Gestione dei rischi informatici nella professione di Ingegnere

Ing. Mattia Siciliano

28 Luglio 2020

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

ORDINE INGEGNERI NAPOLI

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Commissione CyberSecurity

Agenda

- Che cosa è la Cyber Security
- Lo scenario internazionale
- Perché è importante proteggersi
- Le normative italiane e Internazionali
- Gli oggetti ed i rischi associati
- I 10 elementi e regole che un professionista deve seguire
- Conclusioni

Che cosa è la Cyber Security

La società moderna non po' fare a meno di innovarsi, creando un ecosistema digitale, in cui **l'uomo e le sue informazioni rappresentano il vero valore del prossimo futuro**.

In tale contesto l'espansione di internet produrrà sempre nuovi servizi e benefici per la collettività, ma al tempo stesso aumenterà i *rischi legati alla privacy, alla protezione degli asset nazionale, alla sicurezza delle grandi e delle piccole aziende*.

"The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive,"

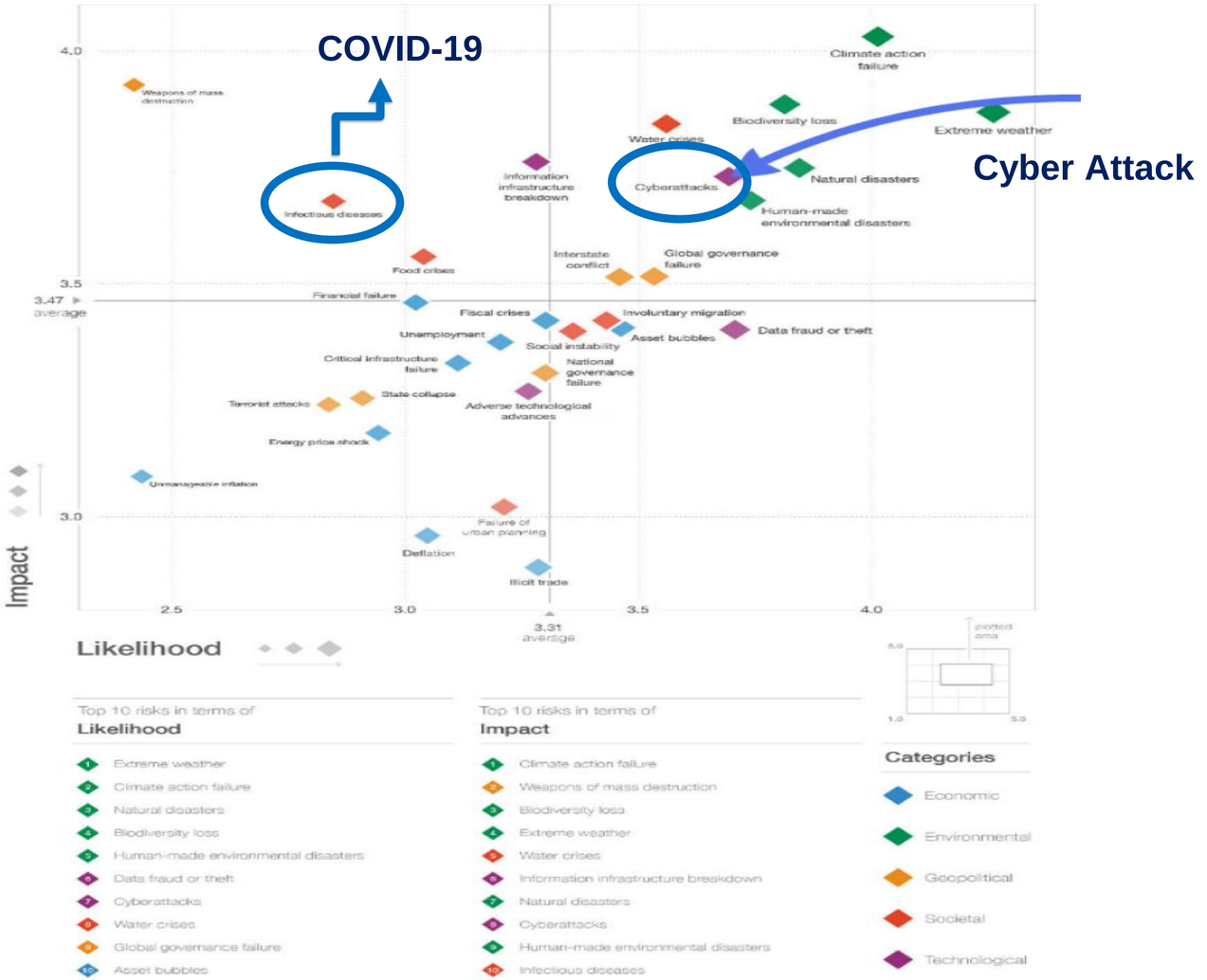
– *Gartner Rethink the Security & Risk Strategy 2019*

Secondo la società d'analisi MarketsandMarkets, l'industria della cyber-security potrebbe salire a oltre 248 miliardi nel 2023. Questo presuppone **un tasso di crescita annuale del 10,2% nei prossimi cinque anni**.

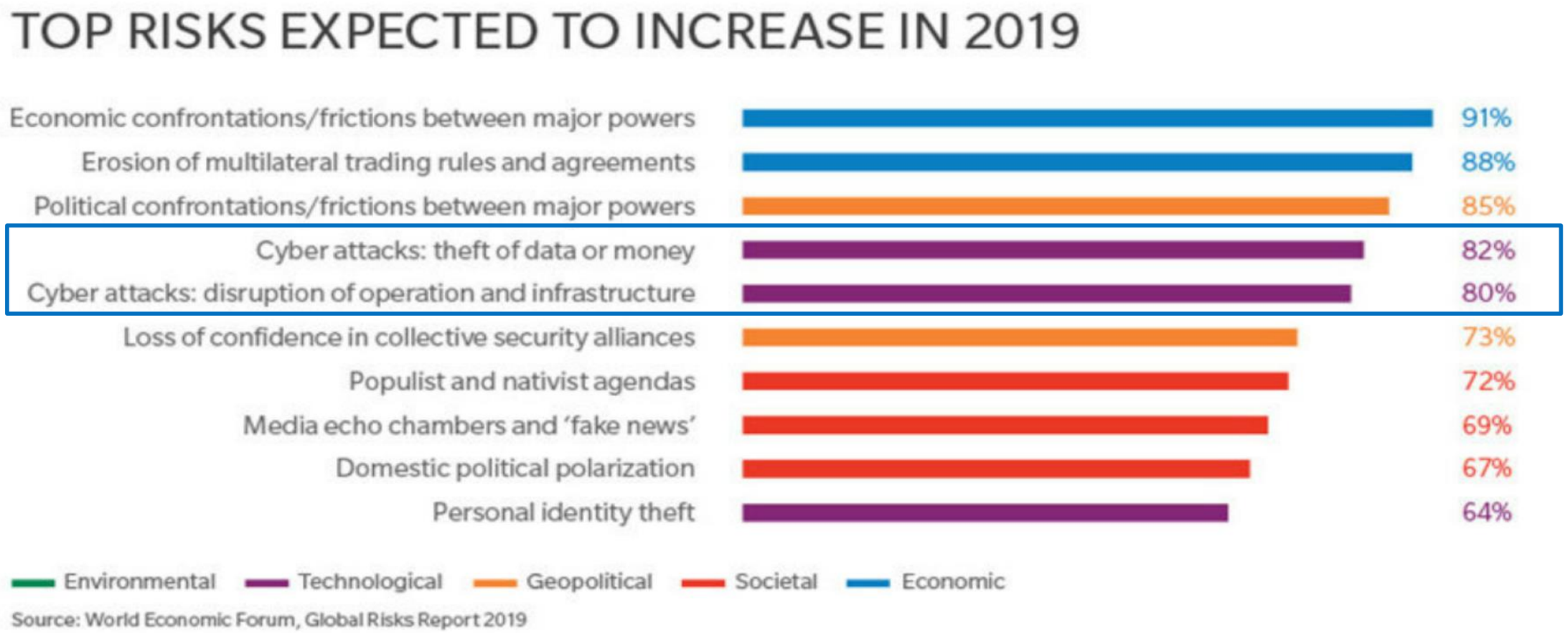
Lo scenario internazionale

Secondo lo studio di ENISA (Agenzia Europea per la Sicurezza Informatica) presentato al WEF – World Economic Forum , la probabilità che si verifichino degli eventi «tecnologici» che possano procurare gravi impatti alla comunità internazionale seguono esclusivamente gli eventi naturali e prima delle pandemie (i.e COVID-19)

Figure II: The Global Risks Landscape 2020



Lo scenario internazionale



Perché è importante proteggersi

Gli attacchi informatici costano 8 milioni di dollari alle aziende in Italia

di Luca Tremolada

2' di lettura

In Italia il costo medio annuo per azienda delle violazioni della sicurezza informatica ha raggiunto gli 8 milioni di dollari (13 milioni di dollari per azienda a livello globale), con un incremento del 19% nel 2018 (12% a livello globale). È quanto emerge dal nono studio annuale di Accenture Security sui costi del cybercrime.

La ricerca, che ha coinvolto 11 Paesi per un totale di 2.647 responsabili security e IT intervistati. Il numero medio annuo di security breach per azienda è aumentato da 50 a 62 (+20% in Italia contro un +11% a livello

MENU | CERCA

la Repubblica

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA ITALIA

Cybersicurezza , il mercato in Italia vale 1,5 miliardi (ma è insufficiente)

Indagine della società di consulenza EY: solo il 45 per cento delle imprese ha investito contro gli attacchi informatici. Nel mondo verranno creati nel settore due milioni di posti lavoro in cinque anni

Le normative italiane e Internazionali

NIS

28 Giugno 2019

The Directive on security of network and information systems

Fornisce misure legali e definisce un quadro di cooperazione per migliorare i livelli di sicurezza degli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).

GDRP

25 Maggio 2018

General Data Protection Regulation

Norma il trattamento dei dati personali delle persone fisiche applicabile a tutte le organizzazioni

AGID

18 Aprile 2017

Misure Minime di sicurezza

Sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni pubbliche

Studi Camera – Istituzioni
Difesa e Sicurezza

D.L. 105/2019: perimetro di sicurezza cibernetica

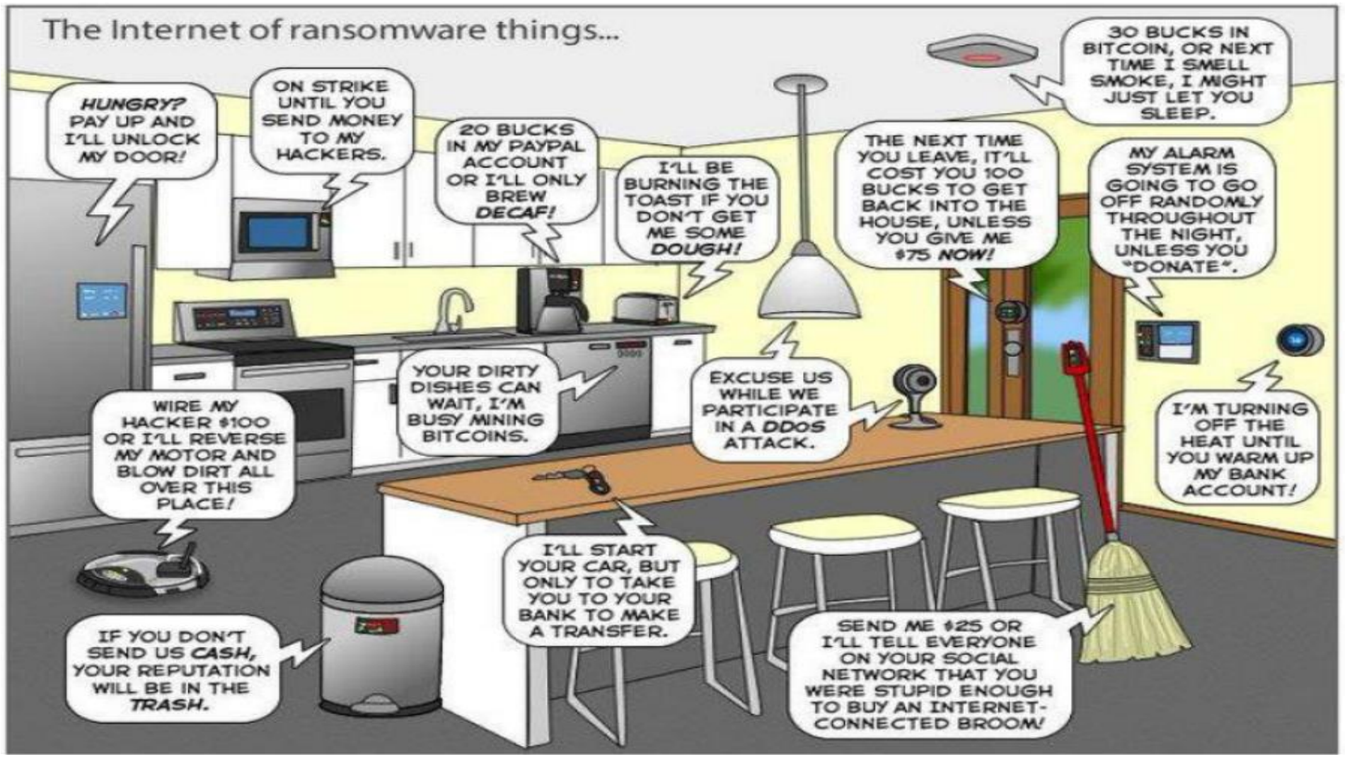
- [ ] Impatto per il Professionista

Gli oggetti ed i rischi associati - 1/2

Internet delle cose (IoT, acronimo dell'inglese Internet of things). Il concetto rappresenta una possibile evoluzione dell'uso della rete internet: gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri

Gli oggetti ed i rischi associati - 2/2

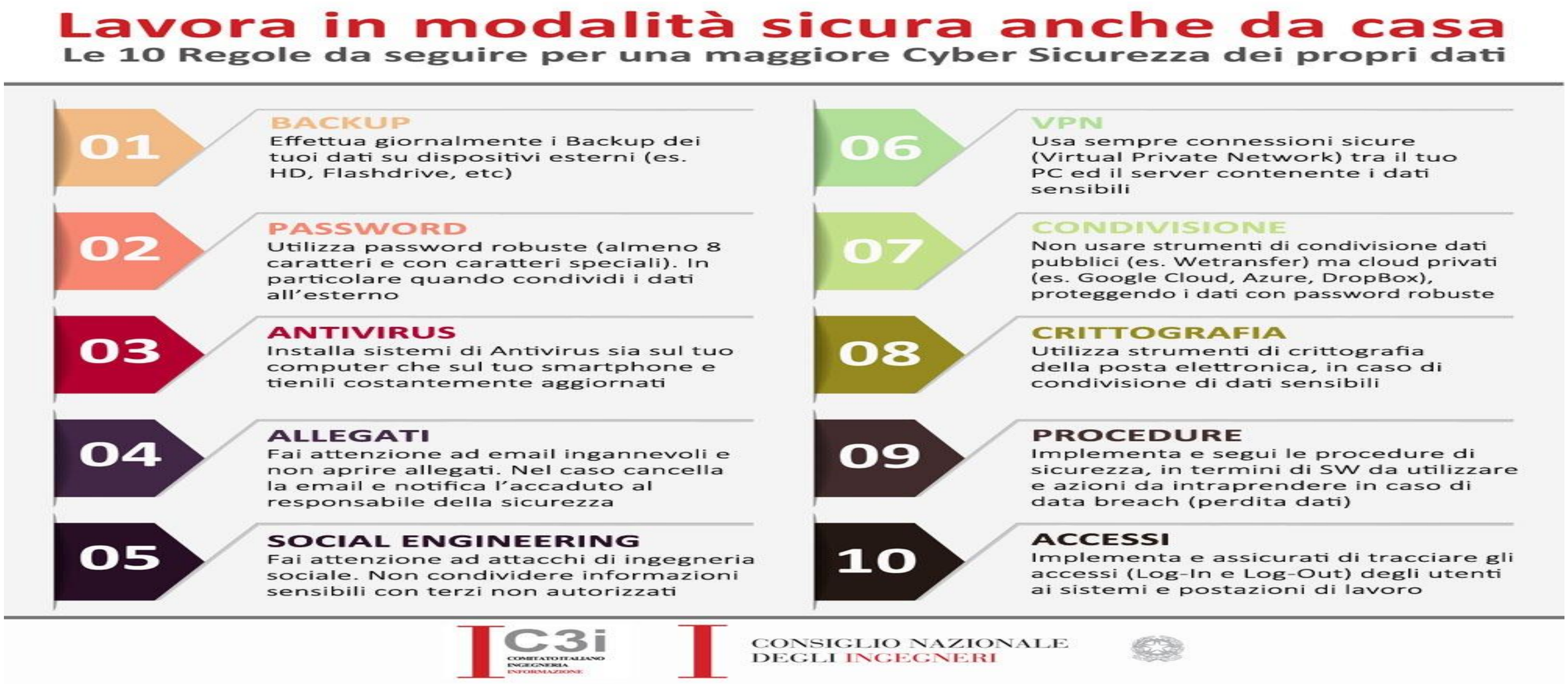
Internet delle cose (IoT) offre molte opportunità in termini di informazioni ma anche molti rischi. In un futuro non molto lontano ci ritroveremo ad affrontare minacce che possono provenire da diversi «attori» , come oggetti presenti in una casa ma anche oggetti impiantati nei nostri corpi



Scenario di CASA

Scenario personale

I 10 elementi e regole che un professionista deve seguire



Backup

01

BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

Va effettuato almeno 1 volta a settimana in maniera incrementale e una volta a mese full. Possibilmente su supporti esterni o cloud

Indica un processo ovvero in particolare la messa in sicurezza delle informazioni di un sistema informatico (o un semplice computer) attraverso la creazione di ridondanza delle informazioni stesse

Rende i dati e le informazioni sempre disponibili in caso di attacco informatico o cancellazione accidentale

Se fatto con continuità il rischio di perdita dei dati è molto basso. L'efficacia in caso di attacco o cancellazione accidentale è molto alta

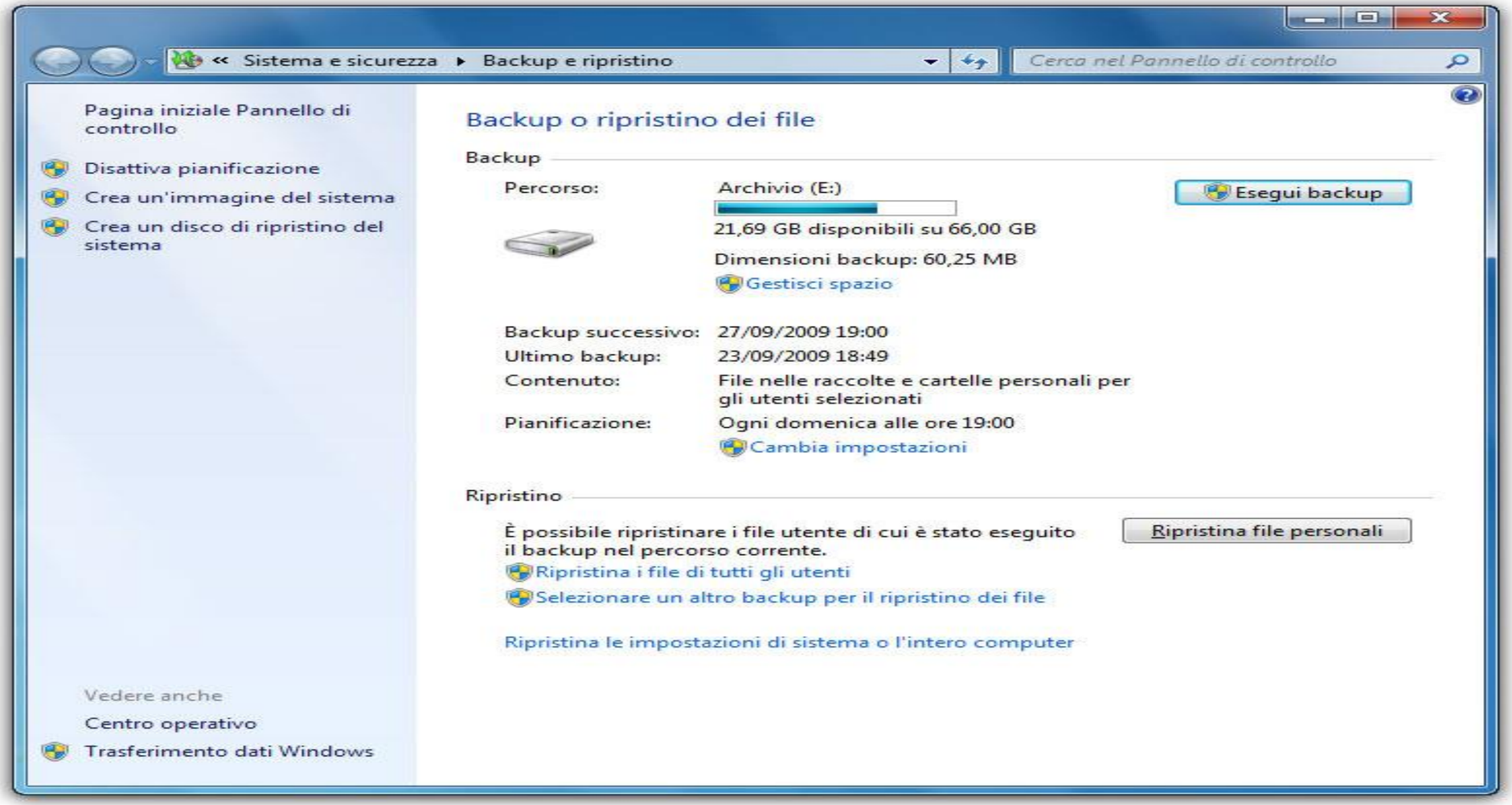
Previene principalmente da minacce di tipo Ransomware (crittografia del proprio PC)

Backup

01

BACKUP

Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)



Password

02 **PASSWORD**
Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

Cambiara la password almeno ogni 90. In alcuni casi prevedere dei sistemi di doppia autenticazione come impronta digitale o 2FA

una sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo a una risorsa informatica

Protegge l'accesso al PC o alle vostre aree riservate da parte di soggetti terzi

Se correttamente creata previene minacce di phishing, brute force, identity theft

Il rischio associato è molto alto, in caso non sia configurata correttamente. Deve avere almeno una lunghezza di 8 caratteri alfanumerica e con caratteri speciali (i.e. $,@, etc). Meglio ancora se sono delle frasi

AntiVirus

03 ANTIVIRUS
Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

Va aggiornato almeno ogni settimana. Meglio ancora se unito con un sistema di Firewall dello studio o con un contratto di prevenzione con l'operatore telefonico

è un software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware per un computer

Serve a proteggersi da Virus esterni in grado di accedere a dati e informazioni sensibili

Il software va sempre aggiornato. Nel caso non lo fosse il rischio di accesso da parte di un virus è molto elevato cosi come la perdita dei dati

Previene diverse minacce come : virus, adware, backdoor, keylogger, spyware, trojan, worm o ransomware

Allegati

04 ALLEGATI
Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

Generalmente è consigliabile fare analizzare gli allegati all'antivirus prima di aprirlo. Nei casi più complessi si possono usare delle Sandbox cosi da comprenderne il rischio

è un file di un computer che viene inviato assieme a un messaggio di posta elettronica

Il generale sono utilizzati per lo scambio della informazioni, ma in alcuni casi possono nascondere dei codici malevoli

Le principali minacce sono il Phishing, ransomware o spyware, trojan (nascoso nel codice dell'allegato)

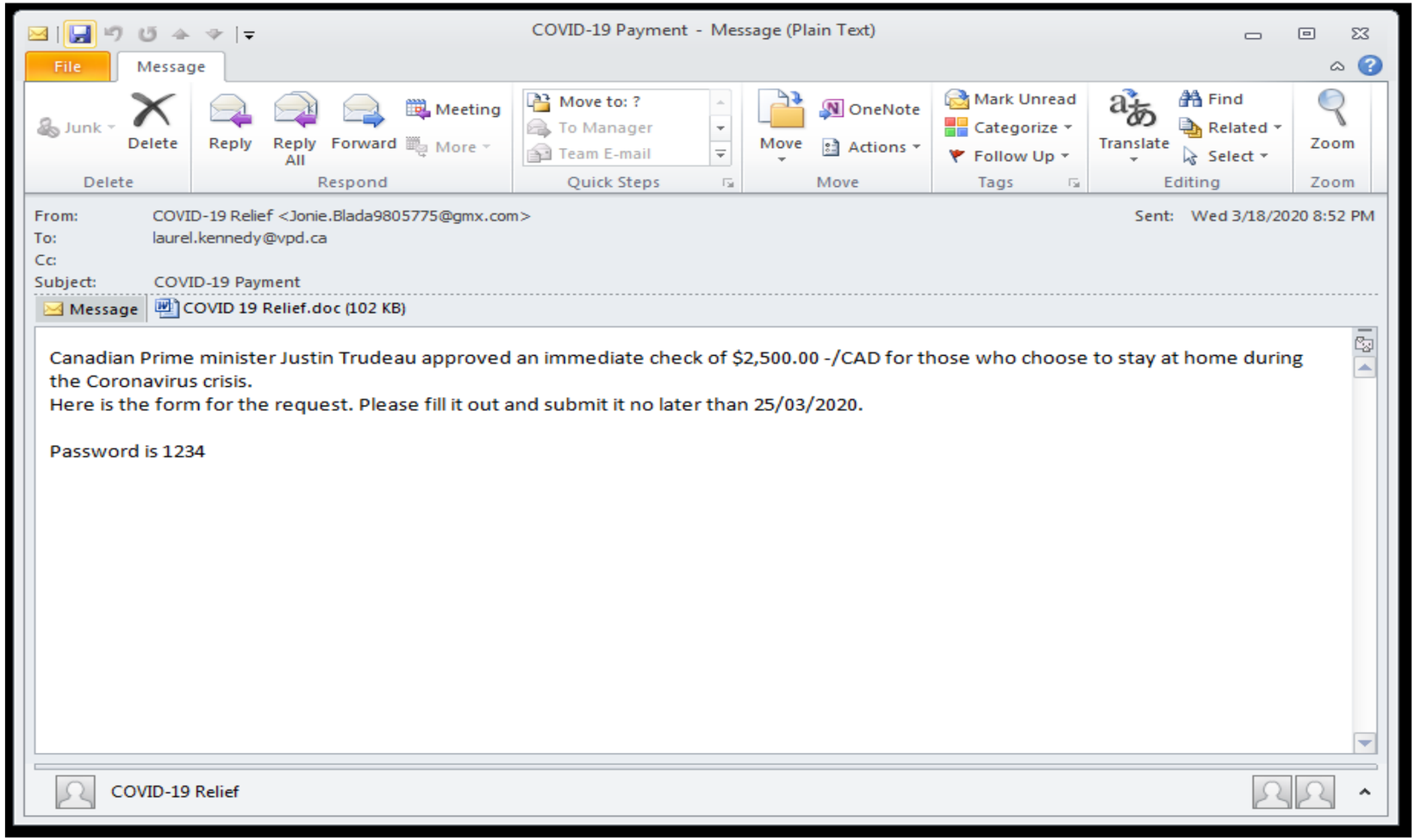
Il rischio associato è molto elevato. Pertanto si consiglia di fare molta attenzione al tipo di file, all'estensione anomale (ie. Se non è Doc, docx, pdf, etc) e al creatore/mittente

Allegati

04

ALLEGATI

Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza



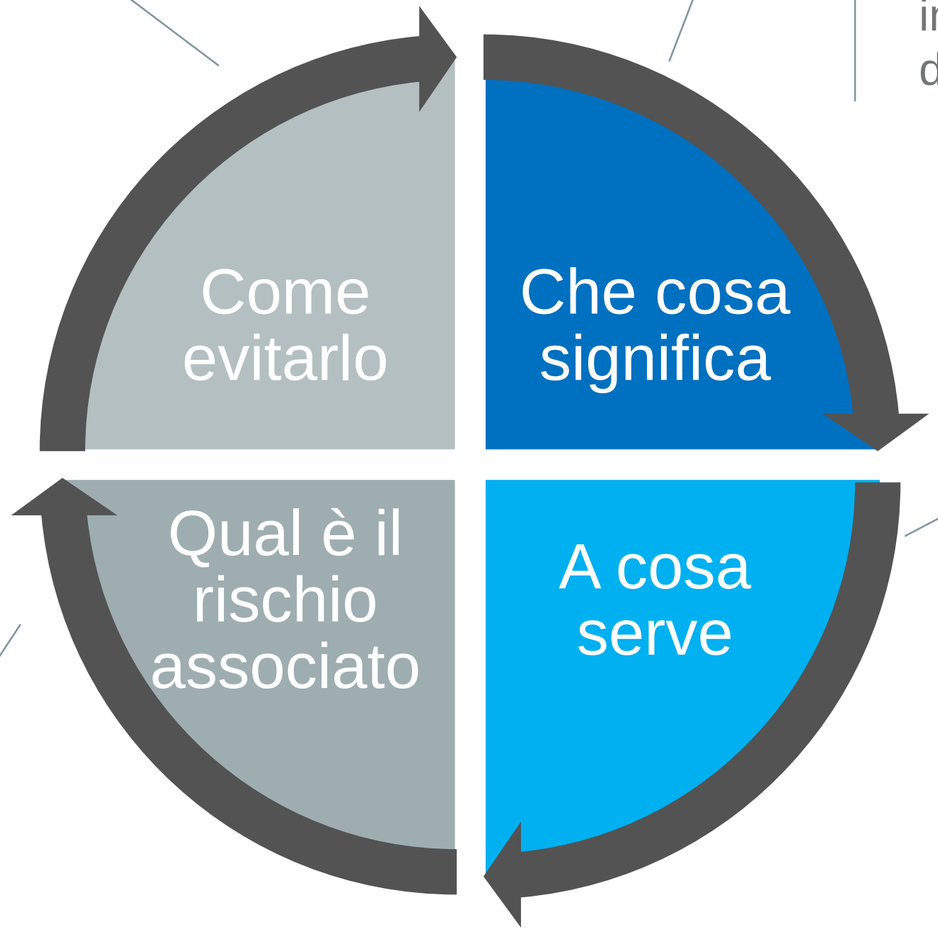
Social Engineering

05

SOCIAL ENGINEERING
Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

Prendere tempo, fare molte domande al richiedente sulla sua identità e non divulgare informazioni sensibili. In casi eclatanti fare denuncia alla Polizia Postale

è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili



Viene usato dai criminali informatici per carpire informazioni con la finalità di frode o ricatto

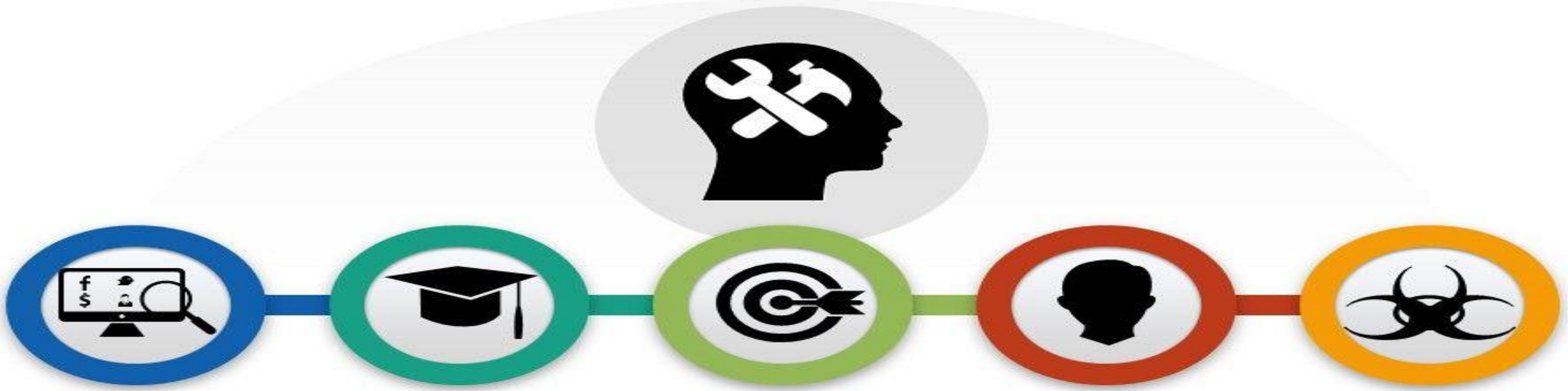
Il rischio di condividere informazioni sensibili è molto altro. Fare molta attenzione alle richieste e al mittente per evitare di essere ingannati

Social Engineering

05

SOCIAL ENGINEERING
Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

Social Engineering With Five Steps Include Data...



Data Collection

This slide is 100% editable. *Adapt it to your needs and capture your audience's attention.*

Extract, Transform, And Load; Feature Selection; And Generation

This slide is 100% editable. *Adapt it to your needs and capture your audience's attention.*

Target Acquisition

This slide is 100% editable. *Adapt it to your needs and capture your audience's attention.*

Initial Contact

This slide is 100% editable. *Adapt it to your needs and capture your audience's attention.*

Attack

This slide is 100% editable. *Adapt it to your needs and capture your audience's attention.*

VPN

06 **VPN**
Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili

Va utilizzata principalmente quando si lavora in modalità smartworking o si vuole accedere al proprio Server in modalità sicura

E’ una tecnologia che permette di collegare due punti/postazioni in maniera sicura

Rende la comunicazione tra due punti (ie. PC dello studio e PC di casa) sicura e crittografata evitando l’accesso a terzi

Previene l’accesso di terzi e di malware (se entrambi i punti sono protetti)

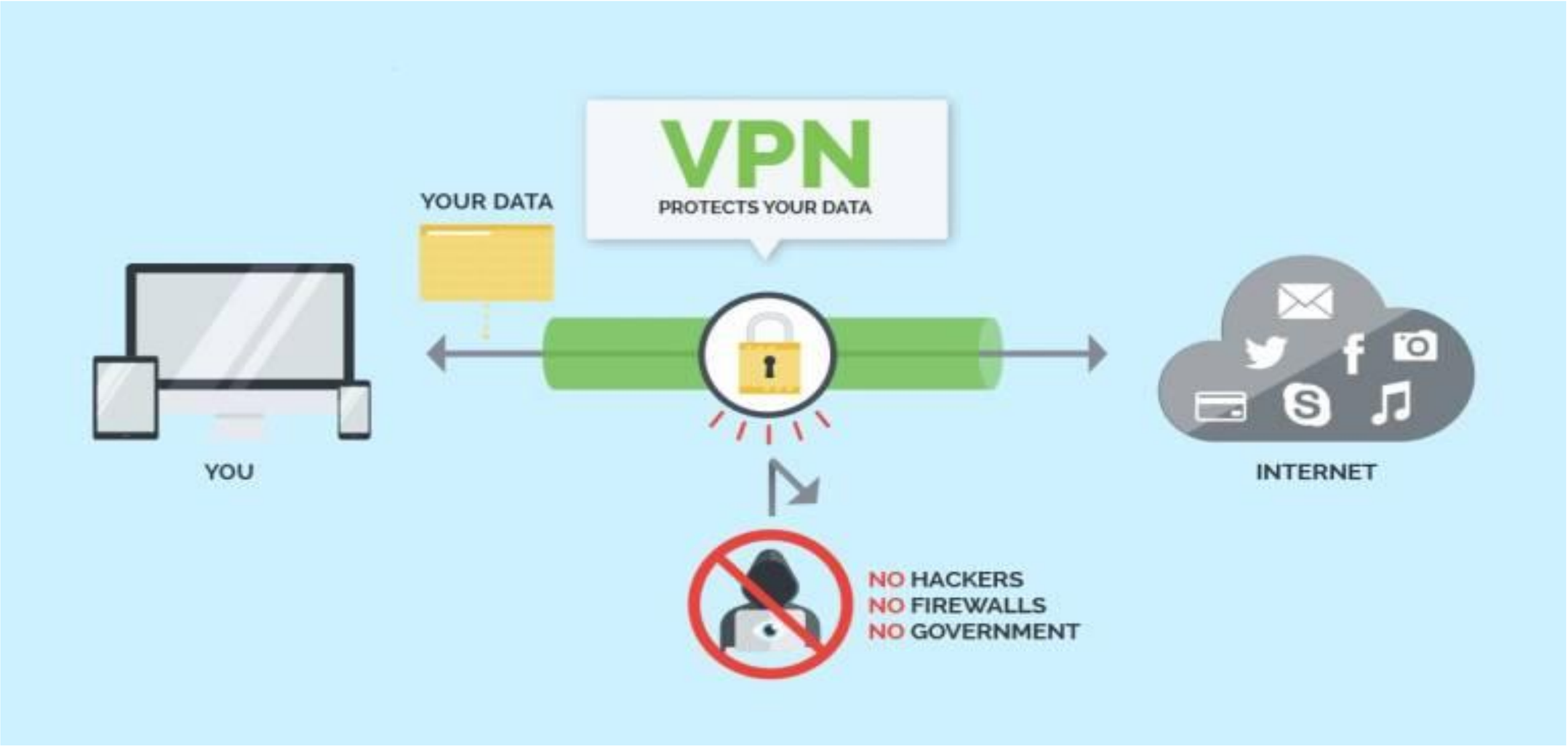
L’utilizzo di questa tecnologia abbatte notevolmente il rischio di un attacco e rende il lavoro in modalità smartworking ancora più sicuro

VPN

06

VPN

Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili



Condivisione

07 CONDIVISIONE
Non usare strumenti di condivisione dati pubblici (es. Wetransfer) ma cloud privati (es. Google Cloud, Azure, DropBox), proteggendo i dati con password robuste

Nel caso di condivisione di file nel cloud è sempre buona norma proteggerli con una password (ie ZIP file) o se possibile crittografarli

E’ un tecnica usata principalmente per lo scambio di file di grandi dimensioni

Scambiare file di grandi dimensioni (ie video, foto, CAD, etc) attraverso canali non convenzionali come la posta elettronica

La condivisione sicura su cloud privati (ie . Google, Azure, Dropbox, etc), previene la minaccia di accesso da parte di terzi in caso di data breach

Il sistemi non convezionali come WeTrasfer conservano i dati su server pubblici esposti a minacce sul web senza specifici apparti ti protezione, pertanto il rischio di accesso a dati riservati o progetti è alto. L’uso di cloud privati garantisce da parte dell’operatore un livello minimo di sicurezza perimetrale

Crittografia

08 CRITTOGRAFIA
Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili

Quando si vuole condividere un informazioni altamente sensibile (ie. un progetto di un cliente). In questo caso usare almeno una crittografia a 128 bit

metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo

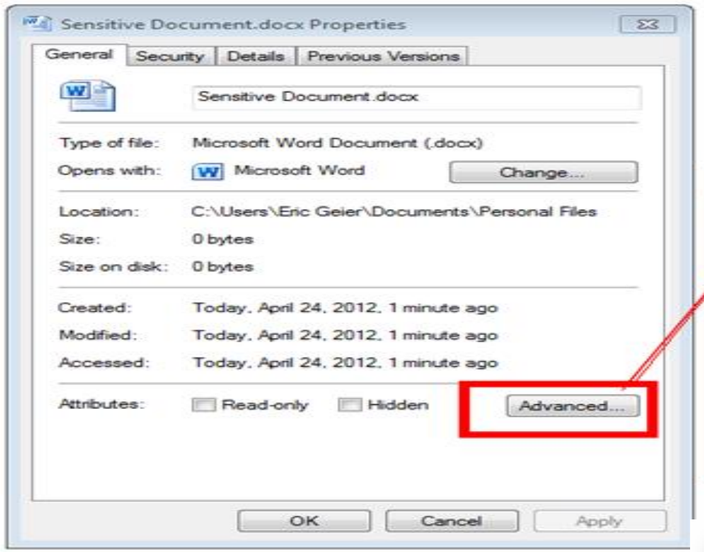
Rendere non leggibile il dato a terzi evitando l'accesso non autorizzato

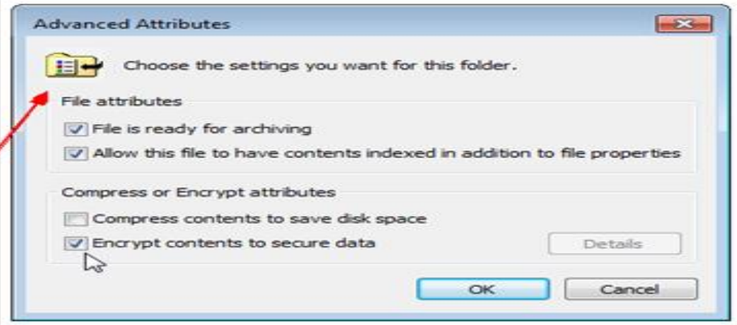
Attacchi principalmente di malware, ma anche insider threat e cyberspianaggio

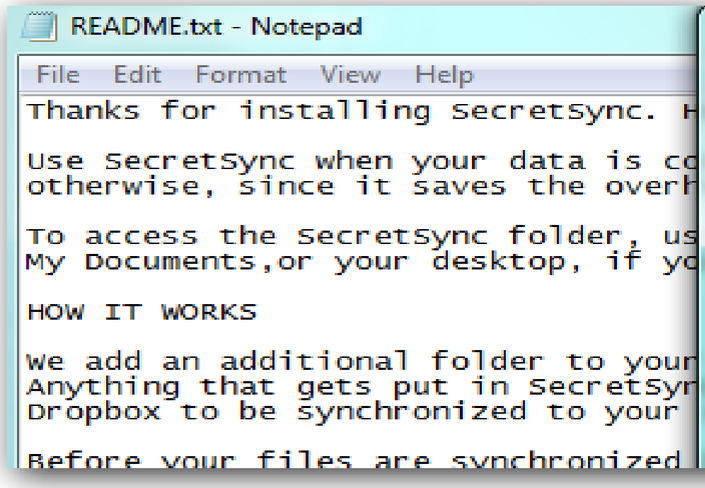
Condividere dati sensibili senza «offuscamento» ha un elevato rischio di data leak che può sfociare in caso di leak in una frode o ricatto

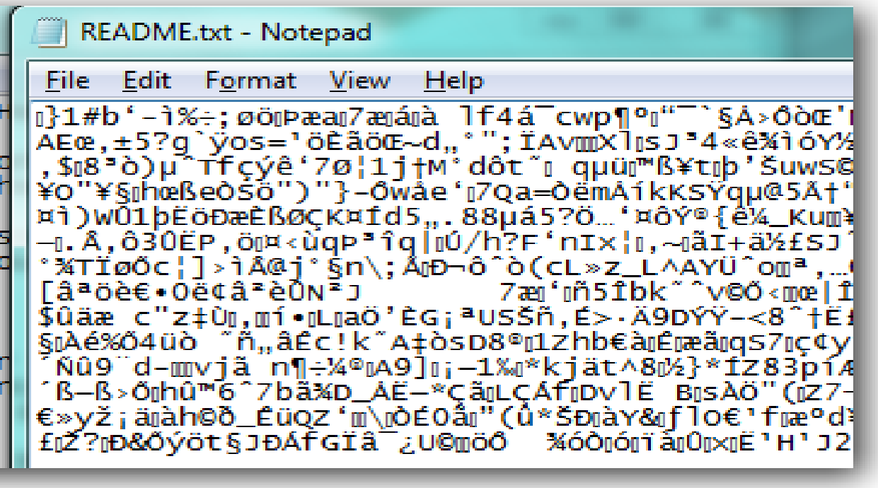
Crittografia

08 **CRITTOGRAFIA**
Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili









Procedure

09 PROCEDURE
Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

Vanno rivisionate almeno una volta l'anno. Tramite dei piani di Audit a cui va seguito un piano di Remediation

Sono un insieme di azioni da seguire quando si gestiscono i dati/informazioni o sistemi (ie. Procedura di backup, aggiornamento antivirus, accesso ai sistemi, etc)

Indicano il modo di agire e le regole da rispettare al fine di evitare la perdita di dati e informazioni

Seguirle diminuisce il rischio di perdita dei dati ed aumenta il valore del Brand. ie. GDPR, ISO27001 , etc

Se seguite in maniera scrupolosa possono evitare la gran parte delle minacce (ie. Phishing, Social Engineering, etc)

Accessi

10 **ACCESSI**
Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

Configurando opportuni sistemi di protezione perimetrale come Firewall o IDS. Tracciando tramite i LOG di accesso le operazioni effettuate dagli utenti

Sono delle tecniche utilizzate per l'identificazione di accessi anomali

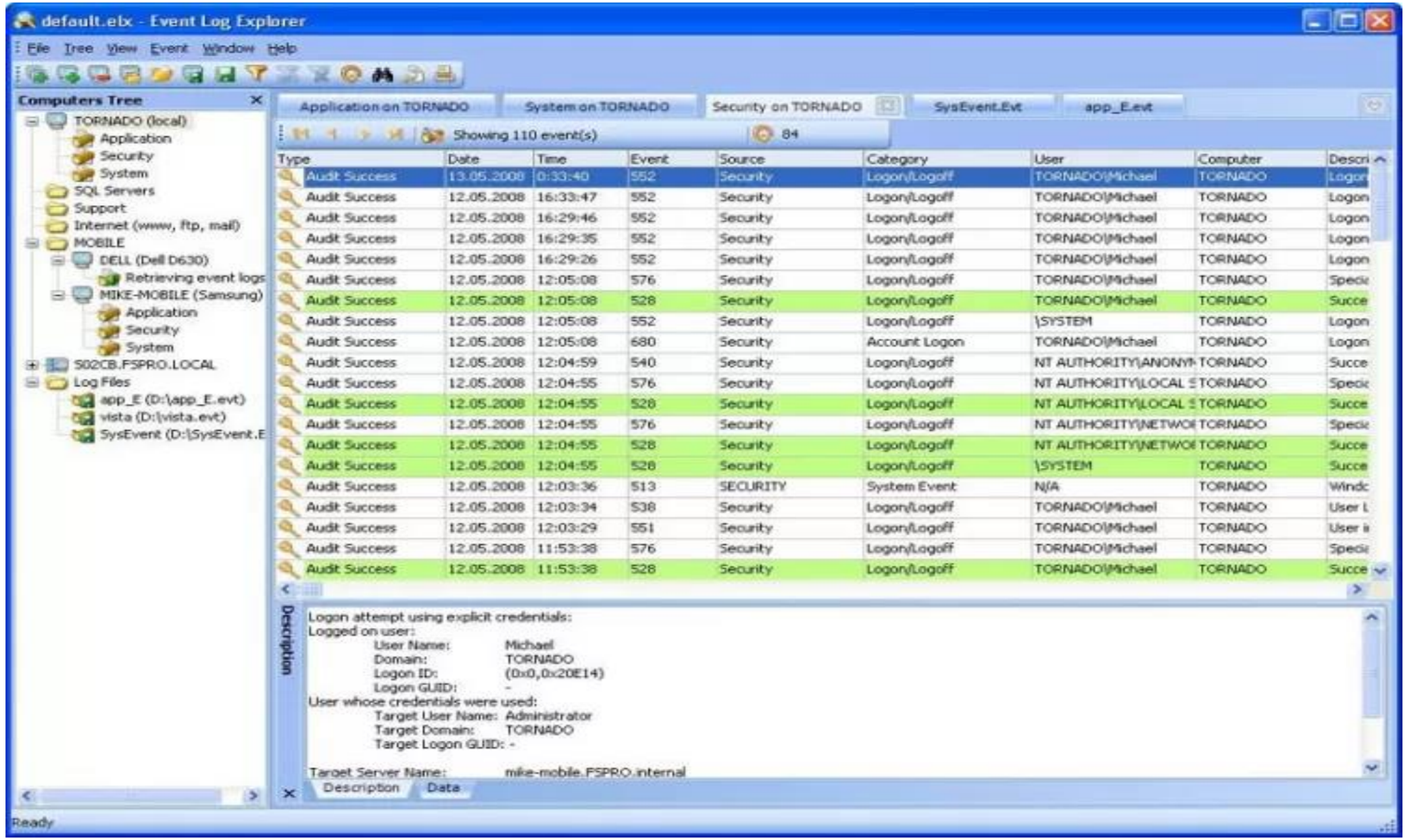
Principalmente a identificare e prevenire accessi anomali da parte di soggetti ad aree non pertinenti o attacchi esterni

Se si identificano accessi da parte di soggetti non autorizzati il rischio di data leak associato è molto alto. Lo stesso vale in caso di attacco dall'esterno

Insider Threat e malware, Ddos, etc

Accessi

10 **ACCESSI**
Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro



Conclusioni

Esistono diversi rischi e minacce nel mondo dell'IT, ognuna della quali ha un impatto sull'operatività e sui dati diversa.

Oltre ai 10 elementi e regole da seguire per un corretto uso in sicurezza dei nostri dati, ne **esiste una 11 esima, legata alla possibilità di sottoscrivere una contratto assicurativo in caso di data breach o attacco informatico**. Dove però la responsabilità primaria ricade sempre nel Titolare del dato stesso.

Non esiste un livello di sicurezza massimo, ma il tutto si basa sulla consapevolezza del singolo rispetto alla percezione del rischio.

L'Human Factor è l'elemento essenziale da considerare nonché l'elemento più debole della catena.