SolarWinds and the Holiday Bear Campaign: A Case Study for the Classroom

By **Robert Chesney** Wednesday, August 25, 2021, 8:01 AM

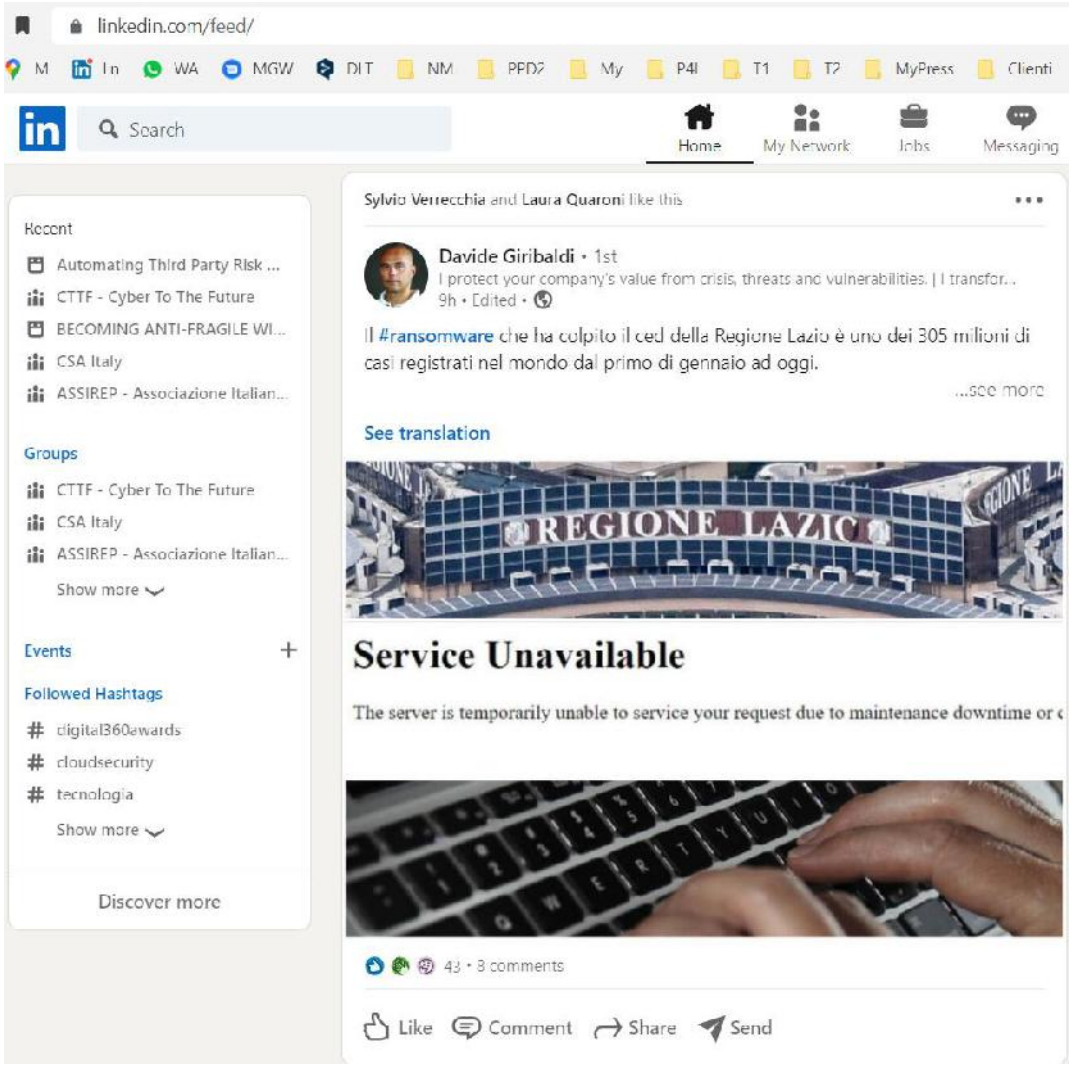
Bobby Chesney is the **Charles I. Francis Professor in Law** and Associate Dean for Academic Affairs at the University of Texas School of Law. He also serves as the Director of UT-Austin's interdisciplinary research center the Robert S. Strauss Center for International Security and Law. His scholarship encompasses a wide range of issues relating to national security and the law, including detention, targeting, prosecution, covert action, and the state secrets privilege; most of it is posted here. Along with Ben Wittes and Jack Goldsmith, he is one of the co-founders of the blog.

Lettura interessante

FONTE: https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom

▲ Nikita Kuzmin a bordo della sua BMW Serie 6 cabriolet

FONTE: https://www.repubblica.it/esteri/2021/09/09/news/cybercrime_malware_e_i_reati_informatici_di_nikita_kuzman_il_mondo_di_gozi-316873694/



Crearsi una rete in rete

Trovare informazioni

Cosa gestiscono i sistemi aziendali?

LA COMPRENSIONE DELL'AZIENDA E DEI SUOI SISTEMI È FONDAMENTALE PER OGNI ANALISI DEL RISCHIO IT

(...E QUINDI SEGUE UNA LORO DESCRIZIONE APPROSSIMATIVA)

Com’è fatta un’azienda e i suoi sistemi informativi

Icone di Alexandra Olawolska http://handdrawing.olawolska.com/

Sistemi per la gestione dei fornitori

- L'ufficio acquisti tratta con i fornitori («vendor»), dopo aver raccolto le esigenze interne, ordinando i materiali necessari. In inglese «purchasing». Vi lavorano i compratori / addetti dell'ufficio acquisti («buyer»).
- I materiali possono essere diretti (direttamente necessari alla produzione) oppure indiretti (tutto il resto, come le penne e l'automobile del presidente)
- I documenti principali sono l'ordine («purchase order»), la richiesta d'acquisto RDA («requisition») che serve internamente per raccogliere le esigenze, la richiesta d'offerta RDO che viene mandata a diversi fornitori per chiedere informazioni su prezzi e condizioni (RFP «request for proposal»; «request for information» RFI). In alcune situazioni, soprattutto nella pubblica amministrazione al di sopra di certi importi, si indicono delle gare tra fornitori («tender») più o meno formali a valle della preparazione del materiale di gara.
- Gli ordini possono essere chiusi («normali») oppure aperti («blanket order» cioè da fare man mano che serve il materiale) e possono avere più articoli, consegne differenziate in luogo e tempi ecc.
- A fronte di alcune condizioni il fornitore emette fattura (elettronica) e questa viene pagata (dall'amministrazione; non dall'ufficio acquisti) se il materiale soddisfa certi requisiti di quantità e qualità (che sono verificati al ricevimento e dall'utilizzatore).
- I dati principali riguardano: le persone giuridiche (fornitori), i prezzi dei materiali e le condizioni di fornitura.

Sistemi per la gestione della produzione

- I sistemi per la gestione della produzione differiscono moltissimo a seconda del prodotto da produrre e delle scelte dell'azienda. Hanno lo scopo di rendere disponibili le giuste quantità di prodotto (non di meno e non di più) della qualità richiesta, producendo nel minor tempo possibile e usando nella maniera più efficiente possibile le risorse,

Figura 1.1: Classificazione dei sistemi di produzione.

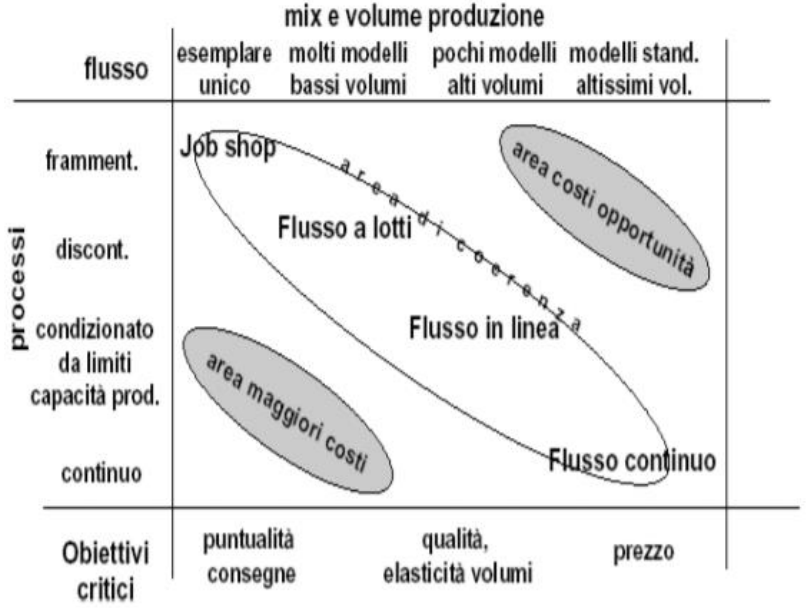


Figura 1.3: Matrice prodotto - processo.

FONTE: https://didattica-2000.archived.uniroma2.it/MSP/deposito/MSP_versione_2.pdf

Sistemi per la gestione dei clienti

- Il cliente è la chiave del successo dell'azienda. Si dice B2B (business to business) un'azienda i cui clienti siano a loro volta delle aziende e B2C (business to consumer) quella i cui clienti sono dei consumatori finali. I clienti sono gestiti dall'ufficio commerciale.
- L'organizzazione commerciale risente di questa caratterizzazione e delle scelte dell'azienda. La guida il direttore commerciale. Possono essere presenti dei commerciali, degli agenti, dei rappresentanti, dei distributori. La retribuzione di questi soggetti è fortemente legata agli obiettivi di vendita (accordi contrattuali, provvigioni e «compensation plan»).
- Se i prodotti da vendere sono sofisticati si affianca spesso una forza di prevendita (assistenza alla vendita) e/o una di post vendita (assistenza all'uso) eventualmente coadiuvata da una rete di partner (aziende terze che intervengono a monte e/o a valle della vendita).
- Il sistema informatico principe è il CRM (customer relationship management) che gestisce i contatti (persone che appartengono all'organizzazione del cliente), le trattative secondo il loro stato di avanzamento e gli ordini. Inoltre, una serie di elementi e indicatori che tendono a prevedere come stanno andando le vendite.
- I dati principali riguardano: le persone giuridiche per il B2B, le persone fisiche che vi lavorano, le persone fisiche per il B2C (consumatori finali), la situazione del venduto (complessivo e analiticamente per ogni cliente), le previsioni di vendita, la situazione provvigionale

Sistemi per la gestione della ricerca e sviluppo

- Le aziende innovano per continuare a stare sul mercato. L'ufficio R&D (research and development) si occupa di questo processo.
- I software utilizzati sono di diverso tipo a seconda del business aziendale e i documenti possono essere disegni in bozza, disegni tecnici molto dettagliati, database di prove, documenti testuali, corrispondenza interna e documenti scambiati con partner e fornitori esterni, modelli in scala e prototipi materiali o immateriali ecc.
- Il lavoro realizzato a volte produce dei brevetti che consentono di ottenere l'esclusività relativamente ad un prodotto o ad un processo innovativo e permettono di sviluppare una posizione dominante sul mercato

Sistemi per il marketing

- Le attività dell'ufficio marketing possono essere molto diverse a seconda dell'azienda (B2B, B2C in primis) e delle scelte aziendali. Possono includere lo studio del mercato di riferimento e l'analisi dell'interazione del mercato con l'azienda per orientare le direzioni di lavoro della ricerca e sviluppo e le politiche dei prezzi dell'ufficio commerciale.
- Inoltre, al marketing viene data la responsabilità di promuovere il brand e la reputazione aziendale organizzando la presenza sui social network e i media (es. con la pubblicità) e altre attività (es. attività benefiche per la comunità e l'ambiente).
- Infine, può essere dato loro l'incarico di preparare brochure di prodotto e organizzare o partecipare a fiere e manifestazioni.
- I dati principali riguardano le analisi di mercato, dati sintetici e proiezioni di vendita e materiali relativi ai prodotti e alle campagne (che sono riservati finché non saranno pubblici).

Sistemi per la gestione delle risorse umane

- L'ufficio delle risorse umane (HR «human resources») (o ufficio del personale) si occupa dell'amministrazione e della gestione del personale attraverso tutte le fasi del rapporto di lavoro (dalla candidatura, all'assunzione, alle dimissioni o pensionamento).
- Si occupa degli stipendi e dei pagamenti ai lavoratori. Spesso approva gli aumenti di stipendio a fronte di un budget di aumenti definito con la direzione generale.
- Lavora in tandem con i manager delle varie linee per comprendere le necessità di nuovo personale («vacancy»), formalizzarle in annunci di lavoro, fare la prima selezione dei candidati e procedere all'assunzione.
- Normalmente verifica anche le esigenze formative e organizza i corsi necessari e quelli obbligatori per legge.
- Organizza i processi annuali di valutazione del personale (competenze, prestazioni, potenziale) per decidere gli aspetti meritocratici e di carriera (carte di successione, alti potenziali ecc.)
- Gestisce le relazioni sindacali e i conflitti interpersonali e tra l'azienda e il lavoratore.
- I dati principali riguardano i dipendenti, retribuzione e valutazioni; tra gli altri, i dati relativi alla salute.

Sistemi per l’amministrazione, finanza e controllo

- L’ufficio AFC ha molti compiti legati agli aspetti economici dell’azienda.
- Tiene la contabilità in partita doppia e redige il bilancio di esercizio composto da conto economico (costi e ricavi), stato patrimoniale (la ricchezza dell’azienda, attivo e passivo) e nota integrativa. Si occupa quindi del reporting di legge e verso la direzione.
- Oltre al reporting di legge provvede alla definizione del budget e della contabilità analitica e si occupa degli aspetti finanziari dell’azienda, come la registrazione delle fatture attive e passive e all’incasso o al pagamento.
- Tiene i rapporti con le banche, controlla i conti, si procura o cede la liquidità e si assicura contro i rischi di cambio se il business è internazionale.

Sistemi per la funzione legale

- Ogni grande azienda ha un ufficio legale e – vista l'ampiezza delle conoscenze richieste – si avvale di ulteriori professionisti specializzati in vari ambiti.
- La funzione legale gestisce il contenzioso di ogni tipo, i contratti particolari, gli obblighi relativi al dlgs. 231/01 (sulla responsabilità amministrativa delle persone giuridiche), a volte quelli al regolamento EU 2016/679 (il famoso GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e le questioni relative alla compagine aziendale (fusioni e acquisizioni, cessioni di ramo d'azienda, brevetti ecc.)
- Le informazioni che tratta in maniera digitale sono normalmente dei documenti di testo.

RID aka CIA

https://standards.iso.org/ittf/PubliclyAvailableStandards/ https://iso27001security.com/index.html

DEFINIZIONE

Confidentiality (Riservatezza)

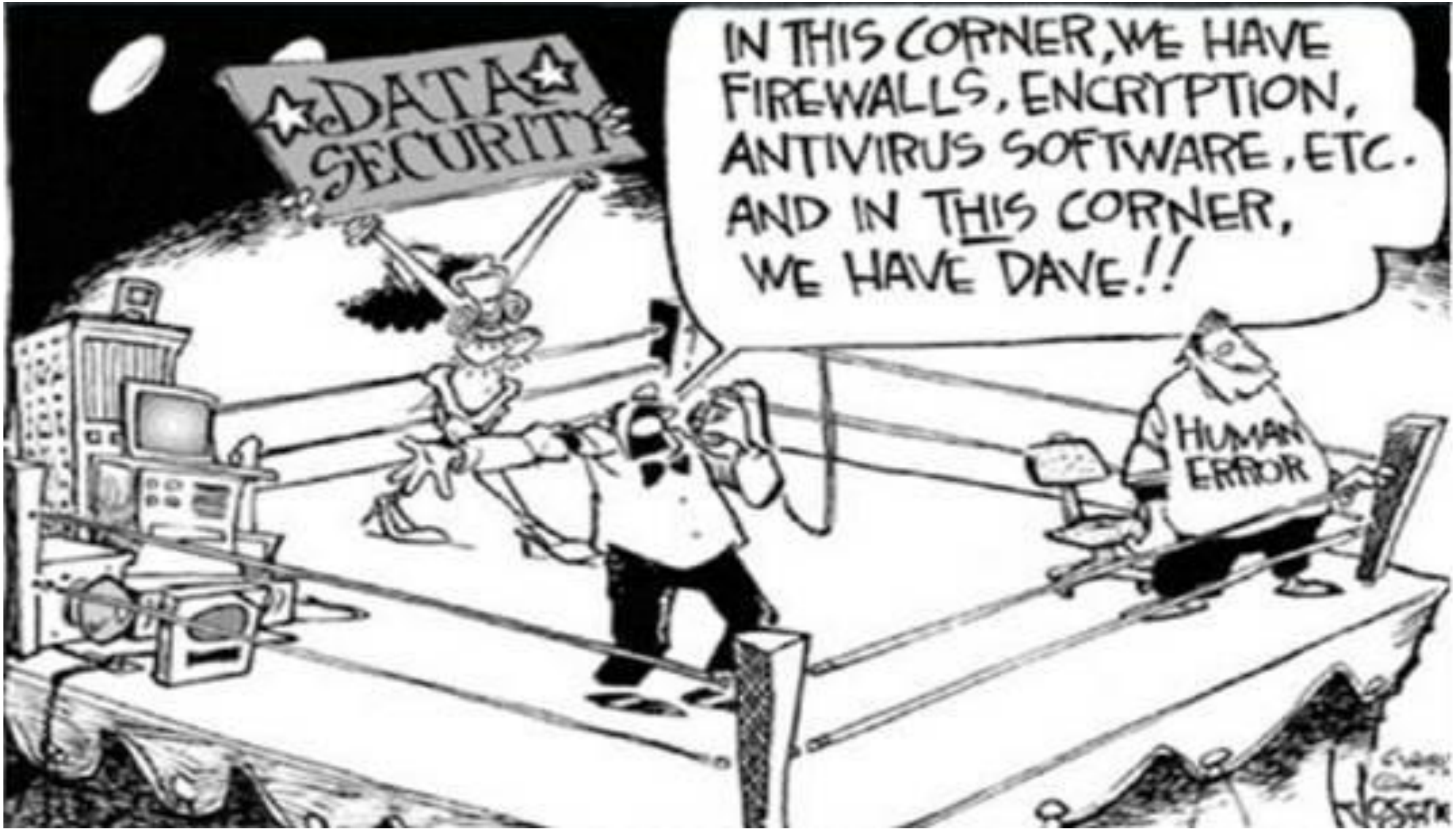
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity (Integrità)

property of accuracy and completeness

Availability (Disponibilità)

property of being accessible and usable on demand by an authorized entity


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

FIGURE

FONTE: Dukece.com https://www.dukece.com/wp-content/uploads/2018/09/Figure-2.png

THE COMPLEXITY CHASM

Cos’è il rischio?

DEFINIZIONE

Risk (ISO 31000:2018)

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

Obiettivi

Gli obiettivi sono di molti diversi tipi e possono riguardare:

- L'organizzazione nel suo complesso e ad alto livello oppure una parte dell'organizzazione a livelli più operativi. Si parla quindi di obiettivi strategici, tattici ecc.
- Aspetti economici e finanziari (obiettivi di fatturato, margine, giacenza di cassa, investimenti ecc.)
- Aspetti non economici e finanziari come, per esempio, la protezione dell'ambiente, la salute e sicurezza dei dipendenti, la felicità della comunità di riferimento

Possono essere espressi in modi diversi e con parole diverse (obiettivo, target, goal ecc.) in maniera formale (scritta) oppure impliciti. Inoltre, sono spesso correlati tra di loro e si influenzano a vicenda.

Incertezza

Rappresenta il deficit che abbiamo della conoscenza del mondo, degli eventi, delle loro probabilità e conseguenze.

Non sappiamo chi vincerà le elezioni, come fluttuerà il tasso di cambio, se mi ammalerò di influenza, se viene 7 dalla somma del lancio di due dadi, se il nuovo guardiano si addormenterà durante il turno notturno, se degli hacker prenderanno di mira la nostra Università…

Effetto dell’incertezza

Corrisponde a mancare l’obiettivo di un piccolo o grande margine.

Nota: Anche se è controintuitivo vedere realizzati dei rischi che producono effetti positivi, la disciplina generale del risk management e la ISO 31000 lo prevedono.

DEFINIZIONE

Risk (ISO/IEC 27000:2018)

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009, 3.5.1.3) and “consequences” (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Risk (effect of uncertainty on objectives)

ISO 31000:2018

[…]

Note 3 to entry: Risk is usually expressed in terms of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

«Risk source» non è definito nella 27000

Nella 27000 troviamo spesso al suo posto «threat» (minaccia) perché, contrariamente alla 31000, il rischio, nell'Information Security, è spesso considerato negativo.

ISO/IEC 27000:2018

[…]

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

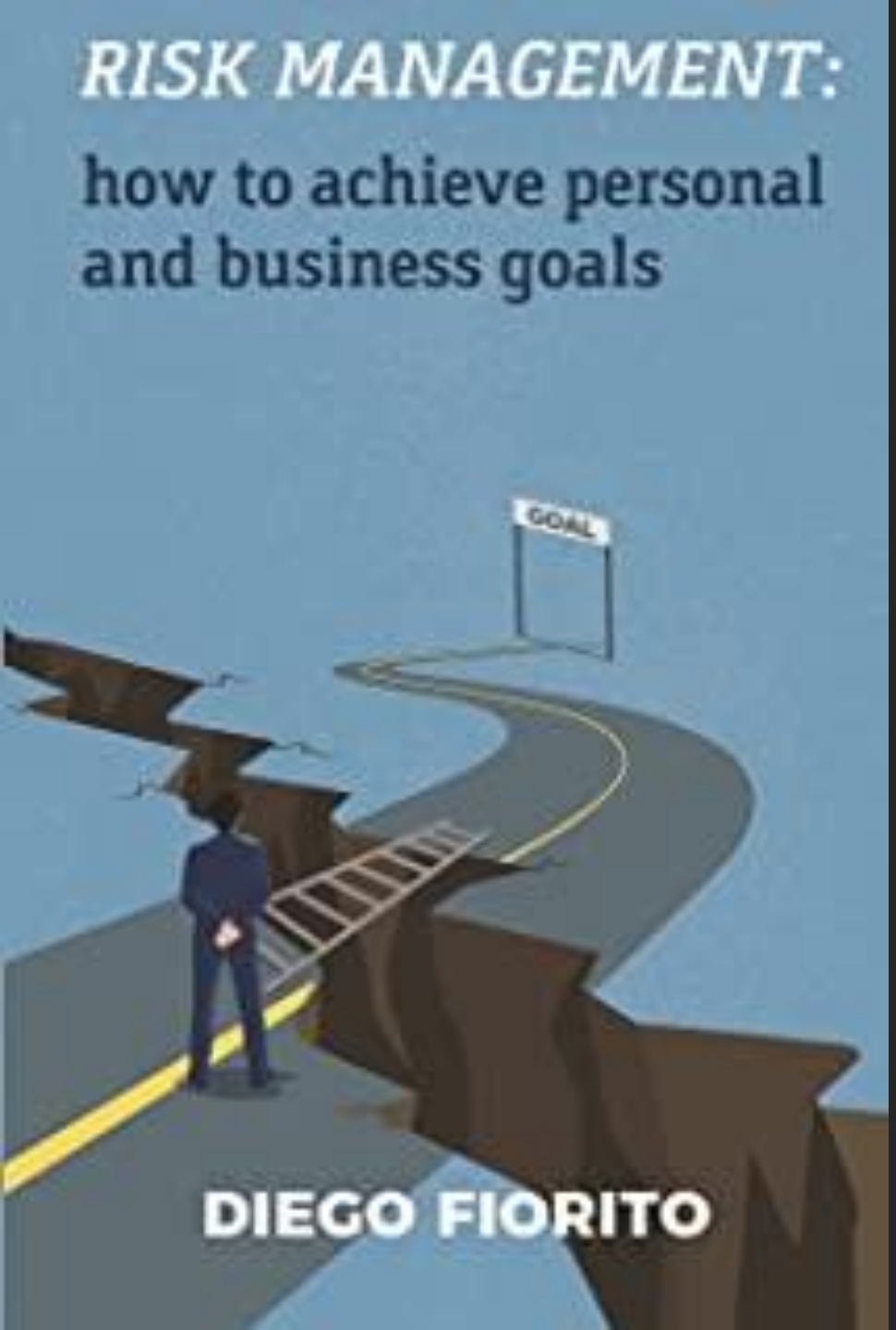
Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Alcuni rischi

Rischio di contagio di coronavirus: finché non sarò contagiato è molto improbabile che abbia un'infezione. Se rimango chiuso in casa probabilmente non mi contagerò

Rischio di credito: la probabilità di non ricevere indietro i soldi dati a prestito dipende da molti fattori tra i quali la capacità del debitore e le garanzie fornite

Rischio di perdita di un asset: se posseggo un bene c'è sempre la possibilità di perderlo, che me lo rubino, che si rompa per l'uso o si distrugga per certi eventi (incendio)

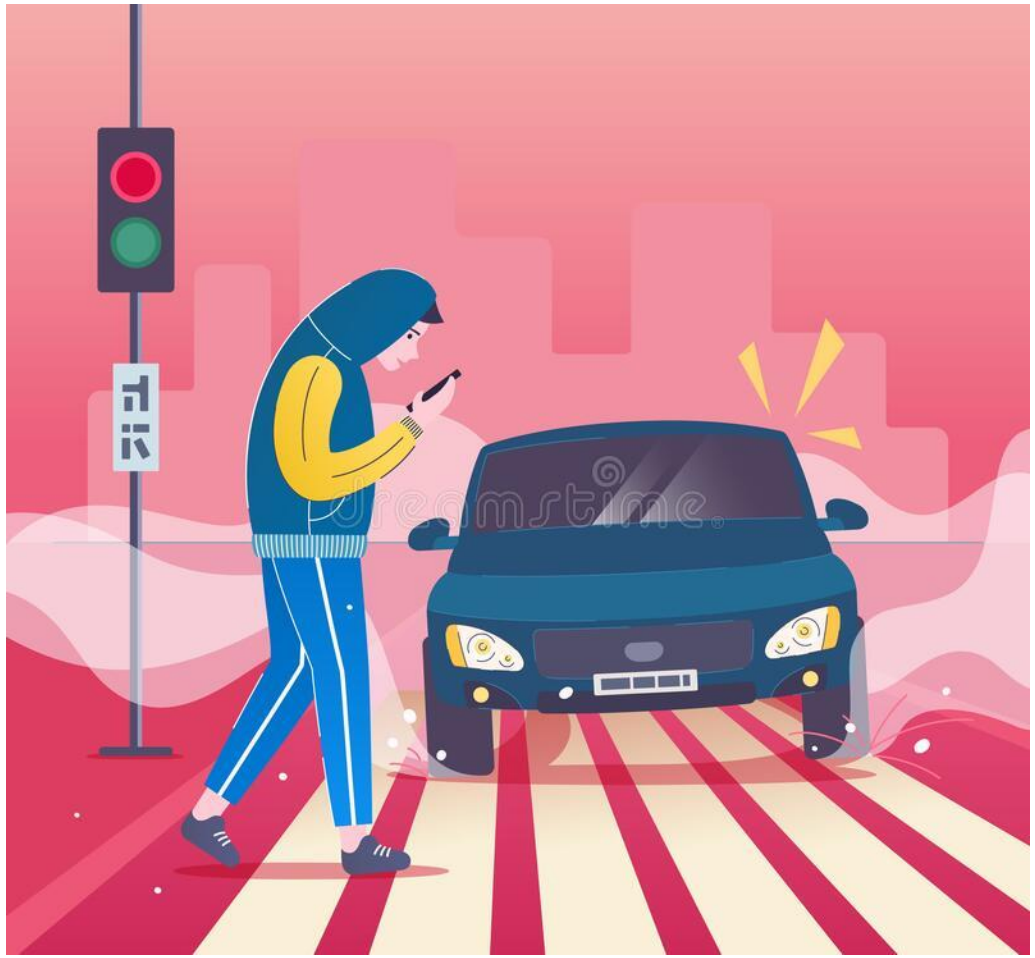


Uniformare la scrittura dei rischi

As a result of <defined cause / causes>,

<this unexpected event> could occur,

which could produce <this effect on targets>



	Pedestrian crossing the road being distracted
1. As a result of <defined cause / causes>,	Come risultato di attraversare la strada guardando il cellulare
2. <this unexpected event> could occur,	Un’automobile potrebbe investirmi
3. which could produce <this effect on targets>	e causarmi morte o ferite e conseguenti costi medici

Fonte dell’immagine:
https://www.dreamstime.com/search.php?securitycheck=3592561f791a84f63f3595d615730338&firstvalue=&lastsearchvalue=&srh_field=pedestrian+accident+vector+illustration+man+smartphone+crosswalk+danger+road+careless+young+dangerous+way+safety+internet+image11892738&s_ph=y&s_il=y&s_video=y&s_audio=y

Risk Management (ISO Guide 73:2009, “Risk management – Vocabulary, ISO 31000:2018 and ISO/IEC 27000:2018)

coordinated activities to direct and control an organization with regard to risk

DEFINIZIONE

DEFINIZIONE

Risk Management Process (ISO Guide 73:2009, "Risk management – Vocabulary, and ISO/IEC 27000:2018)

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk

5 results for risk management process

Orientation: ALL LANGUAGES View: FULL ENTRY GROUPED Results per page: 300

Sort by: RELEVANCE TERM

× Terms & Definitions

Terms & Definitions

risk management process

systematic application

establishing the contex

Note 1 to entry: The pro

ISO 13131:2021(en), 3.

Available in: EN

Un tool utile:
https://www.iso.org/obp/ui#search

Terms & Definitions

risk management process

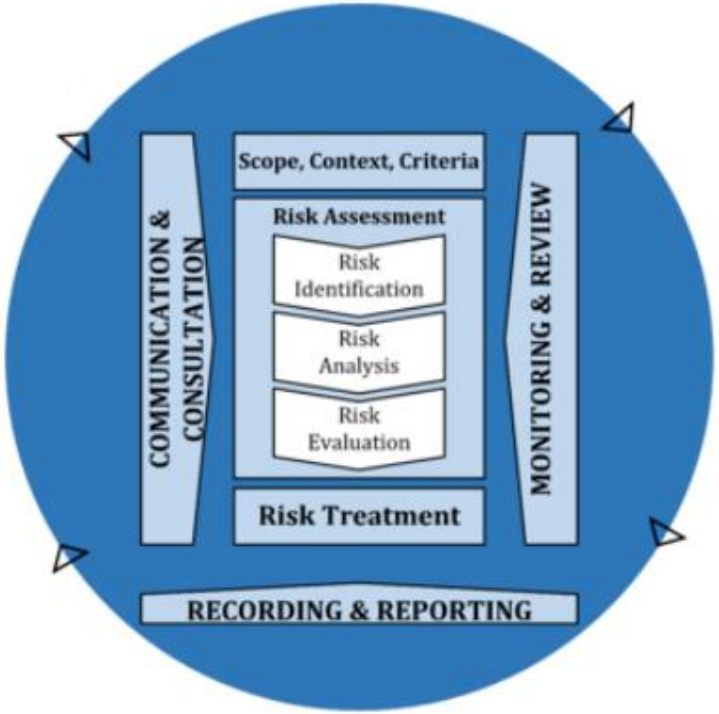
systematic application of management **policies** (3.53), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing **risk** (3.61)

Note 1 to entry: ISO/IEC 27005 uses the term "*process*" (3.54) to describe risk management overall. The elements within the **risk management** (3.69) process are referred to as "activities".

[SOURCE: ISO Guide 73:2009, 3.1, modified — Note 1 to entry has been added.]

Perché il termine Risk Management Process
(che è definito nella ISO/IEC 27000:2018)
non è definito nella ISO 31000:2018?

Risk Management Process as ISO 31000:2018



Process (clause 6)

Classificazione secondo impatto

- Strategic
- Operational (processes and procedures)
- Projects
- Products

Rischi strategici

Sono legati agli aspetti strategici dell'azienda come mission, vision e obiettivi aziendali

(qui si trovano esempi di vision e mission: https://www.clearvoice.com/blog/difference-between-mission-vision-statement-examples/)

Sono di altissimo livello e quindi comprensibili anche dal «pubblico» (stakeholder esterni)

Rischi strategici di Coca Cola Femsa (Mexico) nel 2020

Tabella derivata dal libro Risk management: how to achieve personal and business goals (Diego Fiorito) – la fonte originale non è disponibile

Risk	Description	Impact
Strategic relationship	Loss of the strategic relationship with the distributors	Economic and reputational losses
Demand	Change in consumer preferences	Reduction in demand. Lower income
Patents	Patent violation	Damage to company's brand and reputation
Competition	Aggressive position from the competition	Loss of income, profit or business
Cyber risk	Loss of service or loss of information	Loss of information. Impact on brand reputation
Economic, politic or social conditions	Changes in countries where the company operates	Loss of income. Lower demand. Lower prices. Decrease in profitability
Regulations	New taxes or regulations	Increase in costs. Restrictions. Lower income.
Legal	Adverse results of legal proceedings	Financial impact. Investigations related to taxes, consumer protection, environment or work-related issues
Acquisitions	Little or low ability to integrate acquisitions or fewer synergies than expected	Liabilities. Higher costs
FX (foreign exchange)	FX movement and volatility	Lower profitability due to devaluation of local currencies. Increase of low material (prices). Lower profitability
Climate change	Unfavorable climate conditions	Loss of operations. Lower sales
Social media	Negative or inaccurate information about the company in the media	Reputational impact
Water	Lack of water	Reduced production
Raw materials	Increase in price or lower availability	Higher costs. Difficulties in production. Reduced profitability

Rischi relativi a processi e procedure

(operational)

Sono legati agli aspetti di processo e procedurali dell'azienda

Per essere identificati e compresi richiedono la conoscenza di dettaglio dei processi e/o procedure

DEFINIZIONE

Process (ISO 9000:2015)

set of interrelated or interacting activities that use inputs to deliver an intended result

Note 1 to entry: Whether the “intended result” of a process is called output (3.7.5), product (3.7.6) or service (3.7.7) depends on the context of the reference.

Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes.

Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process.

Note 4 to entry: Processes in an organization (3.2.1) are generally planned and carried out under controlled conditions to add value.

Note 5 to entry: A process where the conformity (3.6.11) of the resulting output cannot be readily or economically validated is frequently referred to as a “special process”.

Note 6 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified to prevent circularity between process and output, and Notes 1 to 5 to entry have been added.

DEFINIZIONE

Procedure (ISO 9000:2015)

specified way to carry out an activity or a process

Note 1 to entry: Procedures can be documented or not.

The difference between process and procedure is that processes are general activities to achieve a goal and procedures are specific steps that must be followed to complete a task.

Risks of «opening of bank accounts»

Due to weaknesses in the design and / or execution of the controls, an error could be generated in the request for transfer of resources (account, amount, bank, etc.), incurring economic losses for the organization.

Due to weakness in the controls or non-application of the controls, or ignorance of the procedures, accounts could be opened in the name of the organization improperly (eg, unauthorized personnel), incurring economic losses.

Due to the lack of a bank analysis or due diligence, an account may be opened at an institution that has high credit risks or financial risks, which could create greater credit exposure and / or image effects for the organization.

Due to the lack of controls or criteria, many accounts could be created (which could not be used), which lead to operational risks and costs associated with their administration.

Due to the absence of personnel, or personnel without specific experience or knowledge in the activities of the process, etc., the procedure could not be executed, affecting the normal flow of operations (partial or total) of the organization.

Due to external events, etc., the procedure could not be executed (unavailability of personal, systems, etc.), affecting the normal flow of operations (partial or total) of the organization.

Rischi relativi ai progetti

Sono relativi ai progetti di ogni tipo, inclusi i progetti di realizzazione / integrazione di software

Per essere identificati e compresi richiedono la conoscenza del progetto, ma alcune caratteristiche sono comuni

Project (ISO 21502:2020 (and PMBOK – Project Management Institute))

temporary endeavour to achieve one or more defined objectives

DEFINIZIONE

I progetti

- Hanno un obiettivo specifico da raggiungere
- Sono limitati nel tempo ed hanno una data di inizio e una di fine
- Utilizzano risorse (umane, economiche, materiali, equipaggiamento)
- Hanno un budget e limitazioni di spesa

Li gestisce un project manager che deve equilibrare i costi, i tempi e l’ambito (scope)

Rischi di prodotto

Sono legati alla progettazione, produzione, commercializzazione e manutenzione di prodotti materiali o immateriali

L’enfasi è sulla realizzazione di qualcosa che verrà prodotto in grandi quantità

Risk management di prodotto

Nella fase di design, il risk management deve focalizzarsi sui difetti del processo di produzione e del prodotto in grandi quantità.

Se coinvolti dei fornitori esterni (molto probabile) si devono identificare eventuali criticità (variazioni della qualità attesa, variazioni dei prezzi e delle disponibilità, ritardi di approvvigionamento, fallimento del fornitore, prodotti / fornitori alternativi).

Si devono raccogliere e utilizzare i feedback del mercato per controllare e modificare il processo di produzione (difetti) e le strategie commerciali (prezzi, sconti, bundle ecc.)

Una possibile classificazione dei rischi

- Rischio di credito
- Rischio di mercato
- Rischio operativo
- Rischio relativo alle risorse umane
- Rischio IT e cyber security
- Rischio legale
- Rischio di compliance
- Rischio di crimine finanziario
- Rischio ambientali
- Rischio sociale
- Rischio di salute e sicurezza sul lavoro