Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

LA SICUREZZA DELLE RISORSE INTANGIBILI

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

Agenda

Condivisione obiettivo e poi.....

Parte 1: Scenari di riferimento

Parte 2: Rischi…Reati?

Parte 3: Risorse immateriali

Parte 4: La tutela delle informazioni aziendali

Parte 5: Come difendersi?

Obiettivo

CULTURA PRATICA E CONCRETA DELLA / ALLA SICUREZZA

1. Percezione di **PERICOLO** e **RISCHIO**
2. Conoscenza di **SCENARI** e dei **RISCHI**
3. Conoscenza degli **AGGRESSORI** e delle **MODALITA' DI ATTACCO**
4. Far cogliere l'importanza degli **STRUMENTI** per indagare e difendersi
5. Renderci **CONSAPEVOLI**

L'ICEBERG DEL RISCHIO

RISCHIO CONSAPEVOLE

esplicito

RISCHIO INCONSAPEVOLE

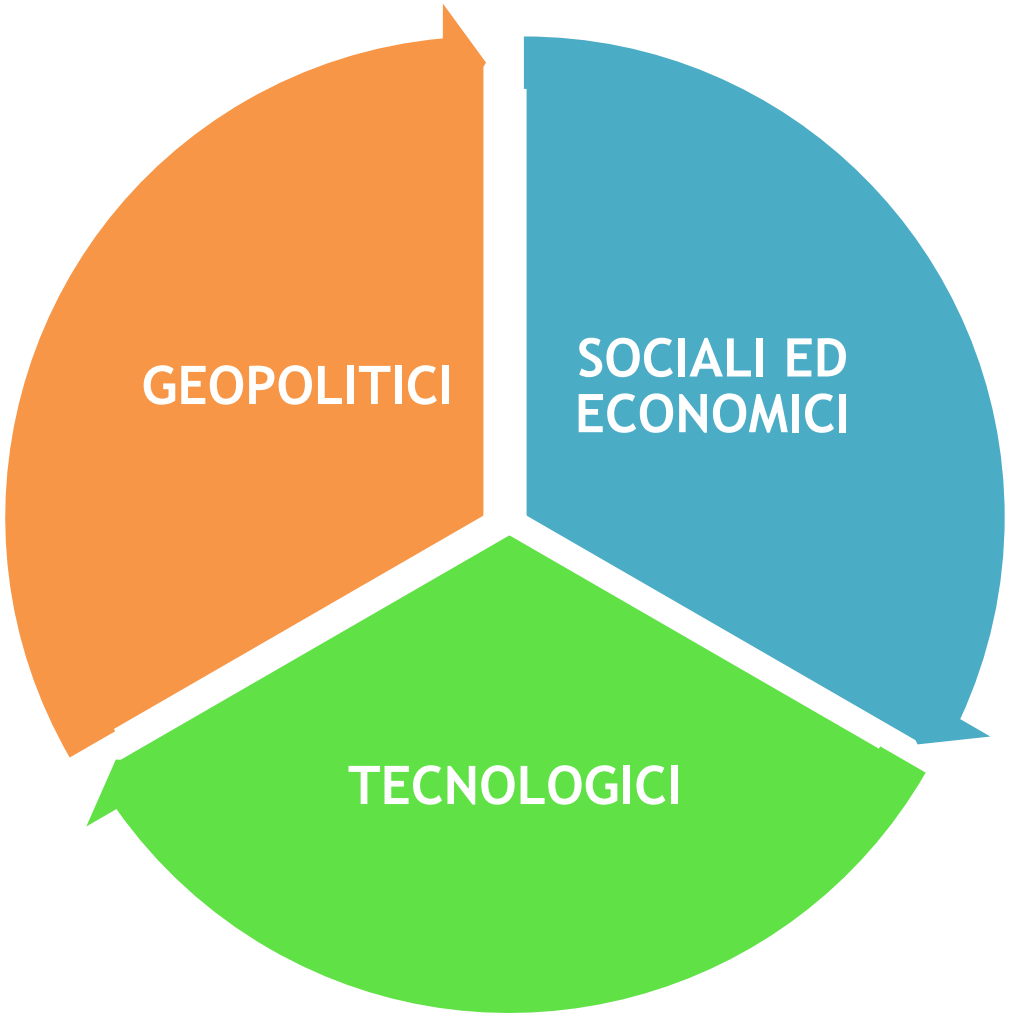
implicito

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

PARTE 1

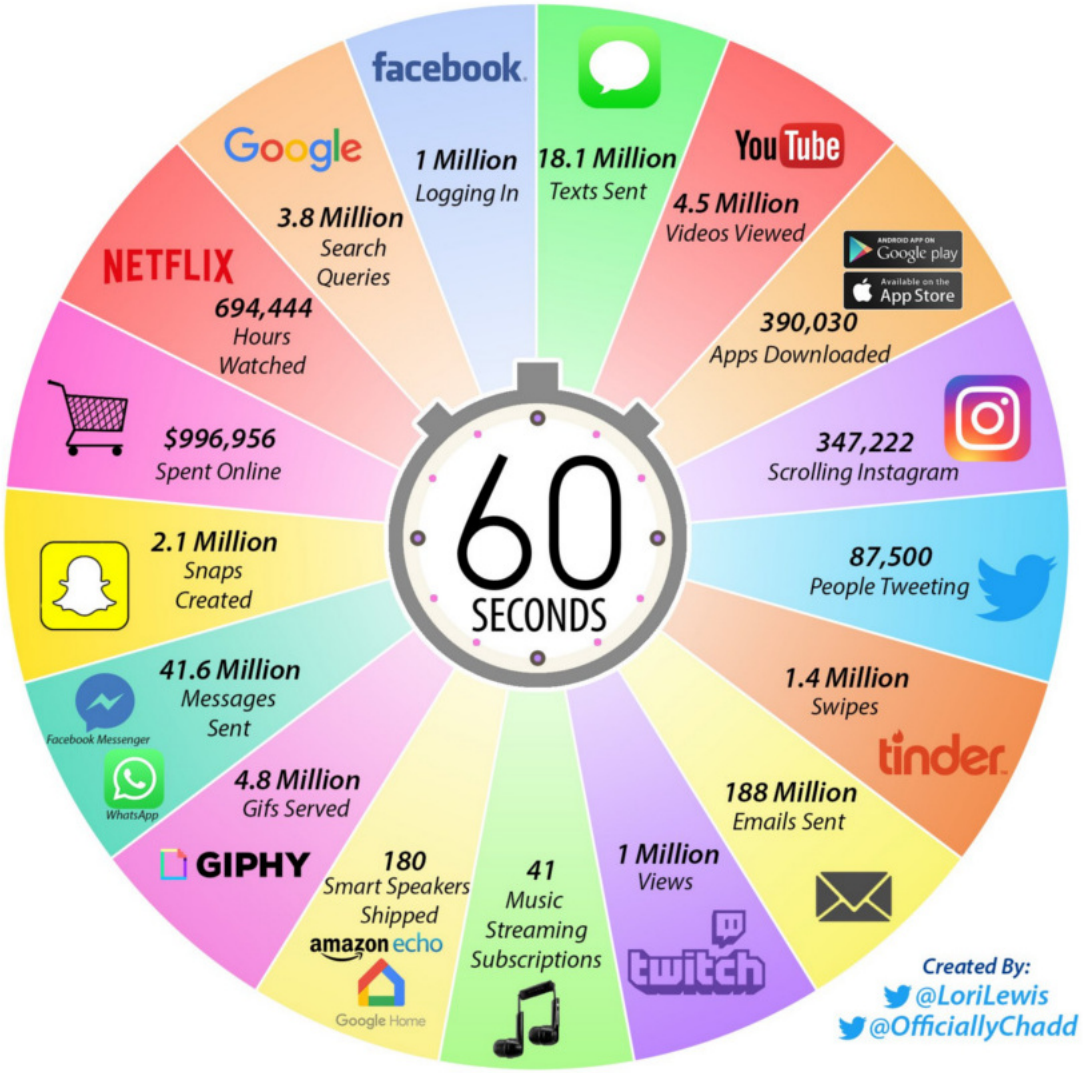
SCENARI

SCENARI GLOBALI

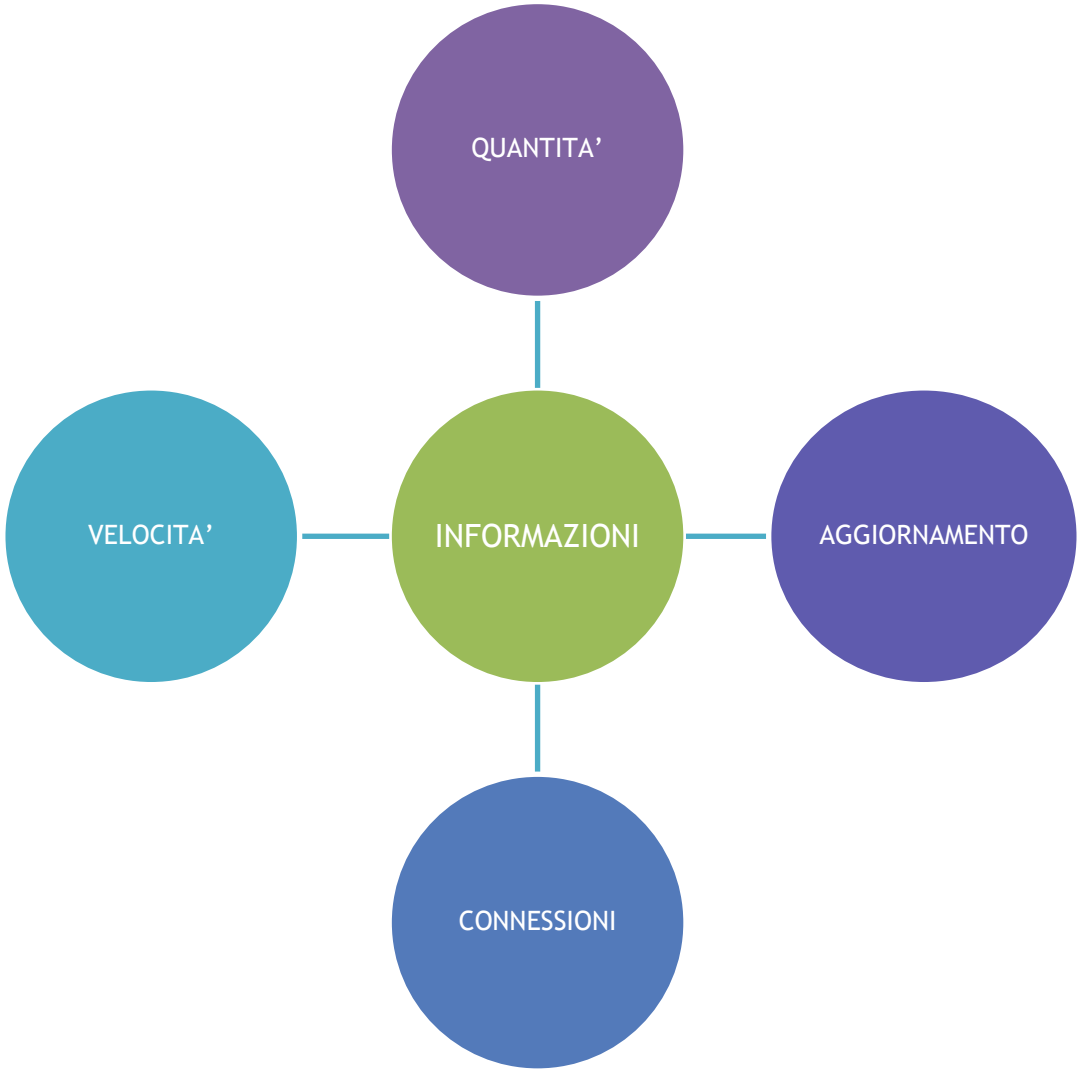


TREND TECNOLOGICI 2019

2019 This Is What Happens In An Internet Minute



OPPORTUNITA’



Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

PARTE 2

RISCHI...

REATI?

RISCHI INFORMATICI

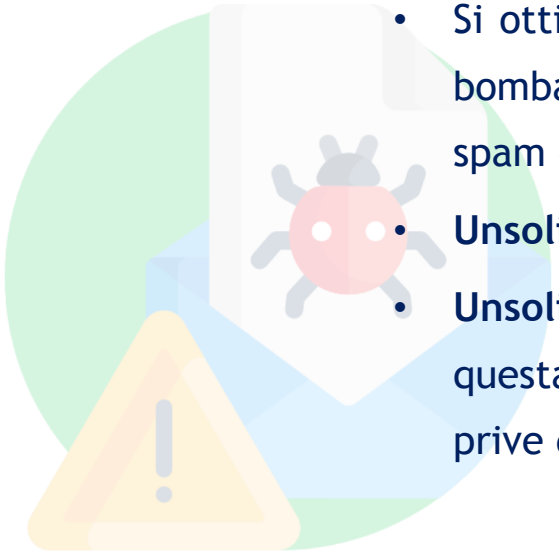
- Virus, malware e software maligni volti a modificare o distruggere i dati
- Accessi non autorizzati a sistemi informatici e telematici volti a danneggiare, bloccare o alterare dati/sistemi e informazioni
- Frodi informatiche – Phishing, Pharming, Spoofing…
- Furto e diffusione delle credenziali di accesso (password e userid) e sfruttamento dell'identità informatica
- Defacement
- Social Engineering
- Sabotaggi e attacchi volti a far bloccare la rete – DOS, Spamming, …
- Intercettazioni di comunicazioni , dati, messaggi - Sniffing, …
- Furto PC portatili o altri supporti informatici
- Abuso collegamenti Internet per scaricare immagini, software illegale, ..
- Utilizzo non accurato delle e-mail
- Errori umani utenti e operatori
- ….

Rischi Informatici

1 Virus:

Sono programmi che causano danni ai computer; si annidano nei meandri della posta elettronica, viaggiando con gli allegati apparentemente innocui.

2 Spamming:



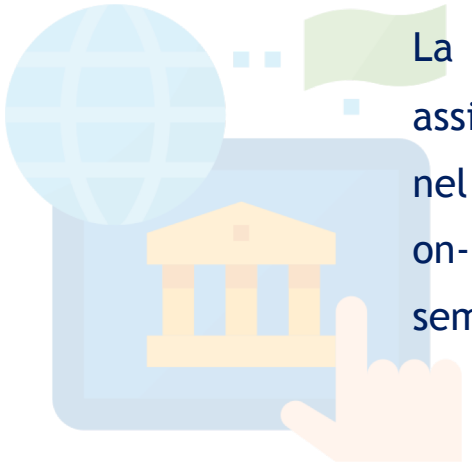
- Si ottiene quando la scorrettezza postale supera i limiti accettabili (carpet bombing: bombardamento a tappeto simile alla pubblicità che tracima dalle cassette postali, spam è il singolo messaggio, spammer è il responsabile dell'invio).
- **Unsolicited Commercial E-mail (UCE)** indica la natura commerciale dell' e-mail.
- **Unsolicited Bulk E-mail (UBE)** mette in evidenza l' invio di massa di un email, in questa categoria rientrano anche le classiche catene di Sant' Antonio le quali sono prive di natura commerciale.

Rischi Informatici

3 Phishing:

E' una frode on-line ideata per sottrarre con l'inganno numeri di carte di credito, password, informazioni su account personali. Attuato generalmente tramite e-mail si basa sull'invio da parte di un utente malintenzionato di e-mail che sembrano provenire da siti web autentici o noti i quali richiedo all'ingenuo utente l'inserimento di informazioni personali.

4 Pharming:



La truffa consiste nel realizzare pagine web identiche ai siti già esistenti (banche, assicurazioni, softwarehouses etc.) in modo che l'utente sia convinto di trovarsi, ad esempio, nel sito della propria banca e sia indotto a compiere le normali transazioni sul proprio conto on-line. Una volta digitate le credenziali (password e user ID) del proprio conto, sarà semplice recuperarle, tramite keylogger o troiani, per utilizzarle a fini fraudolenti.

Security & Safety
Sicurezza Logica | **Posteitaliane**

Egregio Cliente,

La preghiamo di esaminare con la massima serieta e immediatamente questo messaggio di posta elettronica che mostra le nuove misure di sicurezza.

Il reparto sicurezzo della nostra banca le notifica che sono state prese misure per accrescere il livello di sicurezza dell'online banking, in relazione ai frequenti tentativi di accedere illegalmente ai conti bancari.

Per ottenere l'accesso alla versione piu sicura dell'area clienti preghiamo di dare la sua autorizzazione.

Accedi ai servizi online »

Se scegliete di ignorare la nostra richiesta, purtroppo non avremo altra scelta che bloccare temporaneamente il suo account.

Distinti saluti,
BancoPostaonline

Subject: Facebook Account Update

facebook

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.

If you have any questions, reference our New User Guide.

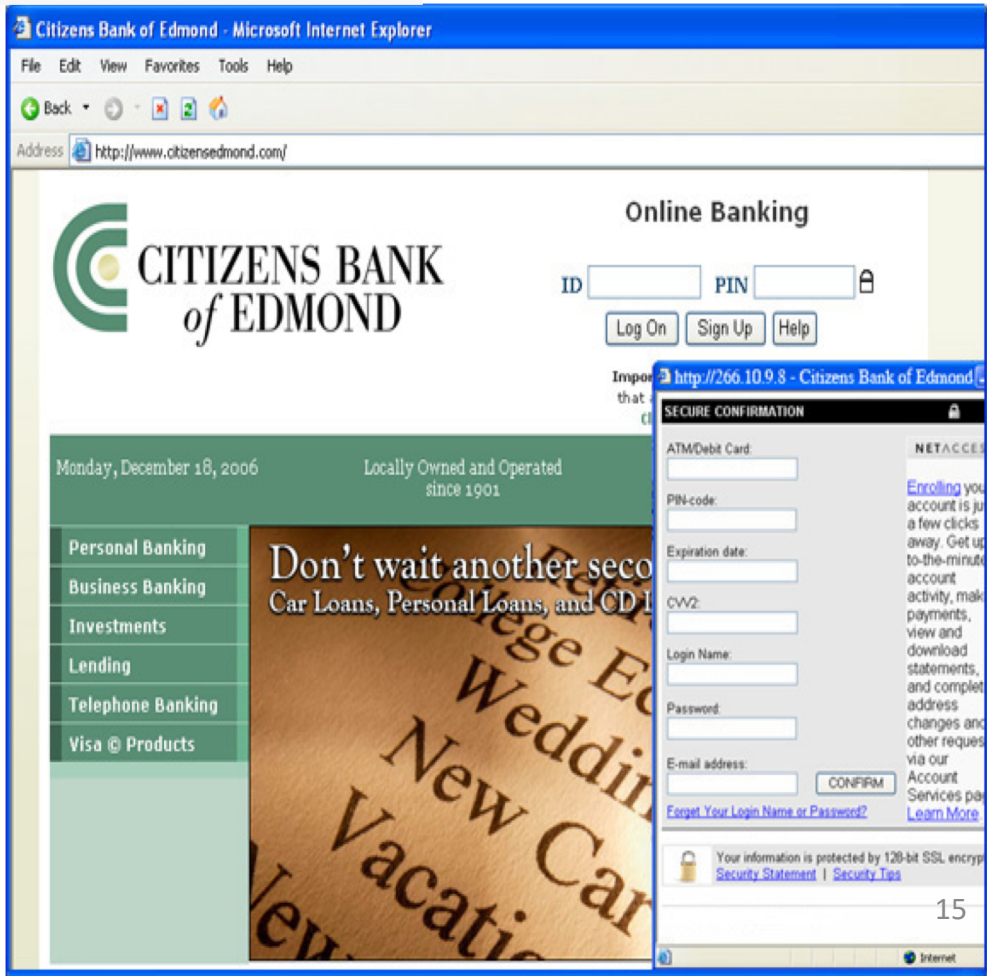
Thanks,
The Facebook Team

Update your Facebook account

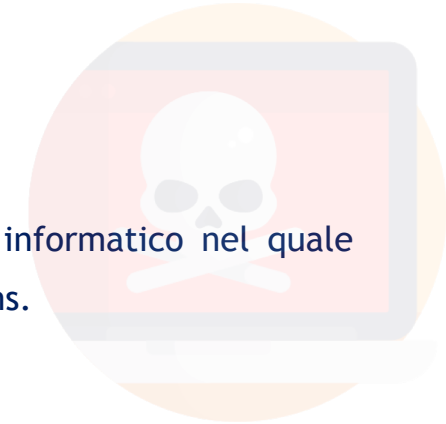
Update

This message was intended for [redacted].
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Facebook Phishing Email



Rischi Informatici



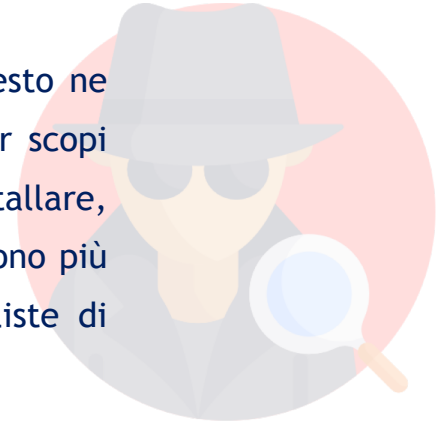
5 Malware:

Programmi realizzati al solo scopi di creare danni all' interno del sistema informatico nel quale vengono eseguiti. In questa categoria rientrano i virus, trojan, backdoor, worms.

6 Cookie:

E' il biscottino che si infila nel nostro computer quando visitiamo alcuni siti, in genere commerciali (spia le connessioni). Rappresentato da un messaggio apparentemente innocuo (un logo), accumula dati sui nostri gusti e sulle nostre preferenze e li ritrasmette a chi ce lo ha spedito.

7 Spyware:



Software in grado di rilevare e registrare le scelte e preferenze dell' utente senza che questo ne sia consapevole e trasmettere le informazioni raccolte a società che riutilizzano i dati per scopi commerciali. Sono programmi che disseminano, nei computer in cui si vanno ad installare, "ripetitori" di informazioni riservate su abitudini e preferenze di navigazione dell'utente. Sono più invasivi dei cookies poichè si impadroniscono di informazioni molto sensibili, password, liste di indirizzi e-mail.

Rischi Informatici

8 Sniffer:

E’ un programma in grado di intercettare i messaggi di posta elettronica (con tutti gli indirizzi in esse contenuti), ma anche i numeri delle carte di credito (quelli non crittografati).

9 Spoofing:

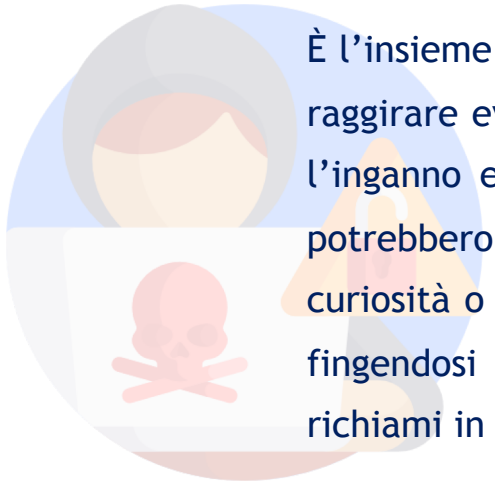
Lo spoofing è una tecnica utilizzata per camuffare files in rete in rete e raggirare ignari ed impotenti utenti. La parola deriva dal verbo inglese to spoof che significa imbrogliare, truffare. La tecnica dello spoofing consiste nel mascherare l’ effettiva estensione del files allegato facendo credere all’ utente (e spesso anche all’ antivirus) che il files allegato sia qualcosa che in realtà non è. Lo spoofer cerca di danneggiare i malcapitati bersagli delle sue fregature attraverso la posta elettronica. Spesso si caratterizza nell ’ invio di e-mail contenenti allegati apparentemente innocui, tipo archivi zip, o immagini, o anche documenti di testo con estensioni rispettivamente .zip, .jpg o .txt.

Rischi Informatici

10 Defacing:

Defacing (o defacement) è l'atto di cambiare illecitamente la homepage di un sito web o modificarne una o più pagine interne da parte di persone non autorizzate. È generalmente un atto vandalico e simbolico effettuato da attaccanti spesso alle prime armi come dimostrazione delle loro abilità e può essere utilizzato anche per diffamare o screditare la vittima.

11 Social Engineering:



È l'insieme delle tecniche che sfruttano il comportamento umano al fine di ottenere informazioni. Questo metodo riesce a raggirare eventuali ostacoli che l'attaccante incontra quando sono messe in atto adeguate misure di sicurezza. Attraverso l'inganno e nascondendo la propria identità o fingendosi un'altra persona si riesce a ricavare informazioni che non si potrebbero mai ottenere facilmente in altro modo. Si sfruttano così debolezze del comportamento umano come la curiosità o l'empatia per poi arrivare all'attacco vero e proprio. Si sceglie di attaccare spesso dipendenti di basso livello, fingendosi superiori (interni o esterni) che necessitano di informazioni immediate, sfruttando la paura di incorrere in richiami in ambio lavorativo.

Rischi Informatici

12 Denial of Service:

Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio.

13 Bot/Botnet:

I computer bot-infected, o anche solo bot, sono i computer sui quali gli attaccanti hanno installato un programma infetto che consente loro di controllare da remoto questi computer e utilizzarli come veicolo di attività malevole. Una rete di pc Bot si chiama botnet.

In questi modo, i cyber criminali sono in grado di controllare un grandissimo numero di computer che permettono loro di lanciare diversi tipi di attacchi come ad esempio un denial-of-service (DoS) contro il sito web di una organizzazione, l'invio massivo di spam e phishing, la propagazione di codici malevoli, spyware e adware, e la raccolta di informazioni confidenziali con serie conseguenze economiche e legali

Informazioni: quali i rischi? RAPPORTO CLUSIT 2019

- Secondo il Rapporto CLUSIT 2019, il 2018 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo, si evidenzia un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza.

- Stando ai dati presenti nel report, frutto degli **attacchi rilevati dal Security Operations Center (SOC) di Fastweb**, nel 2018 sono stati analizzati 1.552 attacchi gravi (+ 37,7% rispetto all'anno precedente), con una media di 129 attacchi gravi al mese (rispetto ad una media di 94 al mese nel 2017, e di 88 su 8 anni).

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

PARTE 3

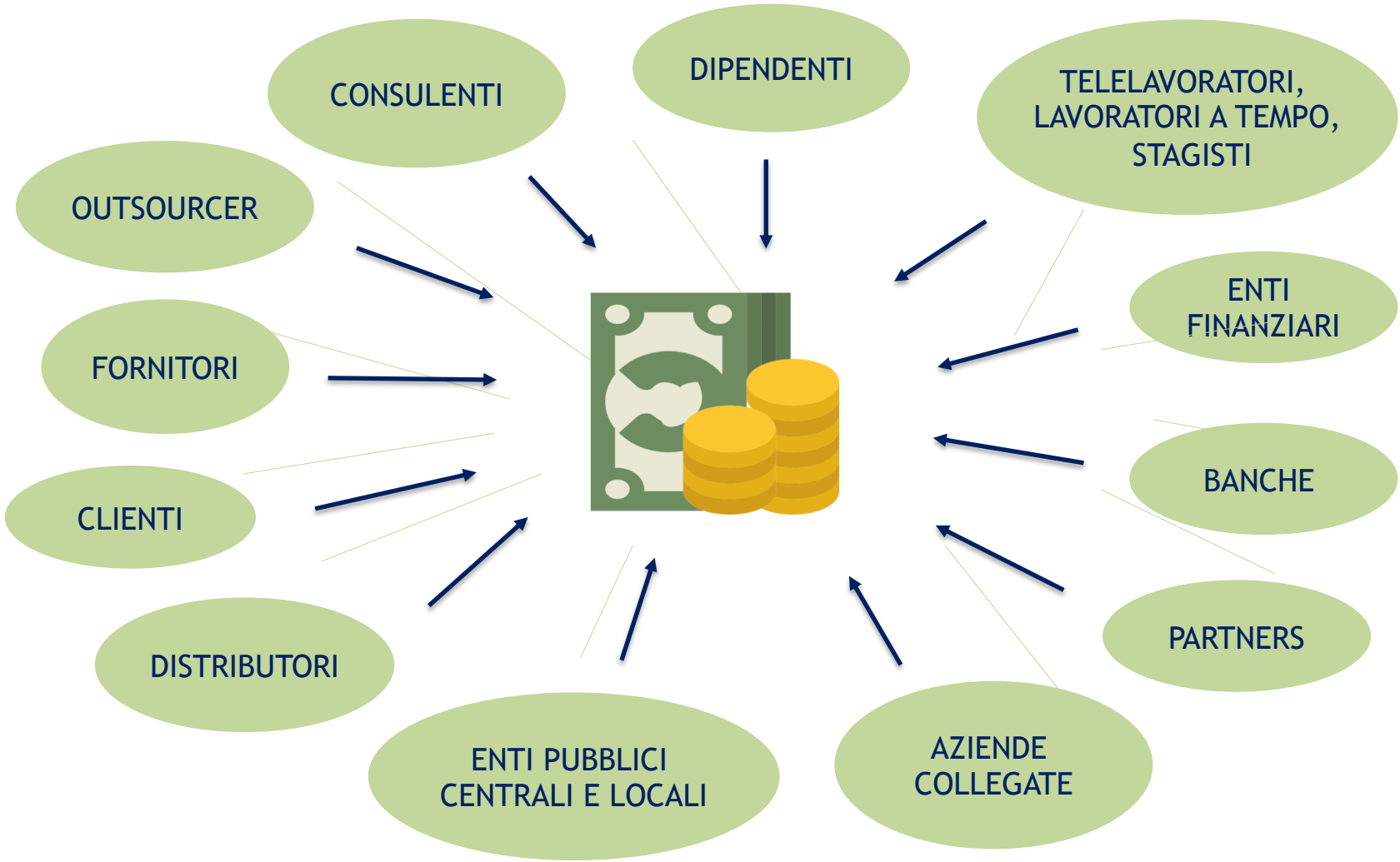
LE RISORSE IMMATERIALI E I RISCHI

Valore e Risorse Immateriali

- "Oggi le nazioni e le imprese in ascesa non sono quelle che possiedono la terra e le risorse materiali, ma quelle che possiedono le idee, le tecnologie e le informazioni." (Gilder)

- "La conoscenza è la nuova base della ricchezza, In passato, quando i capitalisti parlavano della loro ricchezza, si riferivano a impianti, attrezzature, edifici e risorse materiali. In futuro, si riferiranno a alla loro capacità di controllare la conoscenza. (Thurow Lester C.)

“Apertura” Sistema Impresa



Cosa si intende per risorse immateriali?

Non esiste una definizione univoca

Ci si riferisce a concetti/risorse molto diversi tra loro:

- Informazioni (ad es. commerciali, di processo, di prodotto)
- Diritti (ad es. brevetti e marchi)
- Conoscenza (ad es. skills del personale)
- Reputazione (ad es. brand, immagine)

Alcune definizioni

Codice Civile

Art. 2424

- Immobilizzazioni immateriali
- Costi di R&S e pubblicità
- Diritti di brevetto industriale e di utilizzazione delle opere dell'ingegno
- Concessioni, licenze, marchi e diritti simili
- Avviamento
- Immobilizzazioni in corso

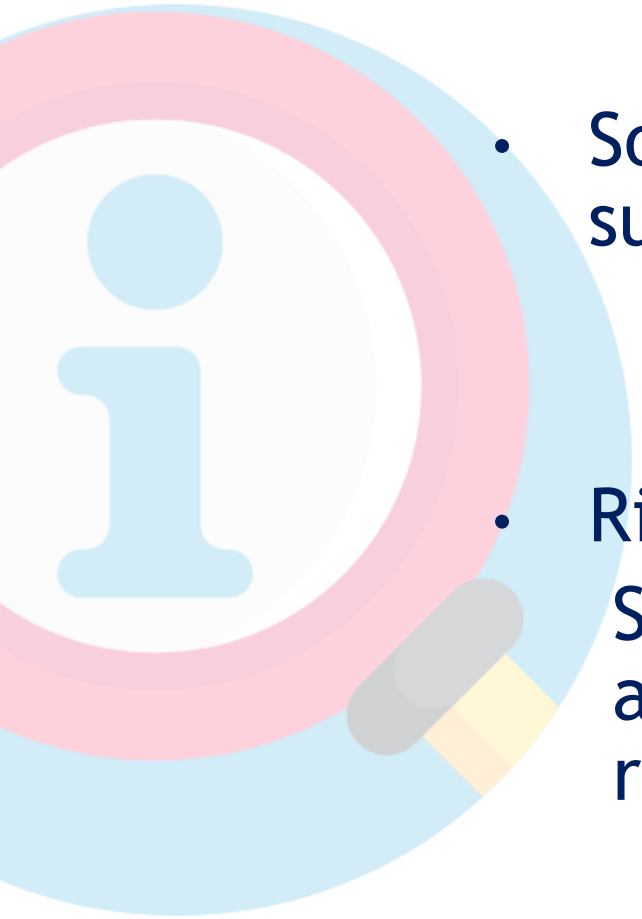
Alcune definizioni

Insieme degli elementi che:

- Residuano una volta che siano state enucleate le risorse materiali
- Contribuiscono in maniera significativa allo sviluppo dell'attività aziendale e alla sua capacità, effettiva e potenziale, di profitto

(A. Renoldi)

Alcune definizioni



- Sono invisible assets le risorse basate sull'informazione o che la incorporano

(H. Itami)

- Risorse aziendali basate sull'informazione …

  Si tratta, cioè, di quella parte del patrimonio aziendale capace di un processo di continua riproduzione e autoalimentazione

(S. Vicari)

Alcune definizioni

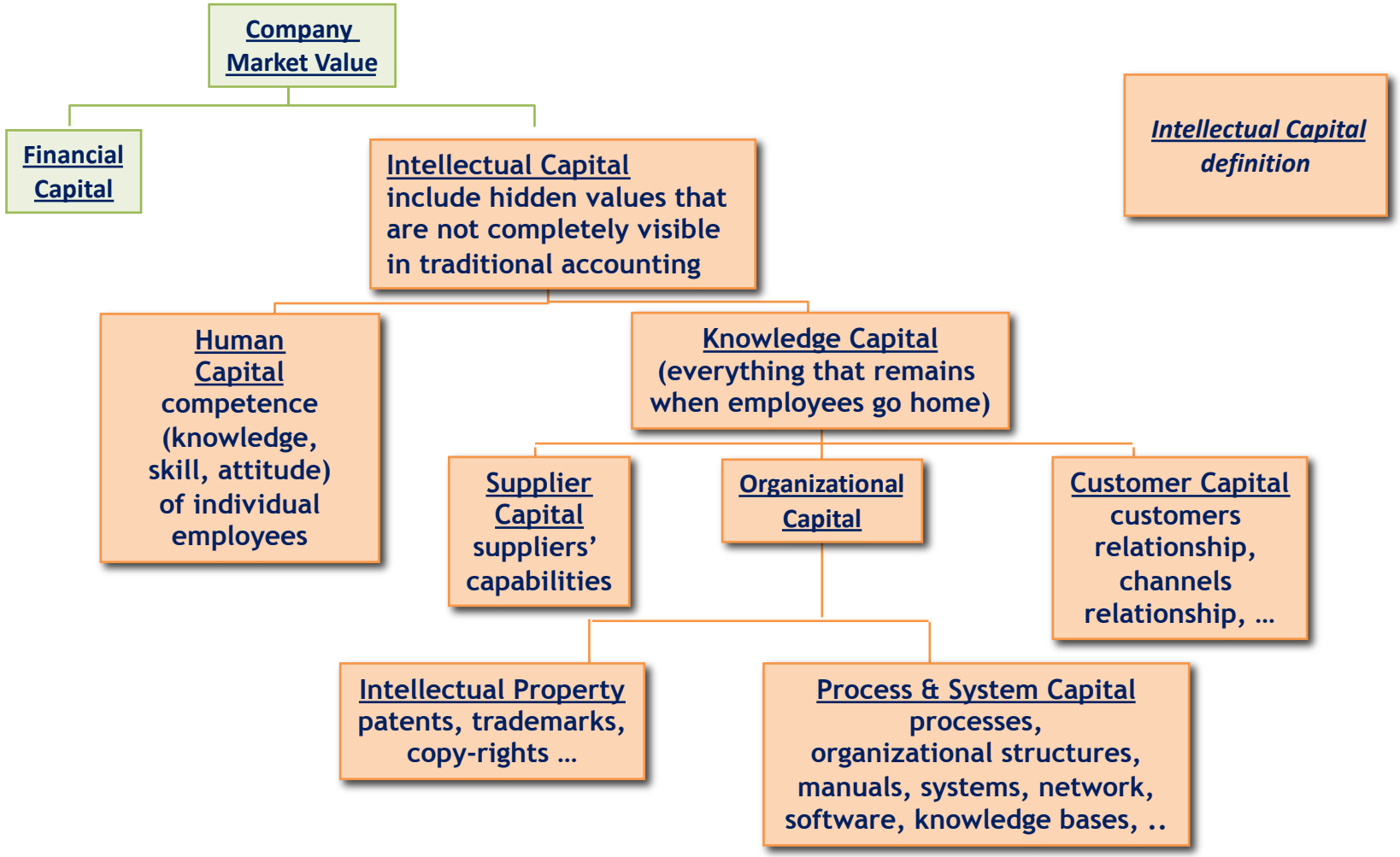
- Risorse intangibili, ovvero quelle potenzialità aziendali che costituiscono investimento a reddito futuro. … Occorre poi distinguere tra attività che corrispondono a **proprietà immateriali** (brevetti, know how, marchi) che trovano la loro valutazione nel bilancio di esercizio e le altre attività di carattere intangibile, come l'avviamento di mercato, l'immagine, il patrimonio di conoscenze che non trovano espressione nel bilancio.

- Le risorse intangibili fanno parte del codice genetico dell'impresa e si pongono alla base della creazione del sistema dei valori…. **(S. Sciarelli)**

Aree di formazione delle risorse immateriali

- Le risorse **umane**, o anche patrimonio umano o intellettuale (conoscenze, competenze, capacità e attitudini dei singoli individui)
- Le risorse **organizzative**, o anche patrimonio organizzativo o strutturale (conoscenze condivise e assimilate dall'organizzazione, esplicita e tacita)
- Le risorse **relazionali**, o anche patrimonio di reputazione o di relazioni (quantità e qualità di relazioni dell'impresa con gli stakeholder)

Valore e Risorse Immateriale



Risorse Immateriali: quali i rischi?

Quali tutelare?

Quali rischi?

RISCHI CONTRO RISORSE IMMATERIALI

INFORMAZIONI

- Vendita e divulgazione non autorizzata di informazioni
- Sottrazione di idee/progetti speciali
- Fuoriuscita di know how (sottrazione dipendenti chiave)
- Frodi informatiche (Phishing, identity theft, …)
- Sabotaggio/Intrusione nei sistemi informativi
- Diffamazione/Attacchi alla reputazione
- Contraffazione marchi e violazione di brevetti

Informazioni: quali i rischi?

Eventi che possono arrecare conseguenze alla:

1 **Riservatezza**
Assicurare che le informazioni siano accessibili solo alle persone autorizzate

2 **Integrità**
Tutelare l'esattezza e la completezza delle informazioni

3 **Disponibilità**
Assicurare la possibilità di accesso alle informazioni quando richiesto delle risorse informative aziendali

ESEMPI:
- Interruzioni Energia Elettrica
- Disastro naturale (acqua, fuoco, …)
- Spionaggio industriale
- Divulgazione non autorizzata o Vendita di informazioni Riservate
- Manomissione/ Alterazione dati
- Errori umani utenti e operatori
- ….

RISCHI

NATURALI

Incendio
Terremoto
Allagamento
Temporale

ANTROPICI

Furti di PC e di informazioni e di credenziali di accesso
Furti/Frodi di identità
Virus, malware
Intercettazioni delle comunicazioni
Spionaggio
Sabotaggi e attacchi volti a bloccare la rete
Attacchi terroristici
Guerre informatiche

TECNOLOGICI ACCIDENTALI

Interruzione energia e funzionamento rete
Errori umani dovuti a scarsa attenzione
Uso non accurato dei devices e della posta elettronica

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

PARTE 4

LA TUTELA DELLE INFORMAZIONI AZIENDALI

Informazioni aziendali

PATRIMONIO INFORMATIVO AZIENDALE

INFORMAZIONI "SEGRETE"

INFORMAZIONI RISERVATE

Informazioni segrete

Fonti normative:

Accordo TRIPs ("*Accordo relativo agli aspetti dei diritti di proprietà intellettuale attinenti al commercio - Agreement on Trade-related Aspects of Intellectual Property Rights*", ratificato dall'Italia con legge 29 dicembre 1994 n. 747):

Art. 39 «Protezione di informazioni segrete»:

Le persone giuridiche hanno **la facoltà di vietare** che **le informazioni aziendali siano rivelate a terzi, acquisite, utilizzate da parte di terzi in un modo contrario a leali pratiche commerciali** se tali informazioni:

- » sono **sottoposte al legittimo controllo delle persone giuridiche**
- » sono **segrete**
- » hanno **valore commerciale**
- » sono **sottoposte a misure adeguate**

Informazioni segrete

D. Lgs. 30/2005 *(Codice della Proprietà Industriale)*

Art. 98 «Oggetto della tutela»:

Costituiscono oggetto di tutela tutte quelle **informazioni aziendali** e quelle **esperienze tecnico-industriali**, comprese quelle **commerciali**, **soggette al legittimo controllo del detentore** che presentano i seguenti requisiti:

sono segrete (non sono nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore. Considerate singolarmente possono essere di dominio pubblico o accessibili con attività non inventiva).

Informazioni segrete

- **Hanno valore economico** (attribuiscono all'impresa che le detiene un vantaggio competitivo rispetto alle imprese concorrenti che non fruiscono di tali informazioni; sono state conseguite con uno sforzo in termini di costi e di tempo impiegato da parte dell'impresa stessa)

- **Sono sottoposte dal legittimo detentore** a **misure ragionevolmente adeguate a mantenerle segrete** (policy e procedure di sicurezza delle informazioni, accordi di riservatezza, patti di non concorrenza)

*È **legittimo detentore** delle informazioni segrete chi le ha ideate o combinate, legittimamente acquistate o ricevute in licenza, chi le usa o le detiene con l'autorizzazione o con il consenso dell'avente diritto.*

Condizioni di protezione

- **Segretezza,** intesa nel senso di non facile accessibilità a tali informazioni.
- **Valore economico** di tali informazioni, inteso sia nel senso del costo della loro acquisizione che del vantaggio competitivo da esse conferito.
- **Misure di segretazione** idonee (Security Policy):
  - Policy e Procedure Sicurezza delle informazioni
  - Accordi di riservatezza
  - Patti di non concorrenza

Informazioni segrete

D. Lgs. 30/2005 (*Codice della Proprietà Industriale*)

Art. 99 «Tutela»

Ferma la disciplina della concorrenza sleale, il legittimo detentore delle informazioni e delle esperienze aziendali di cui all'art. 98 ha il diritto di **vietare ai terzi**, salvo proprio consenso, **di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali informazioni ed esperienze**, **salvo il caso in cui esse siano state conseguite in modo indipendente dal terzo**

Informazioni segrete

- La disciplina contenuta negli artt. 98 e 99 c.p.i. garantisce tutela giuridica al patrimonio conoscitivo aziendale anche quando non è coperto da diritti di privativa registrati (brevetti, marchi). Sono infatti tutelabili:
  - le informazioni tecniche brevettabili (ma non brevettate per scelta del detentore)
  - le informazioni non brevettabili (sprovviste dei requisiti per la brevettazione quali, ad esempio, informazioni per migliorare un processo produttivo o per produrre un bene, che attengono all'organizzazione dell'impresa, di natura strategica o di marketing)

- La tutela non opera nei confronti di chi ha conseguito un'autonoma realizzazione dell'informazione o ha agevolmente acquisito l'informazione (mancano i requisiti della segretezza e della non facile agibilità)

Informazioni segrete

- Il concetto di informazione segreta derivante dall'art. 98 c.p.i. richiama quello di ***Know How*** ossia di «***patrimonio di conoscenze pratiche non brevettate derivante da esperienze e da prove***» *(art. 1 Reg. CE 772/04)* (informazioni di natura aziendale, esperienze tecnico-industriali, anche di carattere commerciale quali business plan, documentazione relativa a piani di sviluppo o a strategie di mercato);
- Il know-how può "*consistere in un procedimento, in formule, in procedure di addestramento e, in generale, in informazioni di interesse industriale o commerciale, frutto di esperienze e di studi, le quali comportino vantaggi di ordine tecnologico o competitivo sul piano della produzione o del marketing e siano caratterizzate dalla segretezza; e rientrano nella categoria, quindi, accanto ad invenzioni non brevettabili prive di contenuto inventivo (ma non di novità, che si ritiene insita nella segretezza), le invenzioni brevettabili che il titolare intende non brevettare e preferisce sfruttare in segreto*" (*Cass. 27.2.1985, n. 1699*).

Informazioni riservate

- Il patrimonio informativo aziendale comprende anche **informazioni che, pur non soddisfacendo i requisiti di legge di cui all'art. 98 c.p.i., hanno per l'impresa un valore tale per cui è opportuno che non vengano divulgate** (cd. *informazioni riservate*).
- La Cassazione Civile (sentenza n. 1100/2014) ha qualificato «informazioni riservate» quelle informazioni che «**valgono ad assicurare la qualità dei prodotti di un'impresa e a differenziarli da quelli delle altre imprese operanti sul mercato**» (ad esempio processi di lavorazione, tecniche di vendita, liste clienti, prezziari).
- Tali informazioni sono tutelabili attraverso misure di natura legale

Oggetto della protezione

- Soluzioni tecnico-scientifiche
- Test di laboratorio
- Test clinici
- Contratti
- Contenuti su accordi di collaborazione o licenza
- Analisi di mercato
- Liste di clienti
- Strategie di marketing e pubblicità
- Politiche di fidelizzazione (clienti/fornitori)
- Analisi di previsione economiche
- Dati finanziari
- Dati del personale (salari, incentivi, commissioni etc)

La tutela preventiva

Art. 2104 c.c. - Obbligo di diligenza

L'articolo 2104 del codice civile ("diligenza del prestatore di lavoro") stabilisce che:

- "Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale

- Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende"

La tutela preventiva

Art. 2105 c.c. - Obbligo di fedeltà

- «Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio»

- Diritto relativo, esigibile solo verso il contraente per il tempo di validità del contrattuale (cessato il rapporto di lavoro il dovere di riserbo del dipendente rimane sostanzialmente limitato alle sole informazioni segrete di cui al c.p.i., fermo restando il limite della concorrenza sleale e fatto salvo un diverso esplicito patto tra le parti, anch'esso fonte di responsabilità contrattuale)

La tutela preventiva

Art. 2125 c.c. - Patto di non concorrenza

- «Il **patto con il quale si limita lo svolgimento dell'attività del prestatore di lavoro, per il tempo successivo alla cessazione del contratto**, è nullo se non risulta da atto scritto, se non è pattuito un corrispettivo a favore del prestatore di lavoro e se il vincolo non è contenuto entro determinati limiti di oggetto, di tempo e di luogo. La durata del vincolo non può essere superiore a cinque anni, se si tratta di dirigenti, e a tre anni negli altri casi. Se è pattuita una durata maggiore, essa si riduce nella misura suindicata».

La tutela preventiva

Art. 2598 c.c. – Concorrenza sleale

«Ferme le disposizioni che concernono la tutela dei segni distintivi e dei diritti di brevetto, compie atti di concorrenza sleale chiunque **si vale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda»**

(Esempi: assunzione di dipendenti altrui esclusivamente per l'utilizzazione delle conoscenze tecniche acquisite presso altra azienda e non in possesso del concorrente, sottrazione illecita di informazioni aziendali riservate attuata dai dipendenti dimissionari di una azienda che copiano CD-Rom, file CAD, progetti o simili per poterli utilizzare dopo essere stati assunti da una seconda azienda concorrente della prima)

La tutela giudiziaria

La disciplina processuale e sanzionatoria prevista dal Codice di Proprietà Industriale per la tutela di tutti gli altri diritti di proprietà industriale si applica anche alle informazioni segrete.

Contro tutte le ipotesi di acquisizione ed utilizzo delle informazioni aziendali il titolare può agire in giudizio in via cautelare ed ordinaria, ai fini dell'accertamento:

- della violazione
- dell'inibitoria della continuazione e della ripetizione delle condotte illecite
- della condanna al risarcimento dei danni

La tutela penale

- Vengono sanzionati penalmente i comportamenti lesivi del segreto professionale e del segreto industriale ai sensi degli artt. 621, 622 e 623 del codice penale.
- In particolare:

Art. 621 «Rivelazione del contenuto di documenti segreti»

Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da lire duecentomila a due milioni.

Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.

Il delitto è punibile a querela della persona offesa.

La tutela penale

Art. 622 «Rivelazione di segreto professionale»

Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione.

La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società .

Il delitto è punibile a querela della persona offesa

Art. 623 «Rivelazione di segreti scientifici o industriali»

Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche , o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto è punito con la reclusione fino a due anni.
Il delitto è punibile a querela della persona offesa.

La tutela penale

Il riconoscimento dell'estensione della tutela prestata dall'art. 623 c.p. al know-how aziendale è frutto di una pronuncia della Corte di Cassazione del 2001 (Sentenza n. 25008. Caso: rivelazione di notizie segrete compiuta, in violazione di un patto di non concorrenza, da parte di taluni dipendenti dimissionari di una società in favore di altra impresa. Le notizie, in particolare, concernevano la tecnologia e le modalità di produzione di una macchina d'ispezione a raggi X per l'industria alimentare)

Disposizioni giuridiche a tutela della proprietà intellettuale

- **Art. 2105 c.c. - Obbligo di fedeltà**
- **Art. 2125 c.c. - Patto di non concorrenza**
- **Art. 2598 c.c. - Concorrenza sleale**
- Art. 2569 - 2572 c.c. – Marchi
- **Art. 621 c. p. - Rivelazione del contenuto di documenti segreti**
- Art. 622 c.p. – Rilevazione di segreto professionale
- Art. 623 c.p. – Rilevazione di segreti scientifici e industriali
- Art. 623 bis – Altre comunicazioni e conversazioni
- **L. 10.02.2005 n. 30 - Codice della proprietà industriale - Artt. 98 - 99**
- **TRIPS Agreement - Art. 39**

Security & Intangible Assets

Considerazioni Strategiche

- La tutela delle informazioni e delle risorse immateriali più in generale è funzionale alla creazione di valore d' impresa.

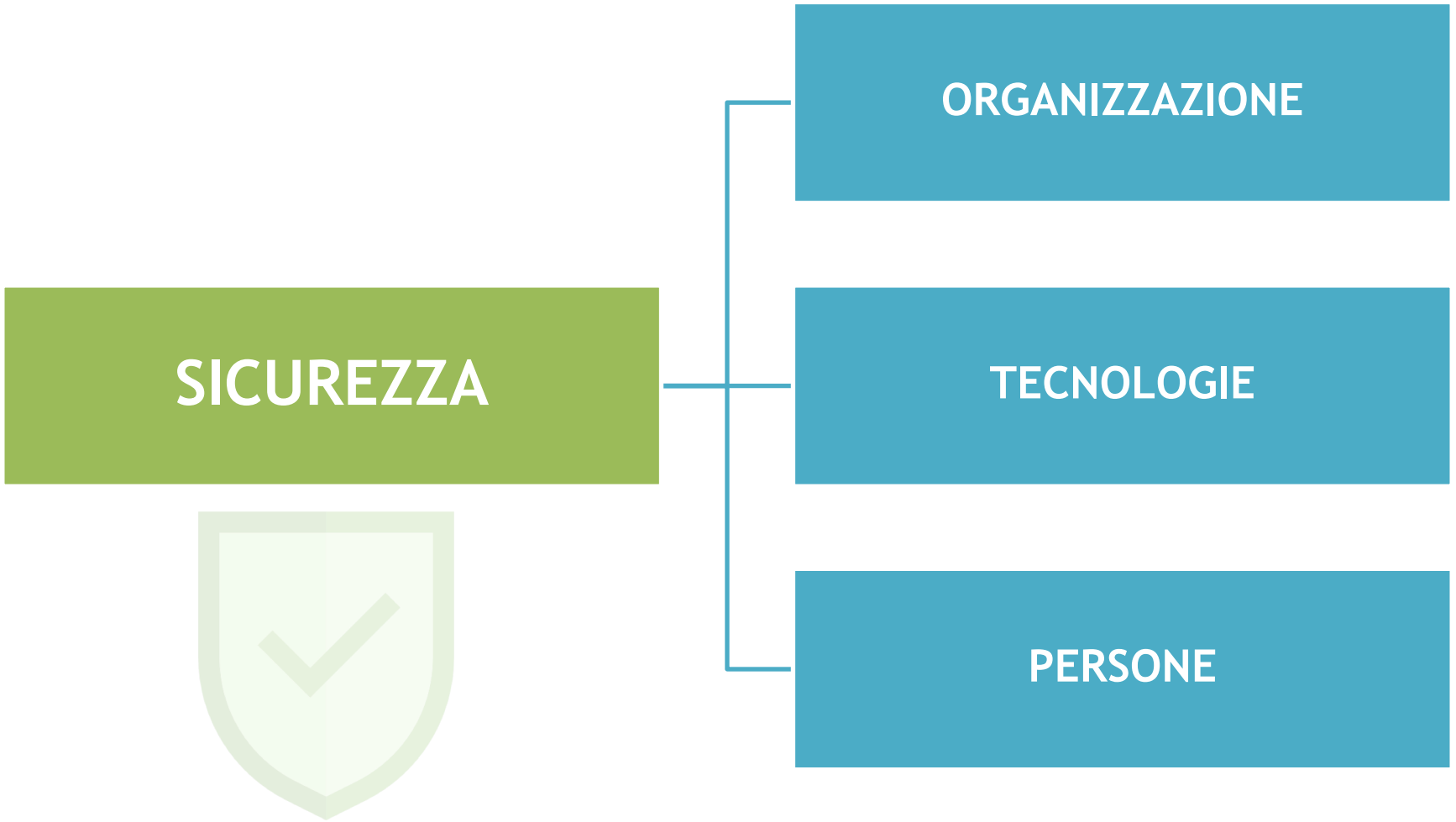
- La non consapevolezza di detenere intangible assets critici e la loro conseguente mancata tutela sono condizioni favorevoli alla distruzione del valore dell' impresa.

Scuola Internazionale
Etica&Sicurezza
Milano - L'Aquila

PARTE 5

COME DIFENDERSI?

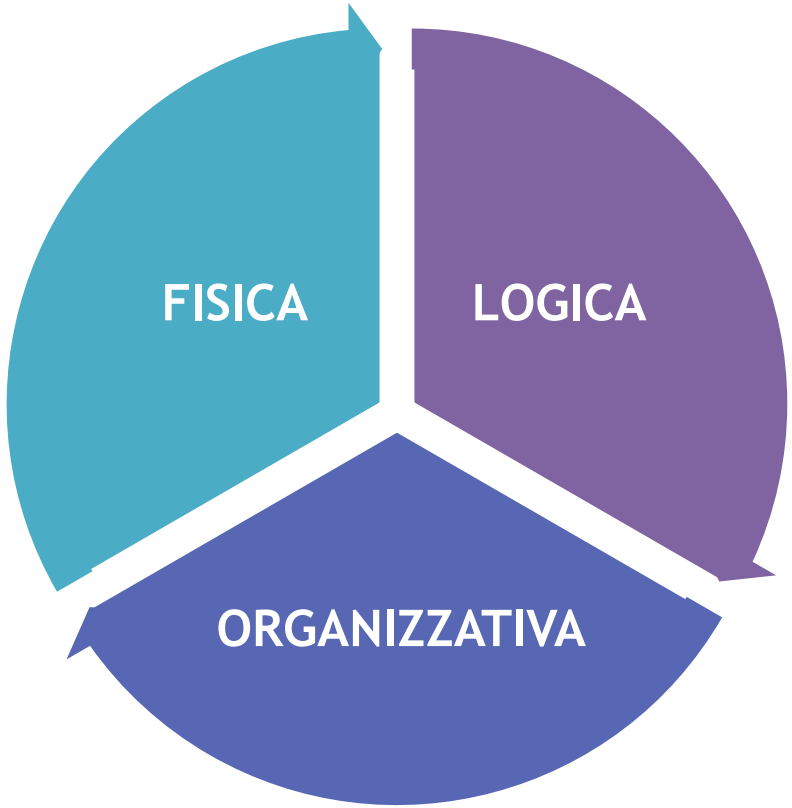
LE 3 LEVE SULLE QUALI AGIRE



SICUREZZA DELLE INFORMAZIONI: I PARAMETRI

CONTROMISURE DI SICUREZZA

Le contromisure sono le realizzazioni e le azioni volte a limitare le vulnerabilità e a gestire i rischi.



Le categorie di contromisure

Le contromisure sono le realizzazioni e le azioni volte ad annullare o limitare le vulnerabilità e a contrastare le minacce.

Si possono classificare le contromisure in 3 categorie :

- **Fisica** (locali, uffici, CED, mezzi di comunicazione, ….)
- **Logica** (back up, antivirus, firewall, crittografia, …)
- **Organizzativa** (procedure accessi logici, uso password, antivirus, classificazione informazioni, utilizzo email, ….)

STRUMENTI ORGANIZZATIVI

IL MAGO DAVE?

WHY SHOULD I BE INTERESTED IN THIS ?

«IT Security is not a technology problem: it's an issue linked to personnel and managers. Bypassing human protections is often easy, it doesn't need investments but the cost of a phone call, and carries out minimal risks.»

"I had access to the most important worldwide companies' computer systems and I've successfully hacked some of the best computer systems ever developed by a human being. I've used different paths, both technical and not, in order to obtain source codes of various operating systems and telecommunication devices, with the goal of studying their vulnerabilities and their internal mechanisms.

[…] Often I wasn't using a keyboard and a modem, but ***picking up the phone and, simply, asking to the person for the access password I was looking for".***

(IN)CONSAPEVOLEZZA?

SAI MANTENERE LA PRIVACY DIGITALE?

La continua condivisione di dati online ci rende vulnerabili agli occhi dei cyber criminali.

Quanto sai tutelarti? 10 domande secche per scoprirlo.
http://www.focus.it/temi/cyber-terrorismo

ED ORA PRONTI VIA …

“Senza sicurezza, non c'è né privacy, né vera libertà. Non avete vita privata se la vostra casa non ha pareti; non si è liberi di camminare per le strade se non è sicuro farlo.”

(Neelie KROES, Vice-President of the European Commission
Responsible for the Digital Agenda)

Scuola Internazionale Etica&Sicurezza

Milano - L'Aquila