Sicurezza Informatica
e Digital Forensics

ROSSANO ROGANI

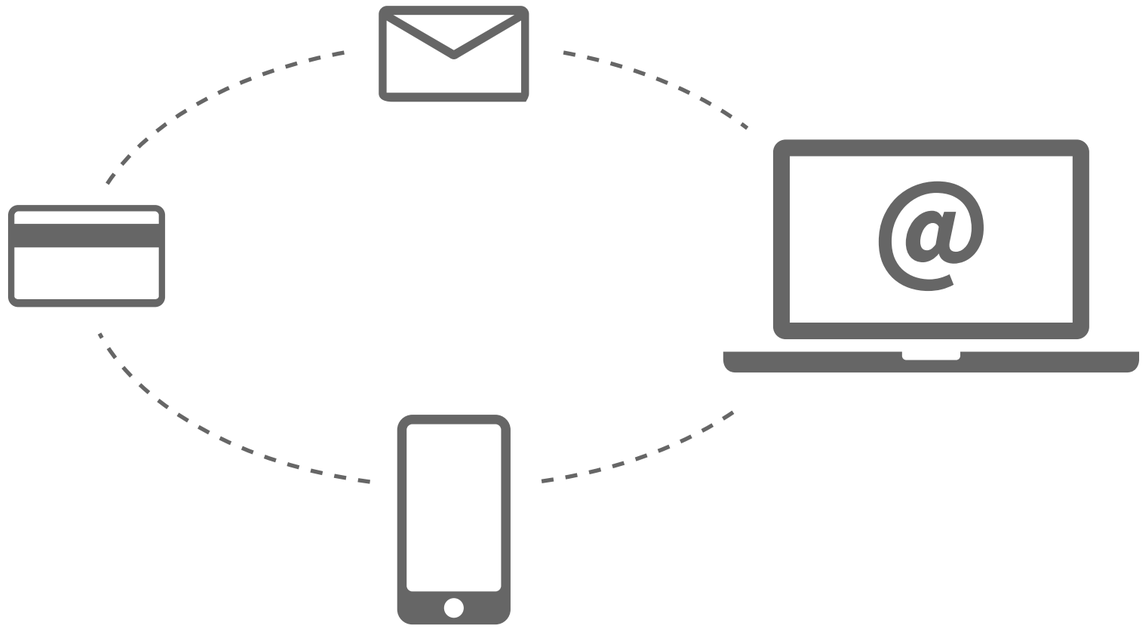
CTU del Tribunale di Macerata
ICT Security e Digital Forensics

Mobile + 39 333 1454144
E-Mail info@digital-evidence.it

INTERNET E LA POSSIBILITÀ DI ESSERE **COLPITI DA ATTACCHI INFORMATICI**

In un mondo sempre più interconnesso, dove internet è il **sistema più usato per lo scambio di informazioni**, per i commerci, per l'accesso alle grandi banche dati, per l'esecuzione di transazioni e disposizioni finanziarie, le possibilità per le PA e per le aziende di **essere colpite da attacchi informatici** o di cadere vittime di truffe telematiche sono sempre più alte.

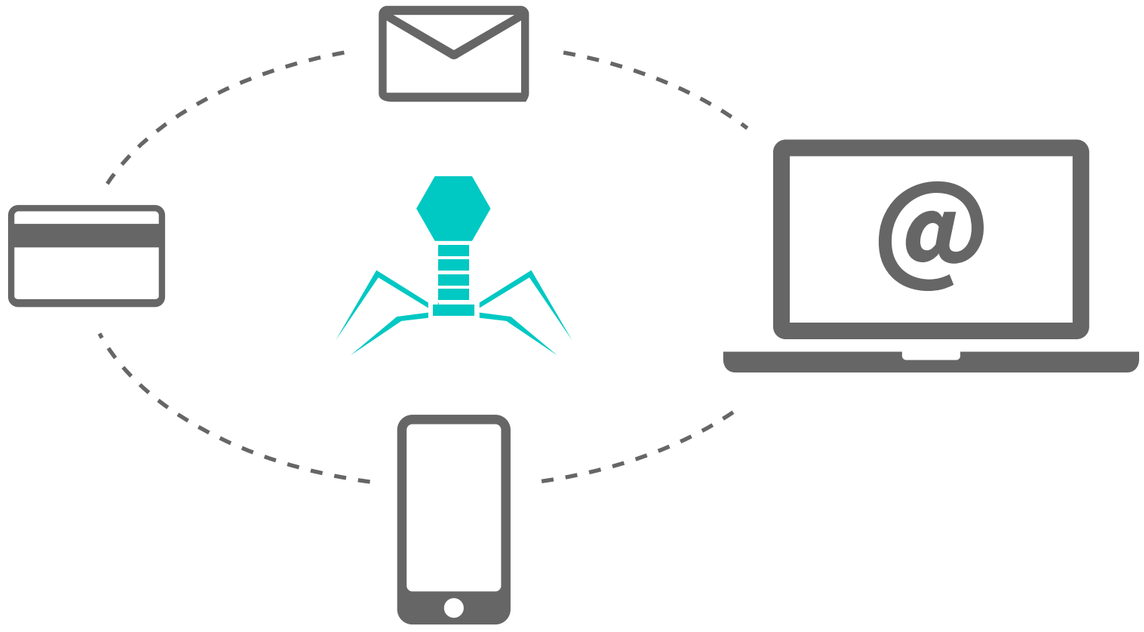
Siamo circondati da svariati dispositivi costantemente collegati alla rete che, se non ben amministrati, rischiano di far **trapelare informazioni riservate** e/o di non tutelare la nostra persona.



INTERNET E LA POSSIBILITÀ DI ESSERE **COLPITI DA ATTACCHI INFORMATICI**

In un mondo sempre più interconnesso, dove internet è il **sistema più usato per lo scambio di informazioni**, per i commerci, per l'accesso alle grandi banche dati, per l'esecuzione di transazioni e disposizioni finanziarie, le possibilità per le PA e per le aziende di **essere colpite da attacchi informatici** o di cadere vittime di truffe telematiche sono sempre più alte.

Siamo circondati da svariati dispositivi costantemente collegati alla rete che, se non ben amministrati, rischiano di far **trapelare informazioni riservate** e/o di non tutelare la nostra persona.



LA MANCANZA DI UN'ADEGUATA **SICUREZZA INFORMATICA** E DI UNA BUONA ANALISI DELL'**INFRASTRUTTURA DI RETE** POSSONO **CAUSARE GRAVI DANNI**.

ANALISI DELLA SITUAZIONE

DELLE FRODI INFORMATICHE

8.000.000.000 €

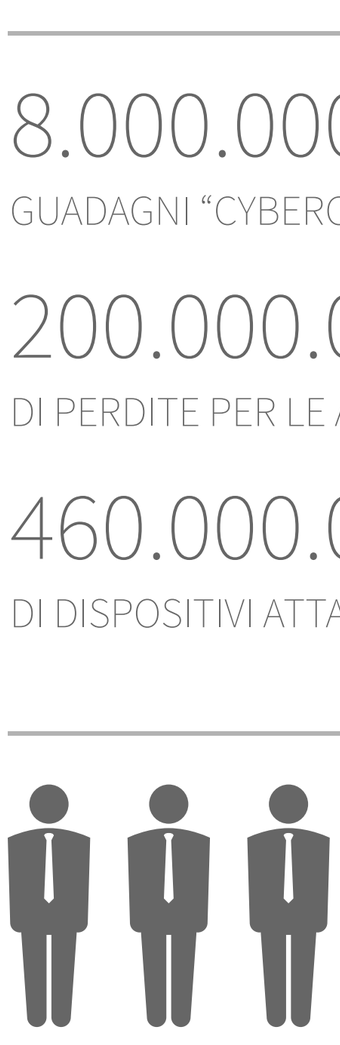
GUADAGNI “CYBERCRIME”

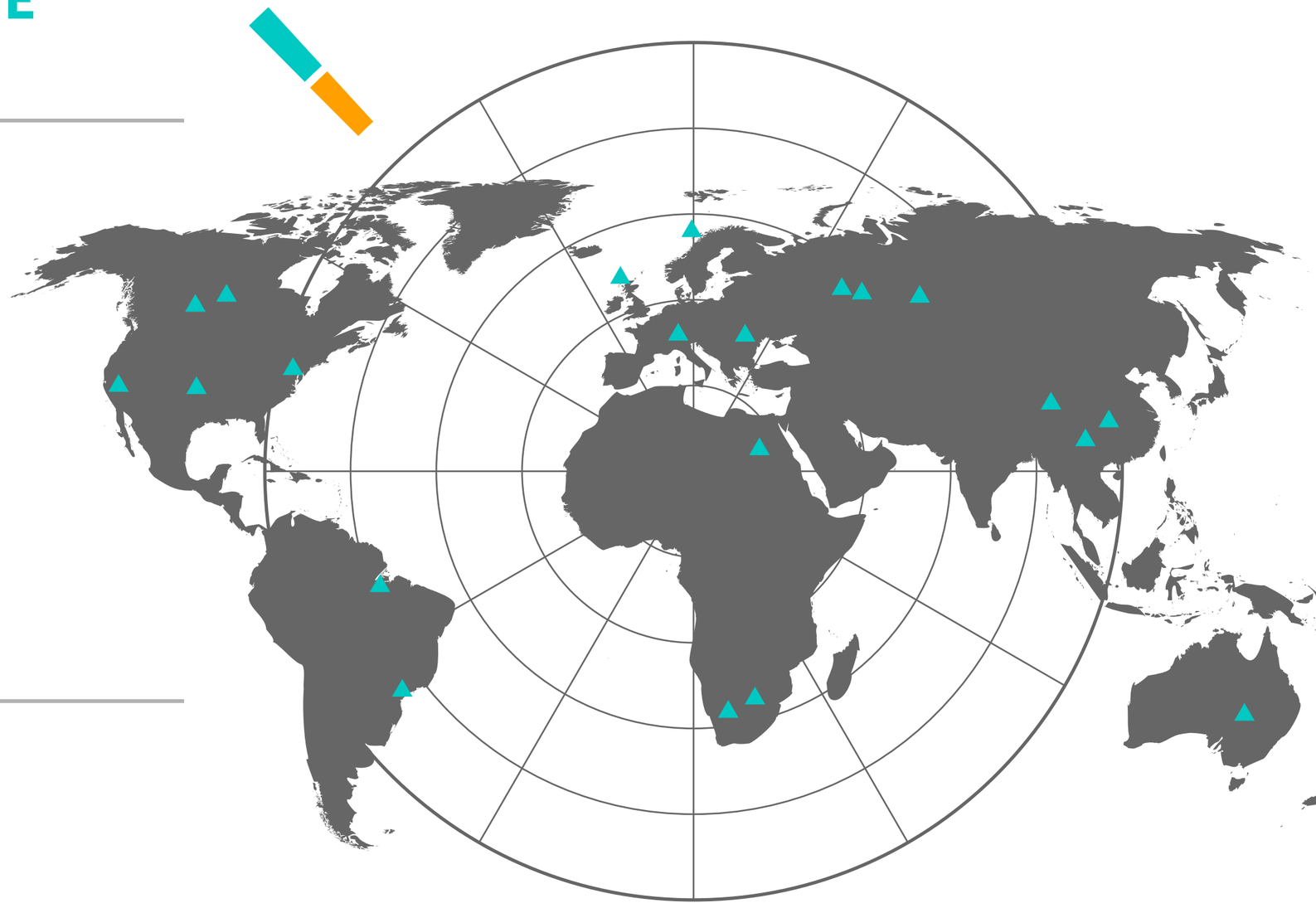
200.000.000 €

DI PERDITE PER LE AZIENDE ITALIANE

460.000.000

DI DISPOSITIVI ATTACCATI





ANALISI DELLA SITUAZIONE

DELLE FRODI INFORMATICHE

8.000.000.000 €

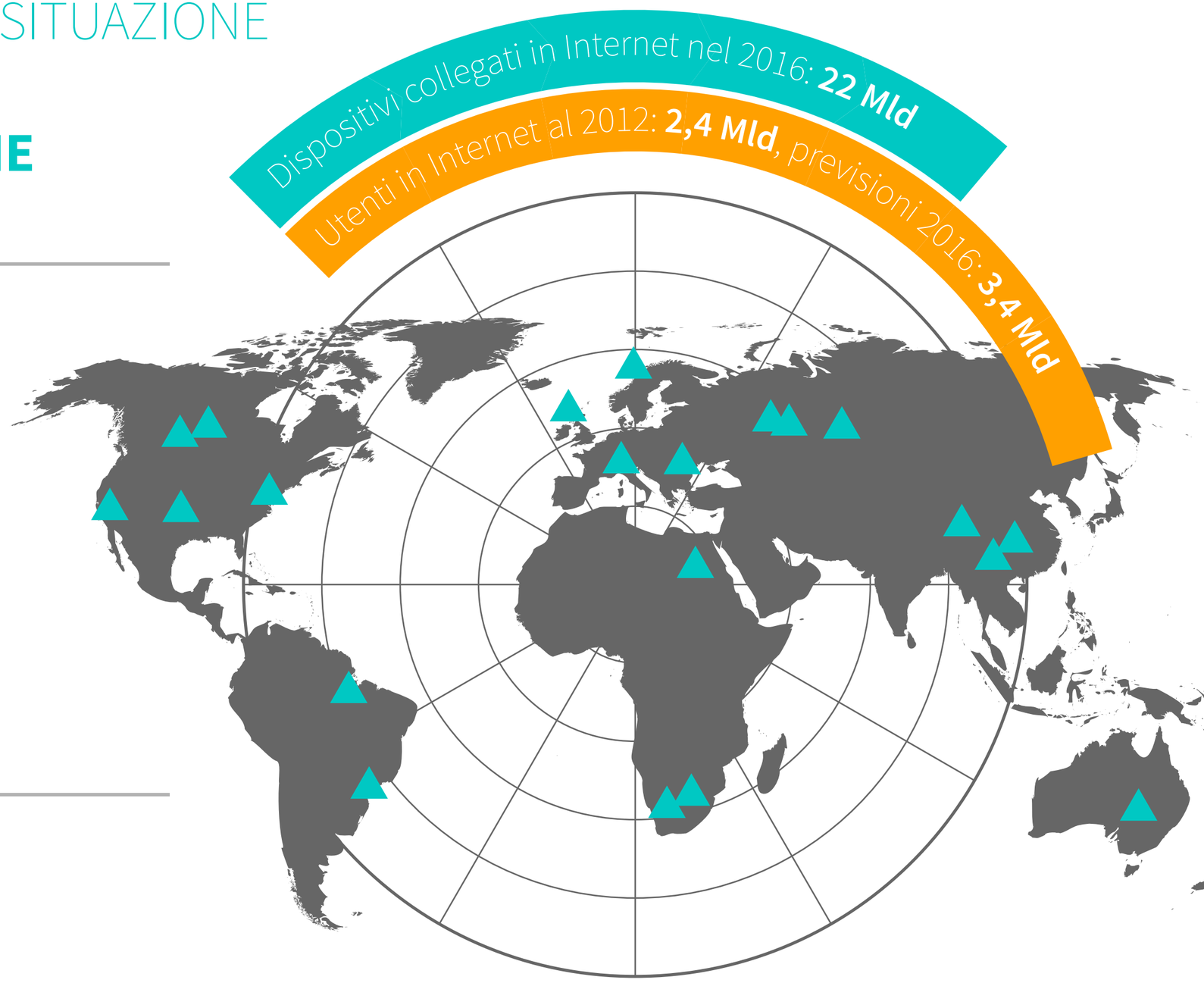
GUADAGNI “CYBERCRIME”

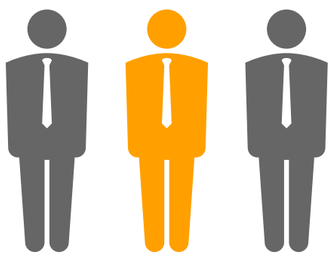
200.000.000 €

DI PERDITE PER LE AZIENDE ITALIANE

460.000.000

DI DISPOSITIVI ATTACCATI



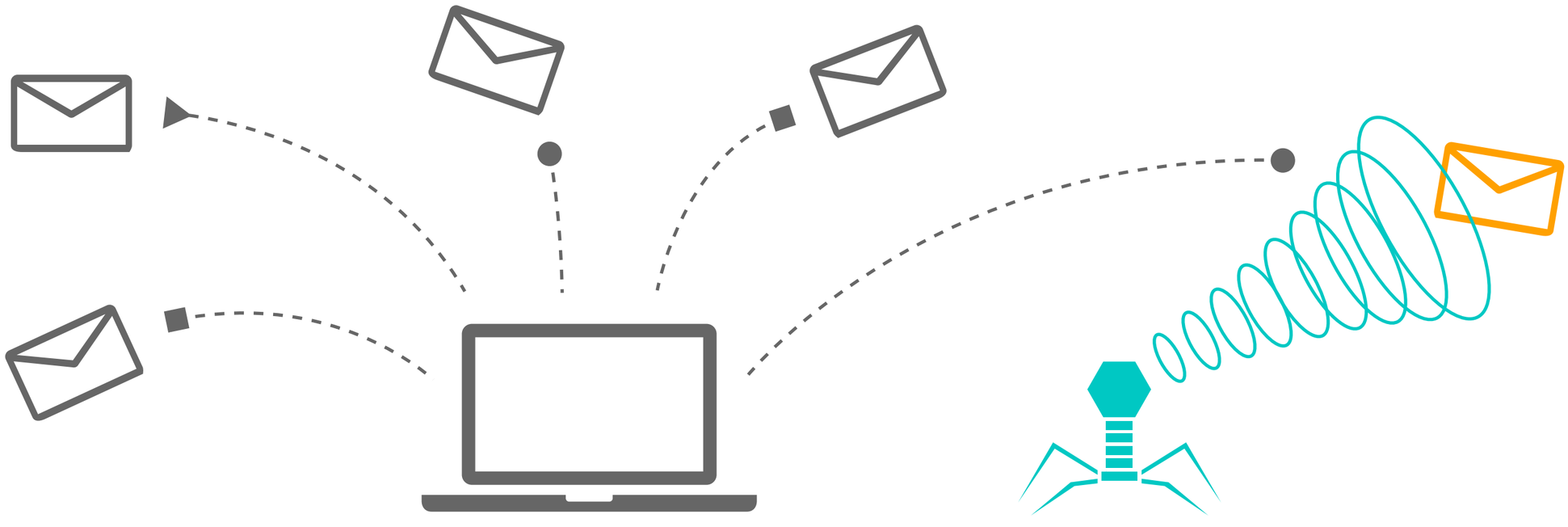


1 UTENTE SU 3 RISCHIA
IL FURTO DELLA PROPRIA
IDENTITÀ DIGITALE

I PERICOLI: RISCHI E POSSIBILI CONSEGUENZE **DELLE FRODI INFORMATICHE**

Tutti gli amministratori di aziende e i possessori di partita iva hanno su di loro la **responsabilità dei reati** commessi in azienda, compreso quello **digitale:** la mancanza di forme di **deresponsabilizzazione** può portare a ripercussioni legali.

Gli illeciti vengono compiuti a danno di **aziende ignare dei reali meccanismi informatici** e delle **possibili violazioni** che possono essere perpetrate tramite **falle dei sistemi** e usate per sottrarre dati sensibili causando notevoli danni: **LEGALI, ECONOMICI, DI IMMAGINE E TECNICI**.



I PERICOLI: RISCHI E POSSIBILI CONSEGUENZE **DELLE FRODI INFORMATICHE**

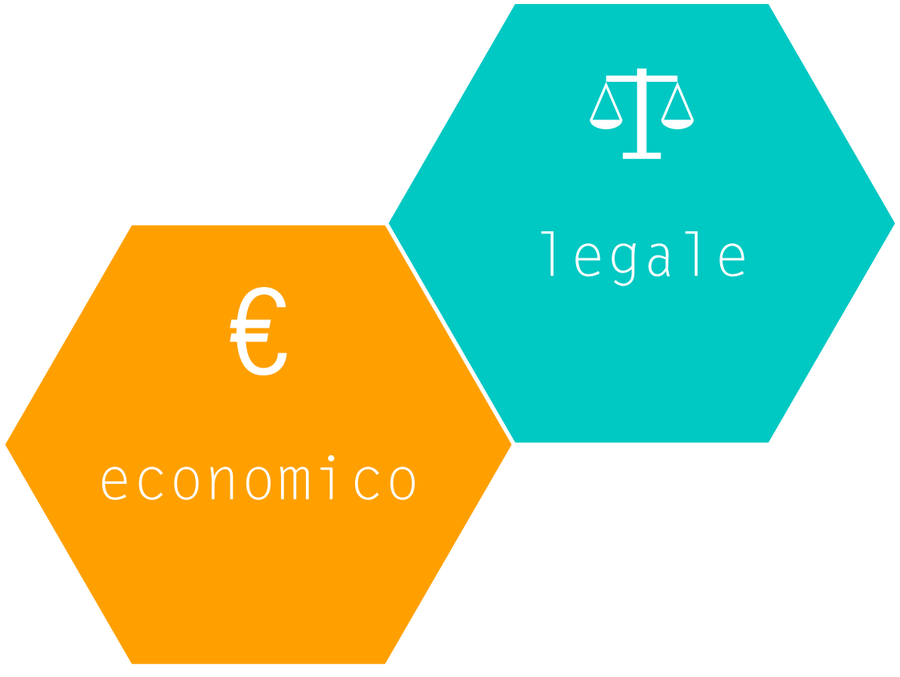
Danno legale

Sottrazione di dati da parte di dipendenti, collaboratori o estranei e pubblicazione degli stessi su internet.

Da una rete aziendale non protetta qualsiasi individuo può **commettere svariati reati** (truffe, stalking etc.) e in caso di controversia l'individuazione della prova informatica sarà praticamente impossibile.

Possibilità di essere **accusati per reati commessi da terzi**. La mancanza di una reale formazione dei dirigenti e degli operatori può far cadere l’azienda nella rete di possibili truffatori.

I PERICOLI: RISCHI E POSSIBILI CONSEGUENZE **DELLE FRODI INFORMATICHE**



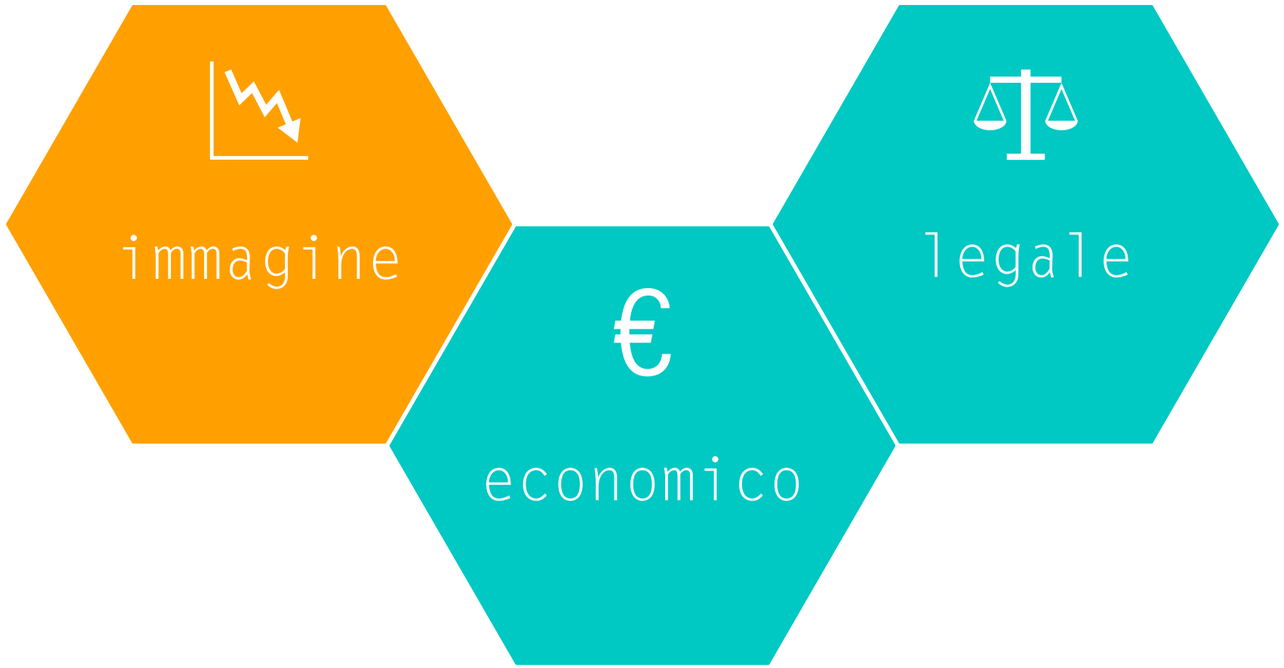
Danno economico

Sempre più spesso le aziende **perdono i loro dati** o gran parte di essi solo per errate configurazioni degli apparati.

Assistenze non ben monitorate consentono a truffatori anonimi di mettersi nelle migliori condizioni per effettuare **transazioni bancarie di migliaia di euro** a danno del titolare d'impresa.

La presenza di Virus può determinare la **perdita di denaro** agli utenti, che si vedranno anche costretti ad un **blocco del lavoro** per il ripristino dei processi compromessi.

I PERICOLI: RISCHI E POSSIBILI CONSEGUENZE **DELLE FRODI INFORMATICHE**



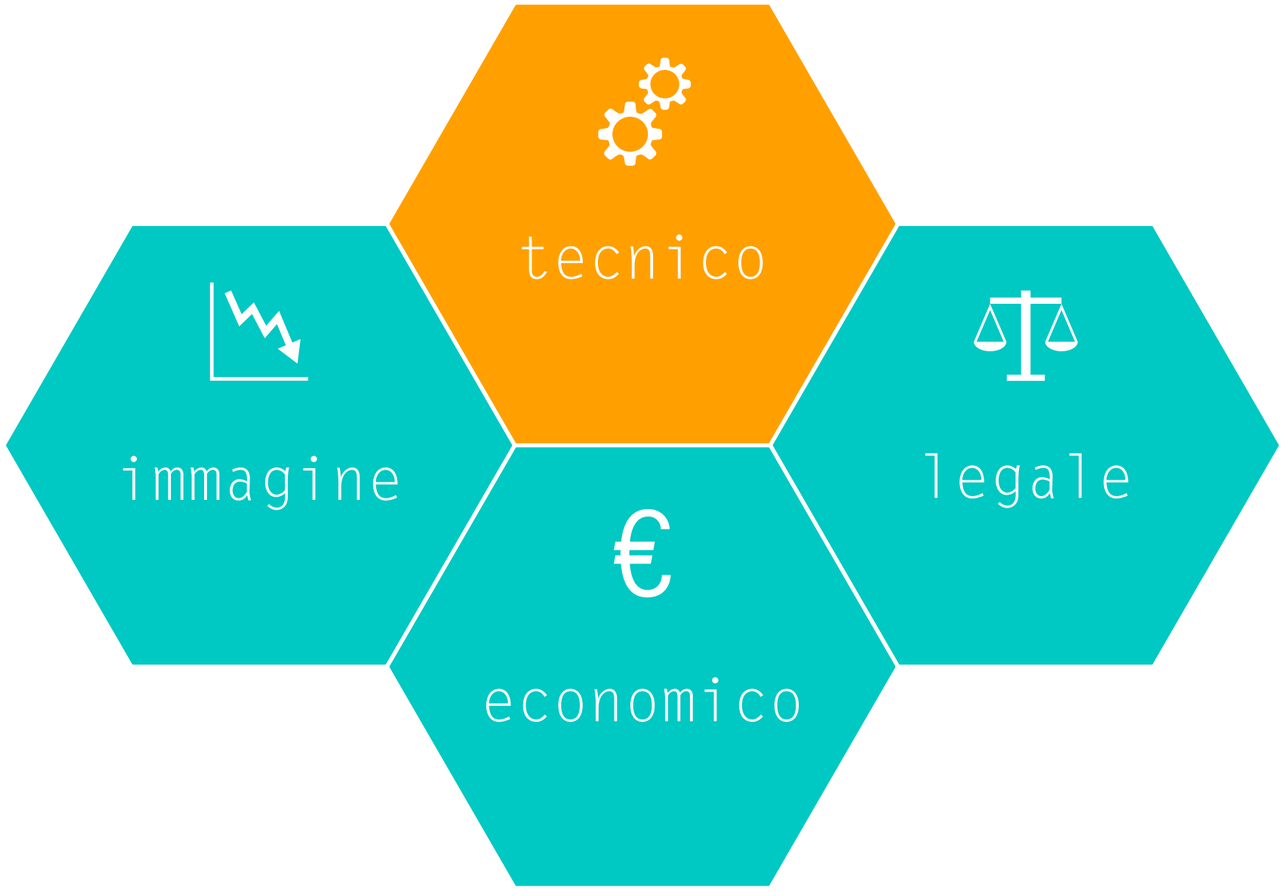
Danno di immagine

Sempre più i siti internet espongono parte del patrimonio economico e la **privacy dei clienti**.

Sottrazione e sostituzione dell'**identità digitale**, anche dei propri clienti (es. attraverso l'acquisizione di file per profilazione utente, anagrafiche etc.).

Furto di documentazione riservata come progetti, brevetti, segreti industriali (Casi Alpitour e NY Times).

I PERICOLI: RISCHI E POSSIBILI CONSEGUENZE **DELLE FRODI INFORMATICHE**



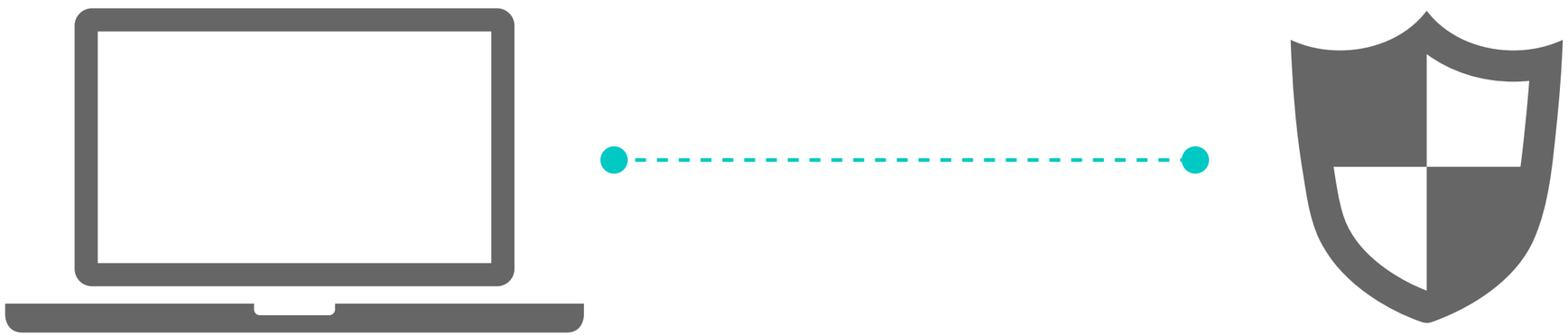
Danno tecnico

Le tecnologie vengono spesso inserite a livello aziendale senza una programmazione ben precisa e **senza una visione globale** dell'intero sistema: il risultato è un sistema informatico aziendale non centralizzato, che può determinare **possibili blocchi** della produttività.

LE SOLUZIONI:
COSA FARE E COME PROTEGGERSI

In azienda è fondamentale passare attraverso una politica di **classificazione del modus operandi** del dipendente rispetto all'uso del proprio dispositivo e adottare soluzioni tecnologiche che **filtrino** in modo intelligente gli accessi.

INDIVIDUARE LE INFORMAZIONI O DATI CHE NON DOVREBBERO MAI ESSERE ACCESSIBILI AL DI FUORI DEL PERIMETRO AZIENDALE, PUÒ **SALVARE DA RISCHI INUTILI** ED INCONTROLLABILI.



LE SOLUZIONI:
COSA FARE E COME PROTEGGERSI

In azienda è fondamentale passare attraverso una politica di **classificazione del modus operandi** del dipendente rispetto all'uso del proprio dispositivo e adottare soluzioni tecnologiche che **filtrino** in modo intelligente gli accessi.

INDIVIDUARE LE INFORMAZIONI O DATI CHE NON DOVREBBERO MAI ESSERE ACCESSIBILI AL DI FUORI DEL PERIMETRO AZIENDALE, PUÒ **SALVARE DA RISCHI INUTILI** ED INCONTROLLABILI.

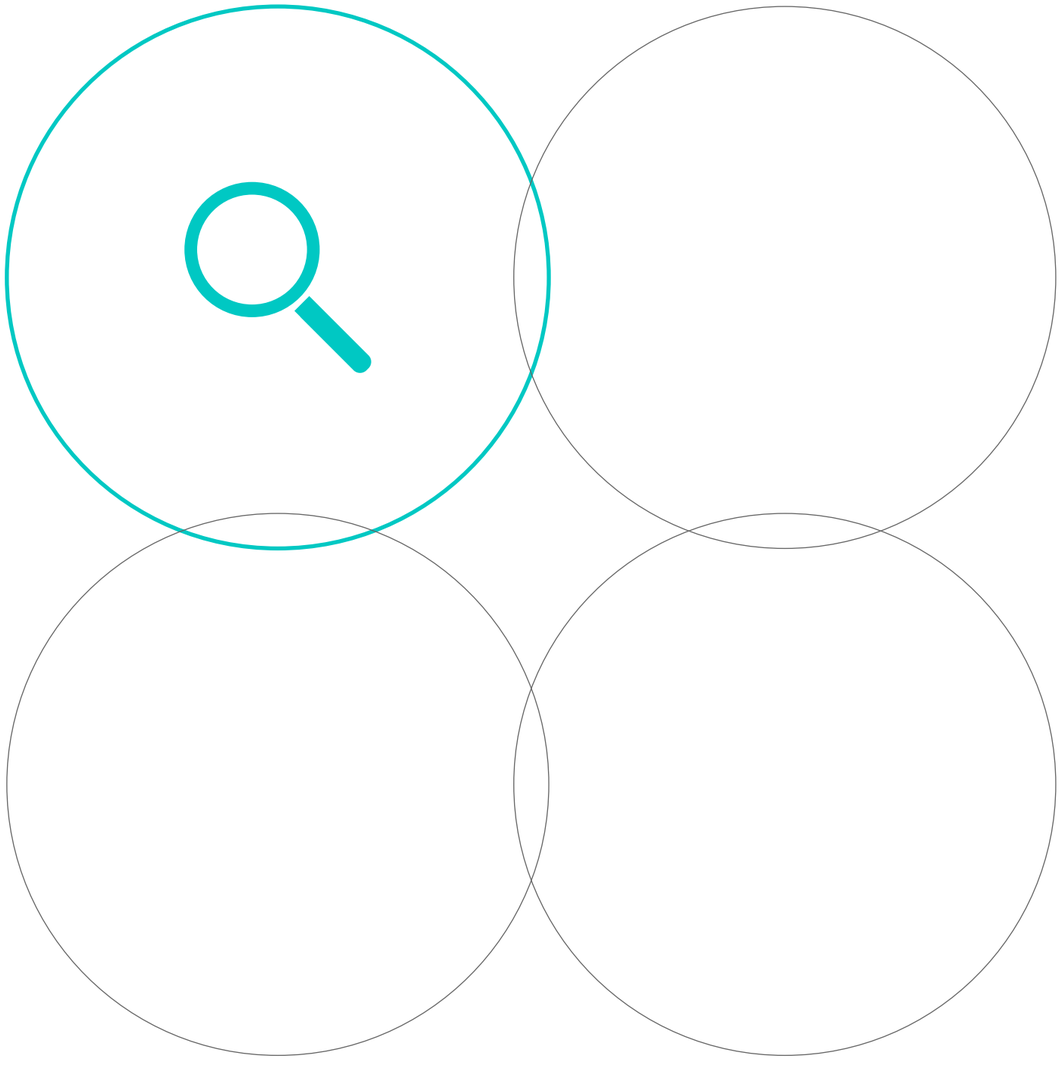
- Password
- Email aziendali e personali
- Programmi di contabilità
- Sistemi di Sicurezza
- SmartPhone
- Home Banking
- PEC Posta Elettronica Certificata
- Firma Digitale
- Software che si utilizzano in modo quotidiano
- Sito web, eCommerce
- Wardriving (intercettazione reti Wi-Fi)

LE SOLUZIONI:
FASI DELLA MESSA IN SICUREZZA DEI SISTEMI INFORMATICI

1 Analisi del rischio

Identificazione e studio dei processi aziendali e dei relativi flussi di dati.

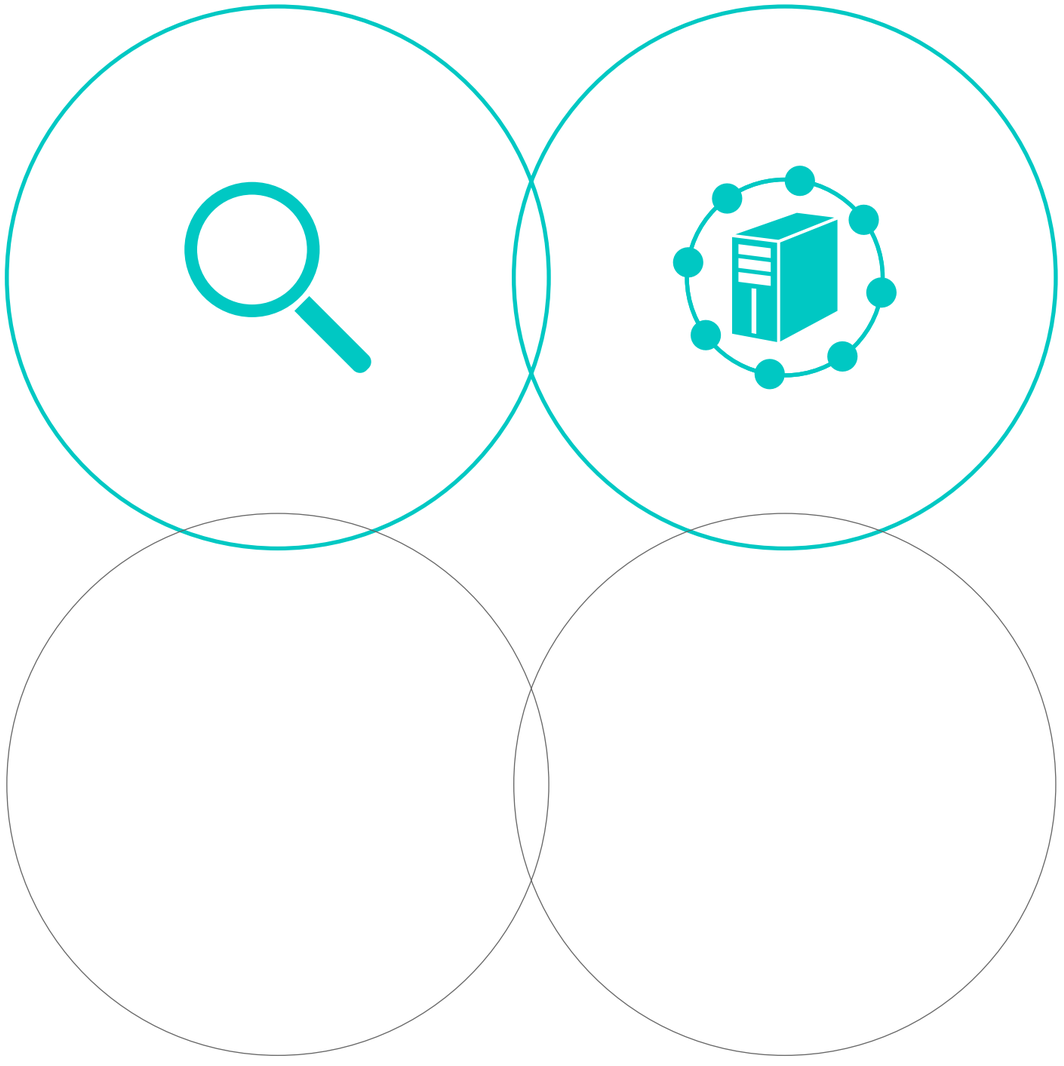
Studio dello **stato della sicurezza** in reti esistenti, identificazione e individuazione dei **punti deboli** e degli elementi di rischio.



LE SOLUZIONI:
FASI DELLA MESSA IN SICUREZZA DEI SISTEMI INFORMATICI

2 Protezione dei dati

Verifica del reale funzionamento dei sistemi di **salvataggio dati**, gestione dei Log, verifica dell'integrità delle Reti esistenti e delle Security Policy per l’accesso alle risorse.



LE SOLUZIONI:
FASI DELLA MESSA IN SICUREZZA
DEI SISTEMI INFORMATICI

3 Attuazione tecniche di difesa

Progettazione, installazione e configurazione di **sistemi di sicurezza passivi e attivi**: Firewall, Host / Network Intrusion Detection Systems, **Antivirus**. Sistemi di logging, laddove non siano stati implementati.

L'adozione di tali strumenti potrà **migliorare la difesa** dell'azienda in presenza di dipendenti / collaboratori infedeli e dimostrare un possibile reato commesso.

LE SOLUZIONI:
FASI DELLA MESSA IN SICUREZZA
DEI SISTEMI INFORMATICI

4 Verifica costante dei sistemi

Verifica dei sistemi di difesa della rete attraverso la **simulazione di attacchi informatici** per valutarne la resistenza alle **intrusioni esterne / interne reali.**

Analisi del traffico, della robustezza delle **password** e delle Security Policy.
Tali verifiche si estenderanno ai siti web e ai servizi di posta aziendali.

LE SOLUZIONI:
FASI DELLA MESSA IN SICUREZZA DEI SISTEMI INFORMATICI

L'attuazione delle Best practices della **Sicurezza Informatica** consentirà alle organizzazioni un maggior adeguamento a nuove forme di lavoro e nuovi processi di business in **totale tranquillità**.

Riduzione dei costi, comunicazioni più efficienti, massima dinamicità, miglior tutela e **pieno rispetto delle nuove direttive** europee / italiane (es. art. 231/01)

Effettivo guadagno in termini di tempo

Snellezza del sistema

Maggiore tutela legale e della propria immagine / identità digitale

Sicurezza Informatica e Digital Forensics

La **Sicurezza Informatica** è un processo evolutivo costante basato prima di tutto sulla **formazione** che ha il compito di **proteggere** adeguatamente la continuità, disponibilità e riservatezza delle risorse informative.

Un **processo evolutivo** non deve essere visto come obbligo di legge ma come un **fattore abilitante** per la vita stessa di qualsiasi organizzazione pubblica e privata.

Per tutti questi motivi che ogni nostro servizio deve tener conto di molteplici fattori, tra cui quello **legale**.

ROSSANO ROGANI

CTU del Tribunale di Macerata
ICT Security e Digital Forensics

Mobile + 39 333 1454144
E-Mail info@digital-evidence.it