CARNELUTTI LAW FIRM

Incident Management del Data Breach

Avv. Stefano Mele

Stefano Mele

Stefano Mele è *Partner* di Carnelutti Studio Legale Associato dove è il Responsabile del Dipartimento di *Diritto delle Tecnologie, Privacy e Cybersecurity*.

Dottore di ricerca presso l'Università degli Studi di Foggia, collabora presso le cattedre di Informatica Giuridica e Informatica Giuridica Avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

È membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano.

E' Presidente del "*Gruppo di lavoro sulla cyber-security*" della Camera di Commercio americana in Italia (AMCHAM), nonché membro del "*Tavolo Cyber Security*" di Regione Lombardia e dell'"*Advisory Board su Cyber Security*" di Assolombarda.

E' Coordinatore dell'Osservatorio *InfoWarfare e Tecnologie emergenti* dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli' ed è socio fondatore e Presidente dell'Associazione CyberPARCO.

È inoltre docente presso istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO, nonché autore di numerose pubblicazioni scientifiche e articoli sui temi della *cybersecurity*, *cyber intelligence*, *cyber terrorism* e *cyber warfare*.

Dal 2018, l'ENISA (European Network and Information Security Agency) lo ha inserito nella sua Lista di Esperti sui temi: "*EU Legal Framework on Data Protection and Privacy*" e "*Analysis of the Legal Framework relevant for Information Sharing*".

Nel 2014, la NATO lo ha inserito nella lista dei suoi *Key Opinion Leaders for Cyberspace Security*. Sempre nel 2014, la rivista *Forbes* lo ha inserito tra i 20 migliori *Cyber Policy Experts* al mondo da seguire in Rete.

Recapiti

Tel: +39 02 65585 1
Fax: +39 02 65585 415
smele@carnelutti.com

Aree di competenza

Diritto delle Tecnologie
Data Protection e Privacy
Cybersecurity
Intelligence

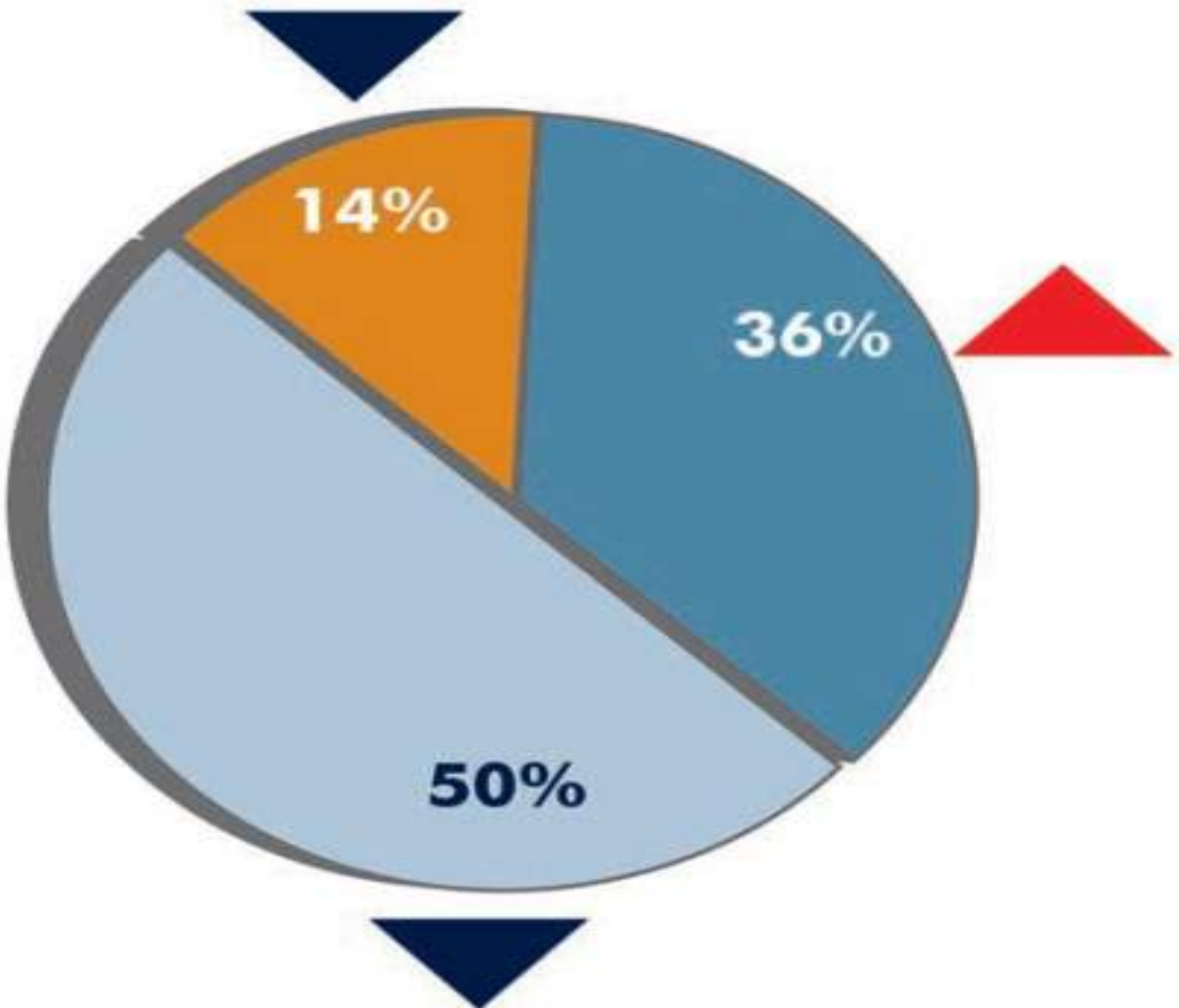
E non possiamo dimenticare la cosiddetta

Internet of Things..!


Target

ATTACCHI CYBER IN ITALIA IN BASE ALLA TIPOLOGIA DEGLI ATTORI OSTILI

(IN % SUL TOTALE 2017)

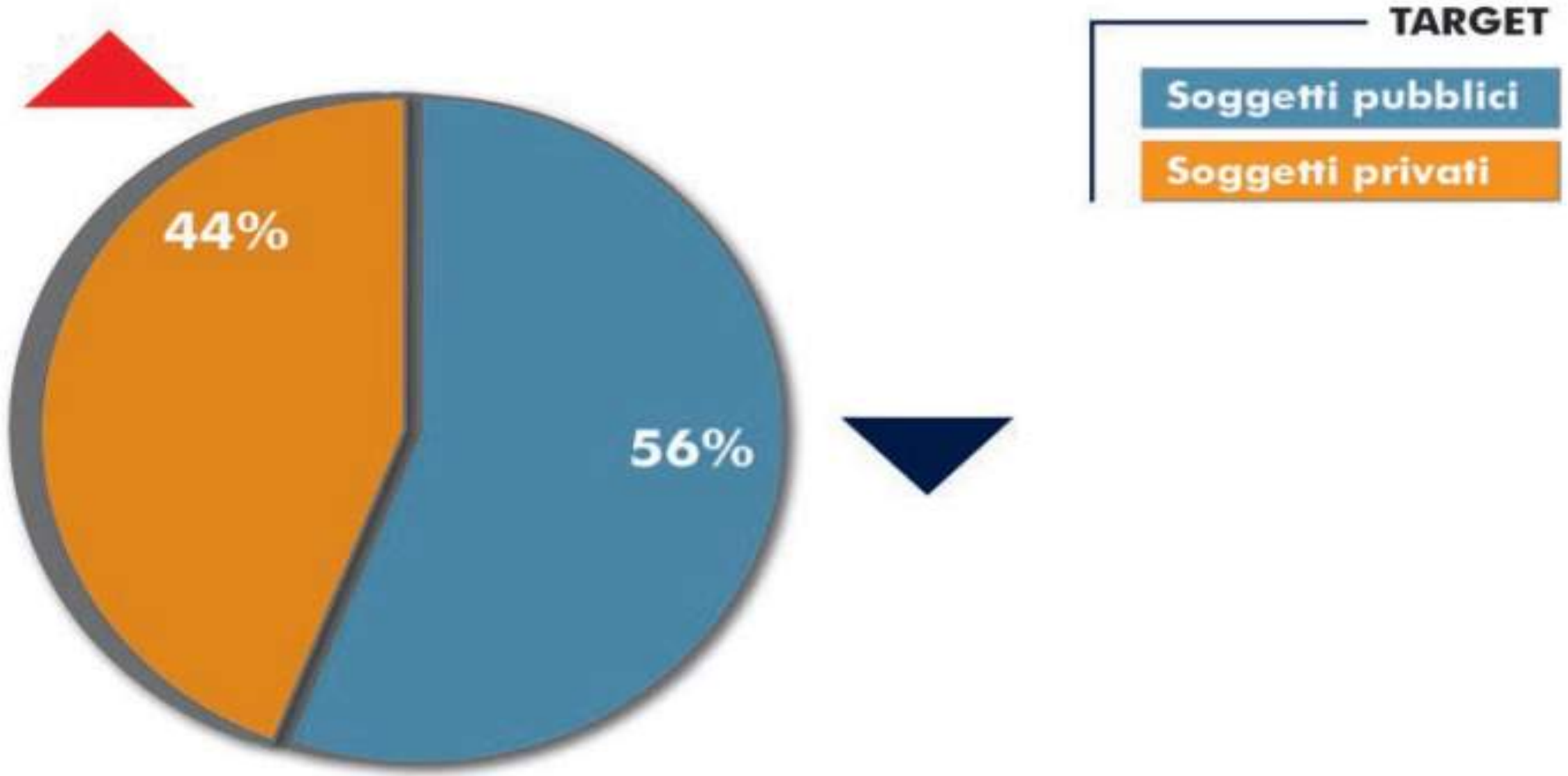


TIPOLOGIA

- Attori non meglio identificati
- Gruppi di *cyber-espionage*
- Gruppi hacktivisti

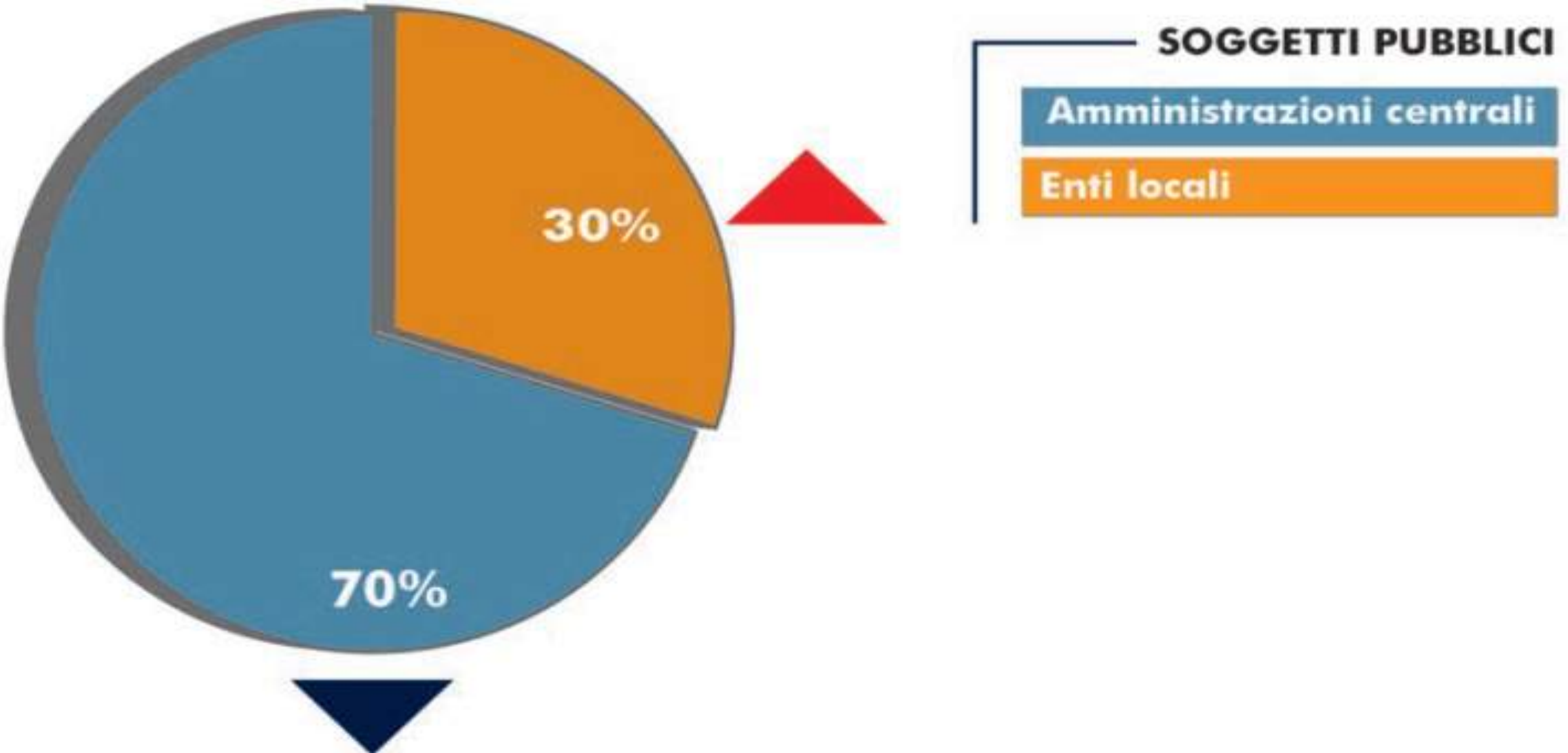
ATTACCHI *CYBER* IN ITALIA IN BASE ALLA TIPOLOGIA DEI *TARGET*

(IN % SUL TOTALE 2017)



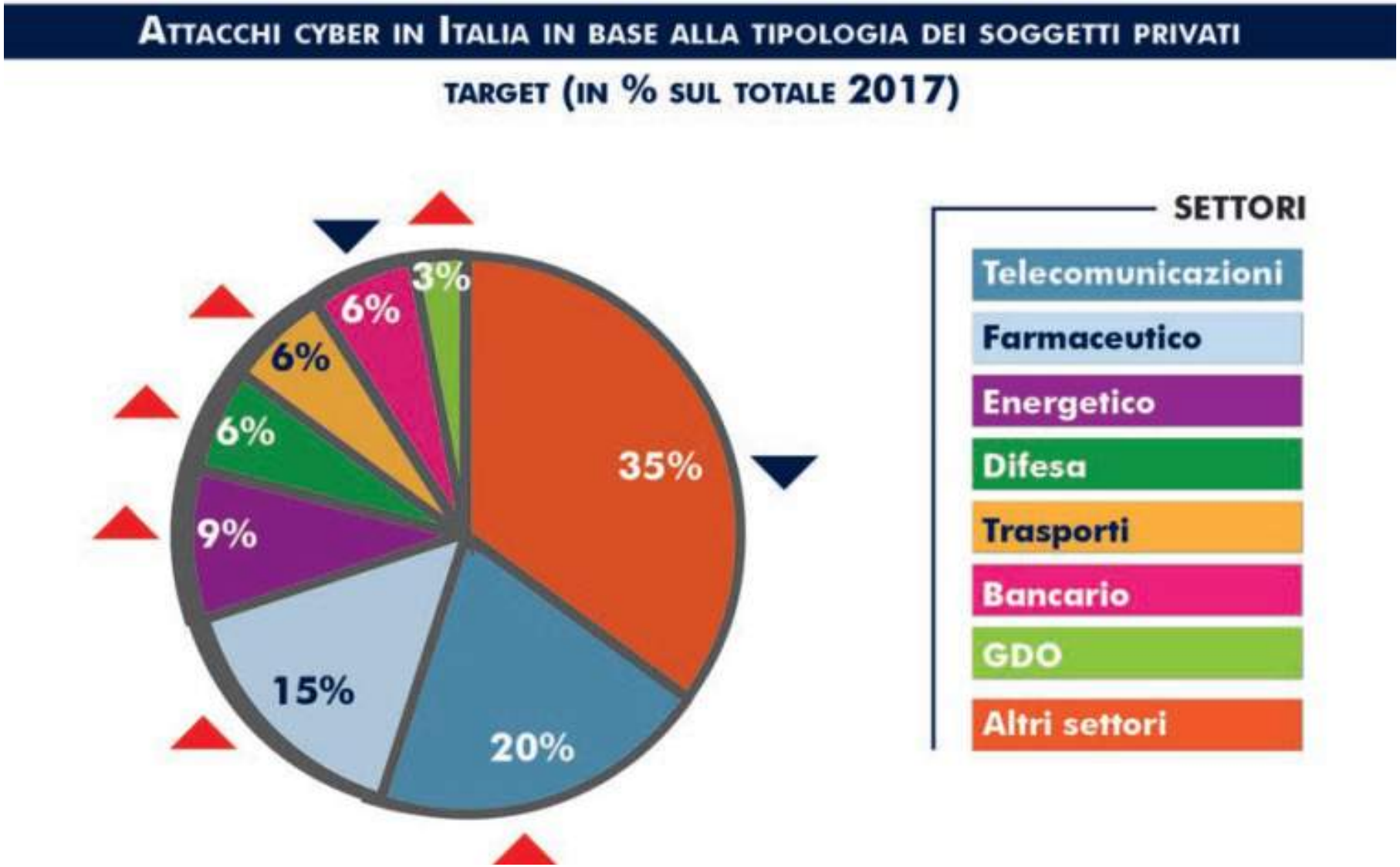
Attacchi cyber in Italia in base alla tipologia dei target pubblici

(in % sul totale 2017, dati aggregati)



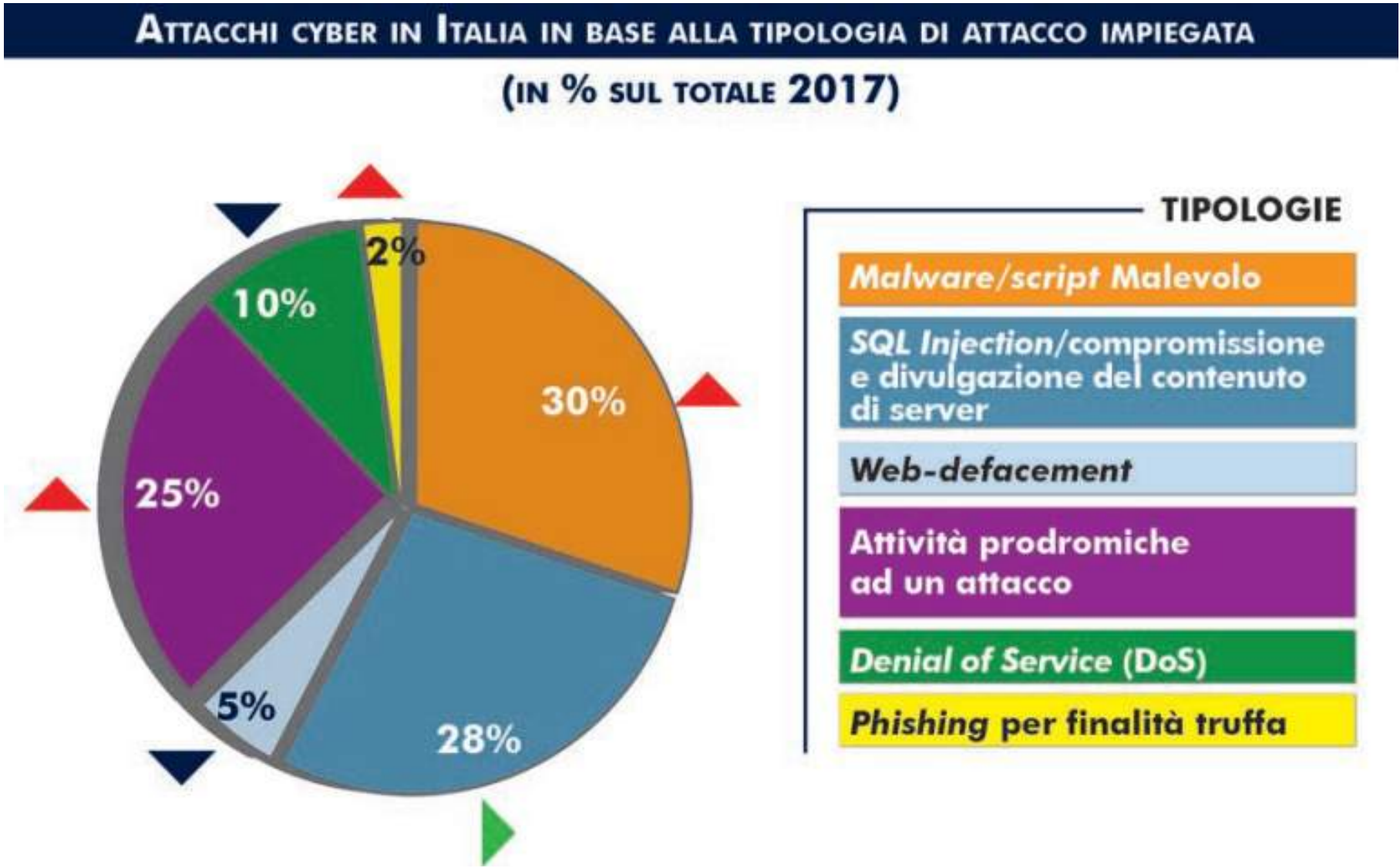
Analisi

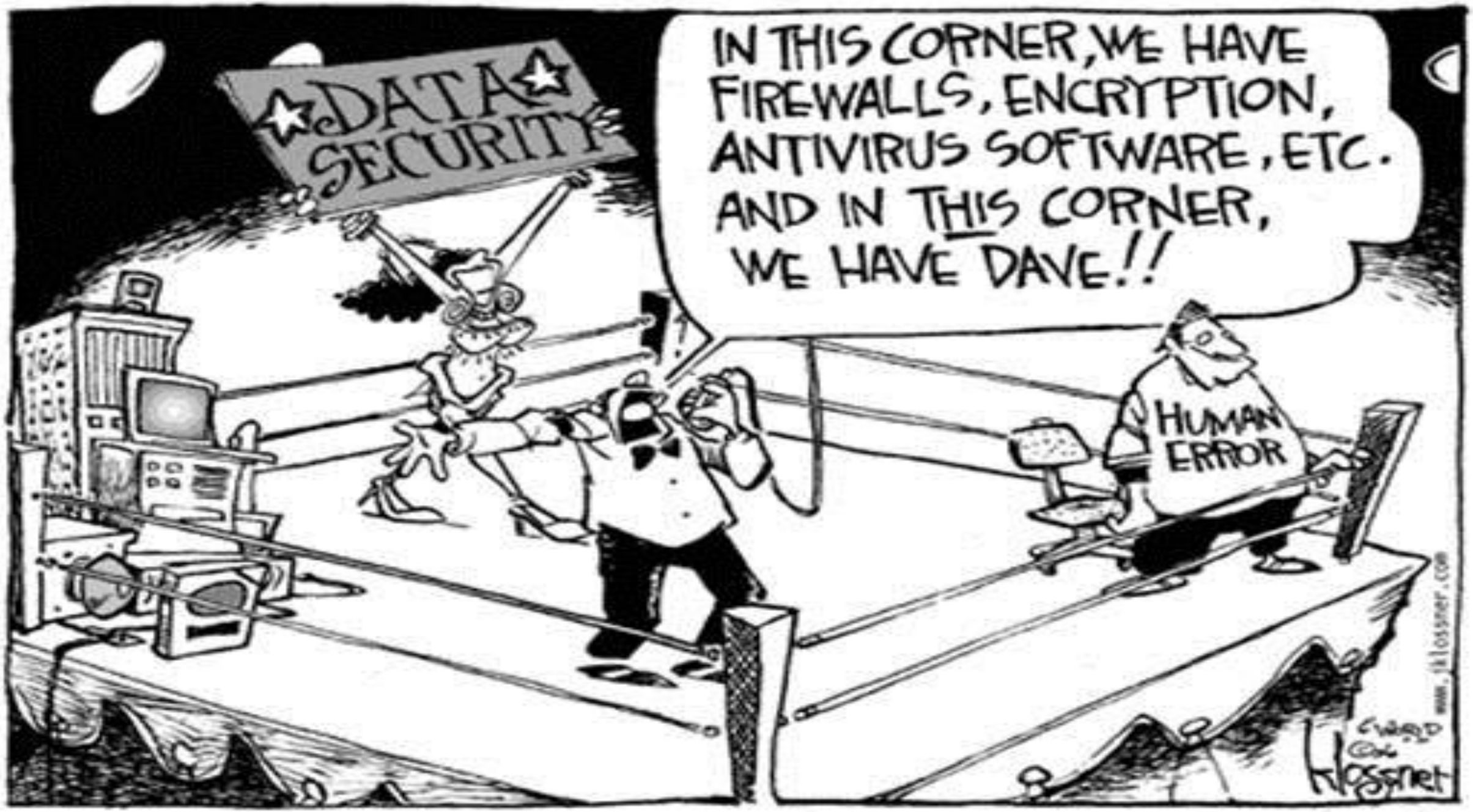
- ✓ emorragia informazioni industriali, commerciali o relative al know-how aziendale
- ✓ perdita di competitività e del vantaggio commerciale sul mercato
- ✓ danni all'immagine



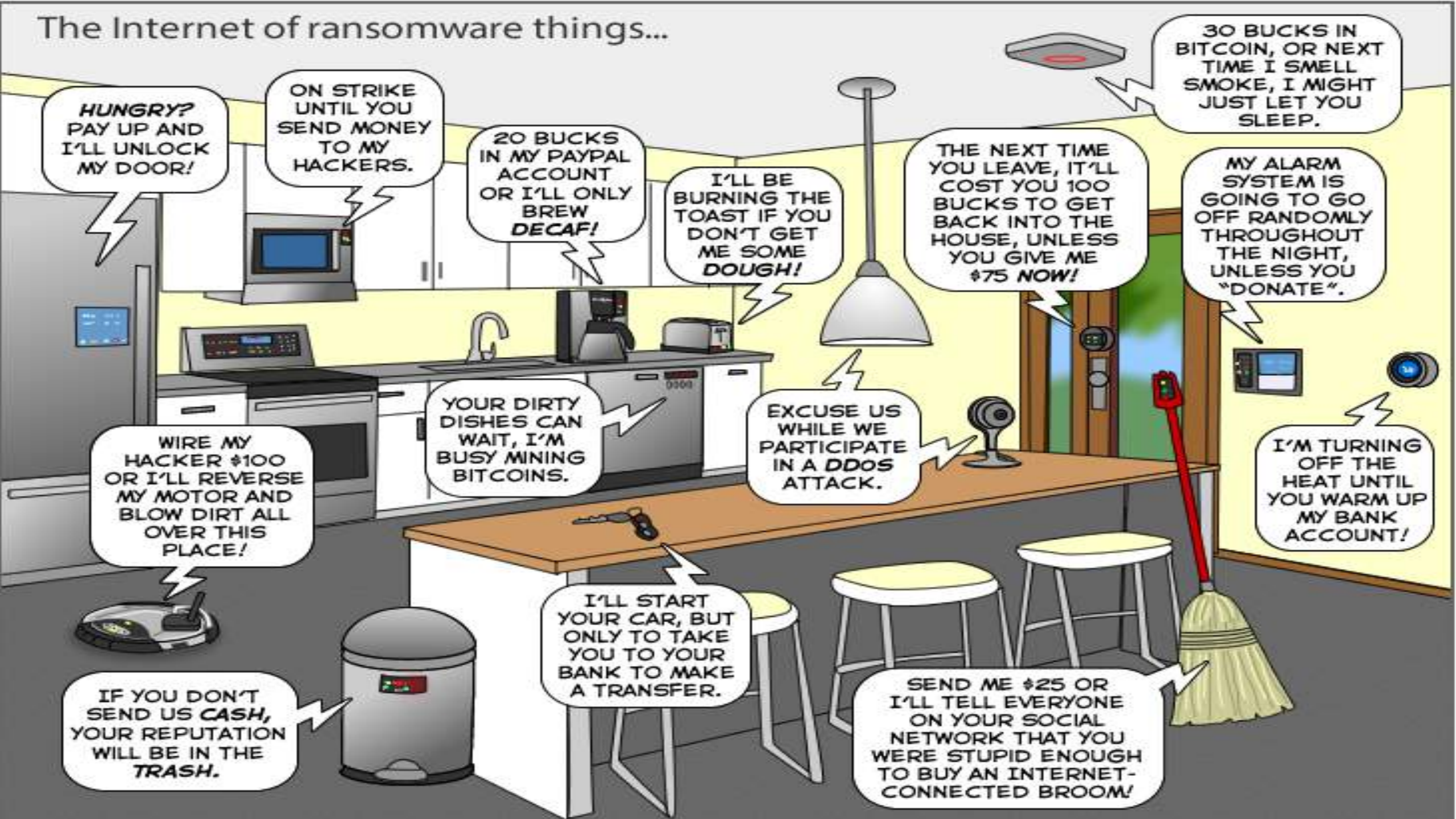
Analisi

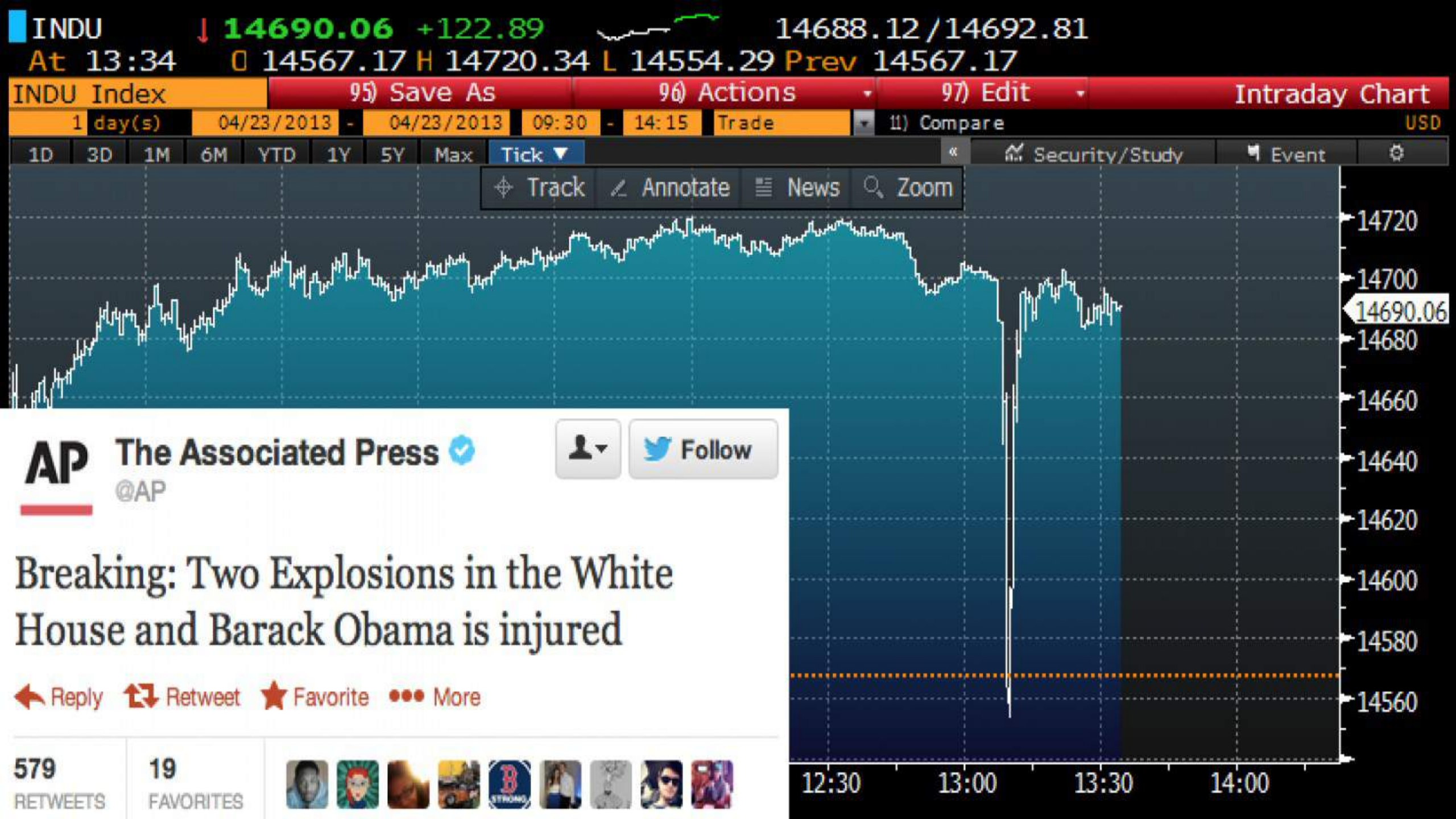
- ✓ cyber-crime/APT as-a-service
- ✓ ICS/SCADA con proiezione anche di danni cinetici
- ✓ internet of things (IoT)




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

Your money or your data

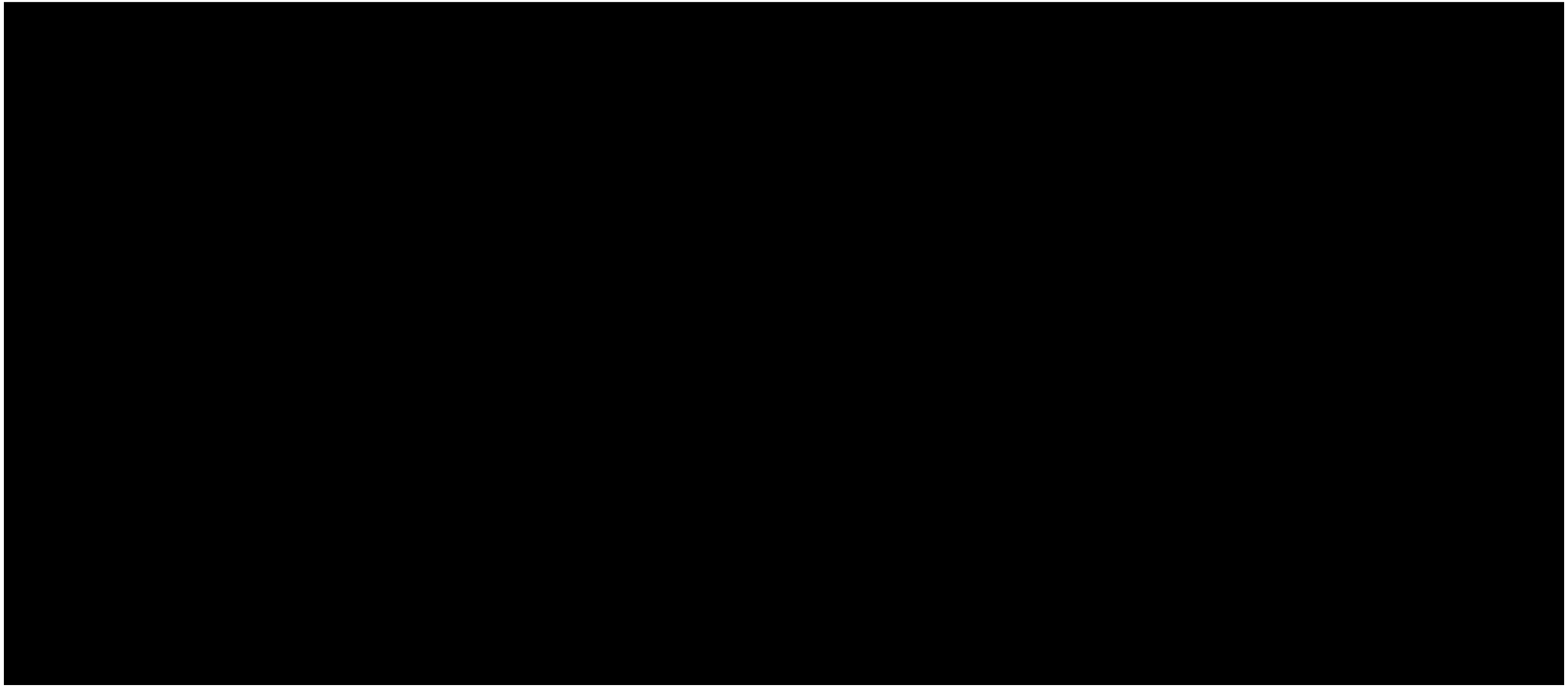

The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!


INDU
14690.06 +122.89
14688.12/14692.81
At 13:34
O 14567.17 H 14720.34 L 14554.29 Prev 14567.17
INDU Index
95) Save As
96) Actions
97) Edit
Intraday Chart
1 day(s)
04/23/2013 - 04/23/2013
09:30 - 14:15
Trade
11) Compare
USD
1D 3D 1M 6M YTD 1Y 5Y Max Tick
Security/Study
Event
Track
Annotate
News
Zoom
14720
14700
14690.06
14680
14660
14640
14620
14600
14580
14560
12:30
13:00
13:30
14:00
The Associated Press
@AP
Follow
Breaking: Two Explosions in the White House and Barack Obama is injured
Reply
Retweet
Favorite
More
579
RETWEETS
19
FAVORITES


13 HEURES
DAVID DELOS
JOURNALISTE TV5 MONDE


verizon
YAHOO!

Privacy..?



Un cambio di rotta..

Il Parlamento Europeo – in data 14 Aprile 2016 – ha approvato definitivamente il nuovo Regolamento concernente la "tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati" ("Regolamento Europeo"), volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la Direttiva 95/46/CE2, che ha portato in Italia all'adozione del vigente D.lgs. 30 giugno 2003 n. 196

Il Regolamento Generale sulla Protezione dei Dati

Definizione di Dato Personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Il Regolamento Generale sulla Protezione dei Dati

Definizione di Trattamento di Dati Personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Il Regolamento Generale sulla Protezione dei Dati

Protezione per impostazione predefinita (*Data Protection by Default*)

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento

Durante l'attività di verifica, pertanto, dovranno essere valutate: la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità

Il Regolamento Generale sulla Protezione dei Dati

Protezione dei dati fin dalla progettazione (*Data Protection by Design*)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

Le misure di sicurezza da applicare al trattamento

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Le misure di sicurezza da applicare al trattamento

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati

Le misure di sicurezza da applicare al trattamento

- ✓ la **pseudonimizzazione** e la **cifratura** dei dati personali
- ✓ la capacità di **assicurare su base permanente** la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- ✓ la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- ✓ una procedura per **testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Violazione dei dati personali

Violazione dei dati personali:

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

Violazione dei dati personali

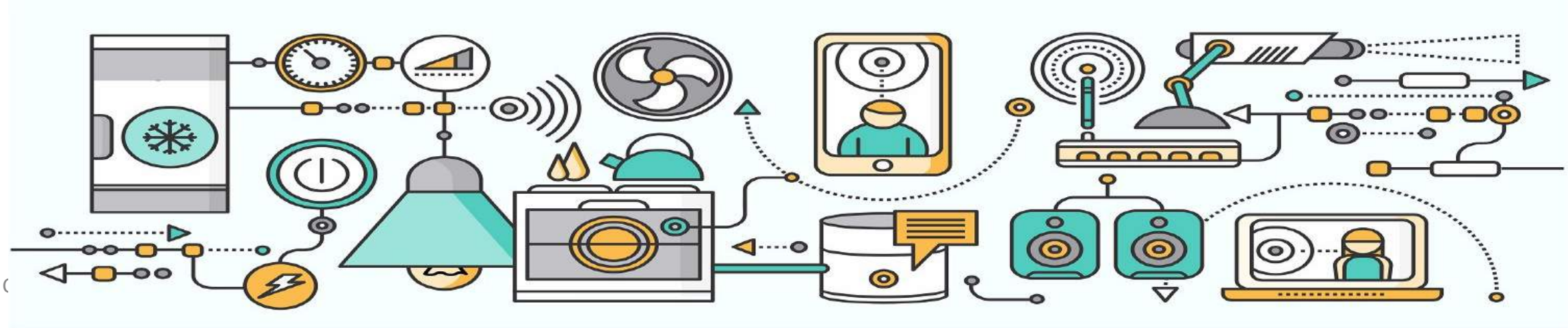
Violazione dei dati personali -- Esempi:

- accesso da parte di terzi non autorizzati;
- azione deliberata o accidentale (o inerzia) da parte del Titolare o del Responsabile;
- invio di dati personali a un destinatario errato;
- dispositivi informatici contenenti dati personali persi o rubati;
- alterazione dei dati personali senza permesso;
- perdita di disponibilità di dati personali.

Notifica all'Autorità di controllo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche

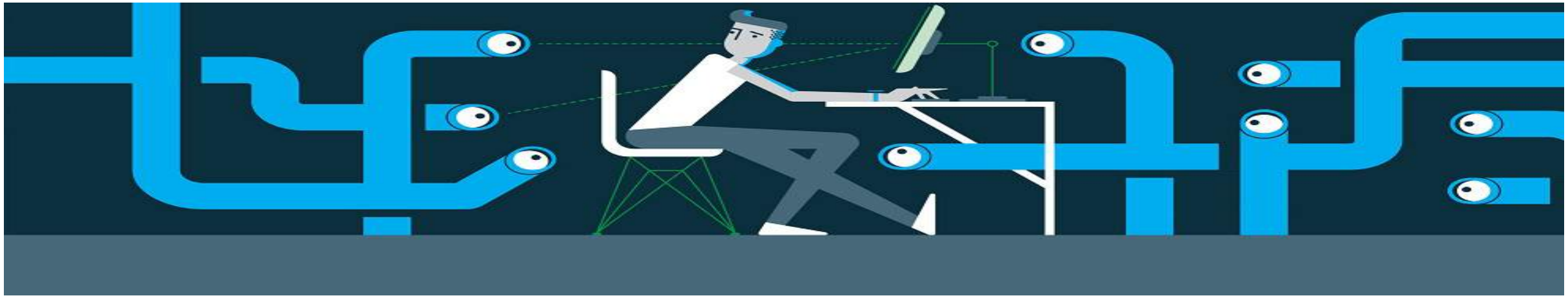
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo



Notifica all'Autorità di controllo

Il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio

Tale documentazione consente all'Autorità di controllo di verificare il rispetto di quanto previsto dalla normativa



Notifica all'Autorità di controllo

Notifica all'Autorità di controllo -- Esempio:

- **Il furto di un database di clienti, i cui dati possono essere utilizzati per commettere frodi attraverso le identità sottratte, deve essere notificato, dato l'impatto che questo potrebbe avere su quegli individui che potrebbero subire perdite finanziarie o altre conseguenze. Contestualmente, di norma, non è necessario notificare all'Autorità, ad esempio, la perdita o l'alterazione inappropriata di una rubrica del personale**

Contenuto della notifica

La notifica deve almeno:

a. **descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione**
b. **comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni**
c. **descrivere le probabili conseguenze della violazione dei dati personali**
d. **descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi**

Ulteriori informazioni e obbligo di collaborazione

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo

Il Responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione

Misure di sicurezza e attività di verifica sui Responsabili del trattamento

- **Non più misure minime di sicurezza, ma solo misure adeguate**
- **La *Designazione del Responsabile del trattamento***
- **I *Self Risk Assessment***
- **L'invio di documentazione per *assessment* esterni a cui i fornitori si devono sottoporre**
- **Attività di verifica *on-site***

Responsabile del Trattamento

Elementi fondamentali in una designazione del Responsabile del Trattamento

Individuazione della società designata

Istruzioni di trattamento del Titolare:

1. Doveri generici

2. Doveri di collaborazione con il Titolare

3. Astenersi dal compiere altri trattamenti

4. Trattamento di dati fuori Paesi EU

5. Adottare misure sicurezza adeguate del Titolare

6. Obblighi di comunicazione in caso Data Breach

7. Sub-Responsabili del trattamento

8. Collaborare per esercizio diritti Interessati

9. Consentire controlli e ispezione del Titolare o DPO

Ulteriori informazioni e obbligo di collaborazione

Ulteriori informazioni -- Esempio:

- **La società (Titolare del trattamento) rileva un'intrusione all'interno della propria rete e capisce che i file contenenti i dati personali sono stati acceduti, pur non sapendo ancora come l'autore dell'attacco abbia ottenuto l'accesso, in che misura è stato effettuato l'accesso ai dati o se l'autore dell'attacco abbia o meno copiato anche i dati dal tuo sistema. La società deve avvertire l'Autorità entro 72 ore dalla presa di conoscenza della violazione, spiegando che non si dispone ancora di tutti i dettagli pertinenti, ma che si prevede di ottenere i risultati delle indagini entro pochi giorni. Una volta conosciuti i dettagli dell'incidente, la società deve prontamente fornire all'Autorità maggiori informazioni sulla violazione**

Ulteriori informazioni e obbligo di collaborazione

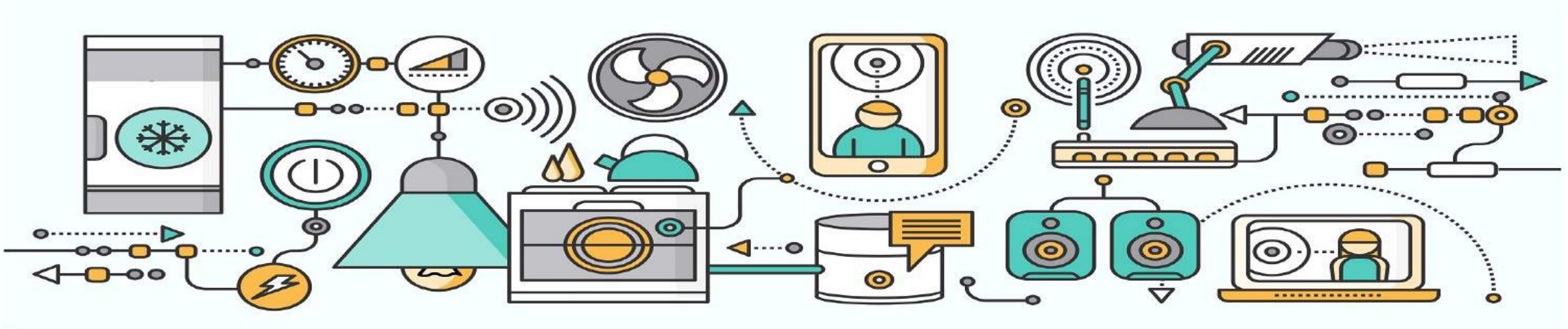
Obbligo di collaborazione -- Esempio:

- **La società (Titolare del trattamento) ha un contratto con un'azienda di servizi IT (Responsabile del trattamento) che prevede la raccolta e l'archiviazione dei record dei clienti. L'azienda IT rileva un attacco informatico alla sua rete, che ha come conseguenza l'accesso illegale a dati personali relativi ai suoi clienti. Trattandosi di una violazione dei dati personali, l'azienda IT deve notificare tempestivamente al Titolare che la violazione è avvenuta. A sua volta, il Titolare deve notificare all'Autorità**

Notifica all'Interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali



Valutazione della violazione (I)

Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:

- **Tipo di violazione: la gravità del rischio può essere diversa a seconda che venga violata la confidenzialità dei dati, la loro disponibilità o l'integrità di questi**
- **Tipo di dati oggetto del Data Breach: più i dati sono «sensibili», e quindi appartenenti a categorie particolari, e più alto sarà il rischio per gli Interessati**
- **Facilità con la quale l'Interessato può essere identificato: in alcuni casi, infatti, a seguito di una violazione, tale attività può risultare particolarmente semplice**
- **Gravità delle conseguenze per gli Interessati: a seconda della natura dei dati violati, le conseguenze possono essere particolarmente serie**

Valutazione della violazione (II)

Nella valutazione, il Titolare del trattamento deve tenere conto della probabilità del rischio e della sua gravità basandosi su:

- **Caratteristiche peculiari degli Interessati: alcune categorie di soggetti, ad esempio i bambini, rischiano di essere maggiormente esposti in caso di violazione**
- **Numero di individui Interessati: maggiore è il numero di soggetti, maggiori rischiano di essere le implicazioni di un'eventuale Data Breach. Anche in questo caso, però, è necessario valutare le circostanze, in quanto, in alcuni casi, la violazione può comportare gravi rischi anche per il singolo**
- **Eventuali caratteristiche del Titolare del trattamento: anche questo è un elemento da tenere in considerazione, infatti, a seconda del tipo di attività svolta, la violazione può essere più o meno grave**

Contenuto della notifica

La notifica deve almeno:

a. […]

b. comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni

c. descrivere le probabili conseguenze della violazione dei dati personali

d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Quando NON è richiesta la notifica

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a. **il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura**

b. **il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati**

c. **detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia**

Attività dell'Autorità di controllo

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni è soddisfatta


Q&A