IC
InfoCamere
Innovare è Crescere

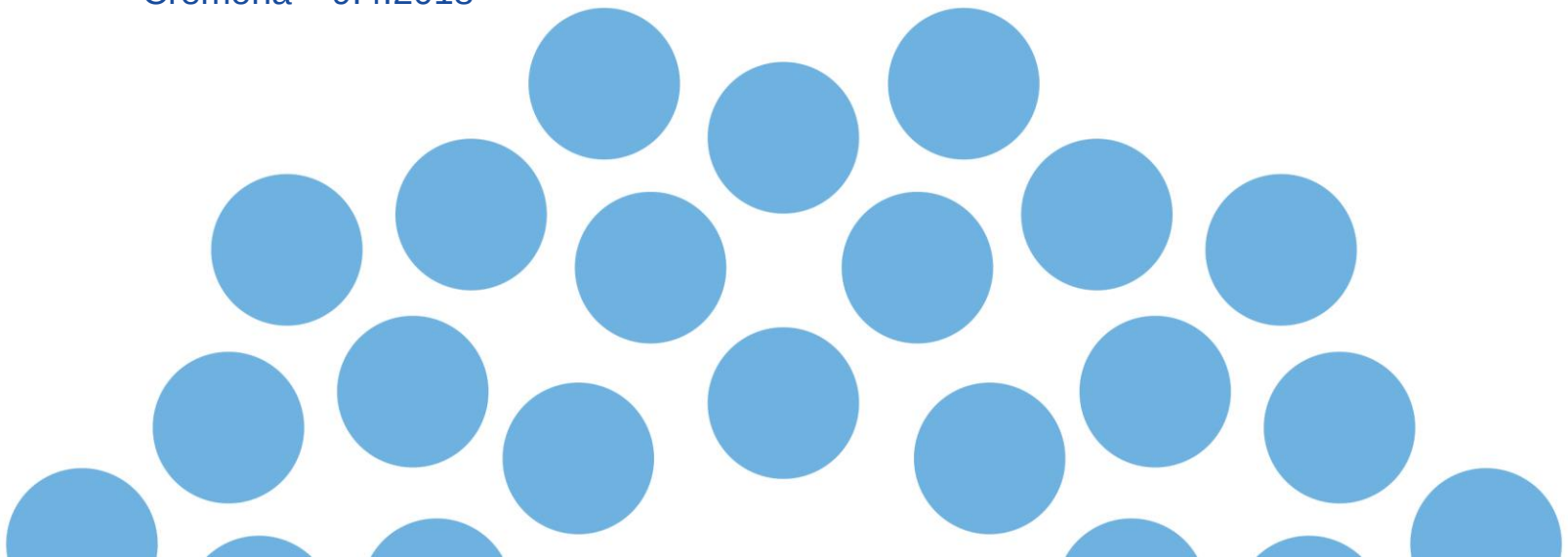
CYBER-SECURITY e PRIVACY

Sicurezza delle informazioni e nuova normativa sulla protezione dei dati

Paolo Grigoletto

Sicurezza delle informazioni e privacy

Cremona – 9.4.2018



InfoCamere

Chi siamo

801
Dipendenti

66 ML
Transazioni giornaliere

145
Servizi con SLA 99,9%

1 SEDE LEGALE A ROMA

1 DATACENTER A PADOVA

1 DATACENTER A MILANO

TUTTE LE CAMERE DI COMMERCIO IN RETE

235
SEDI STACCATE

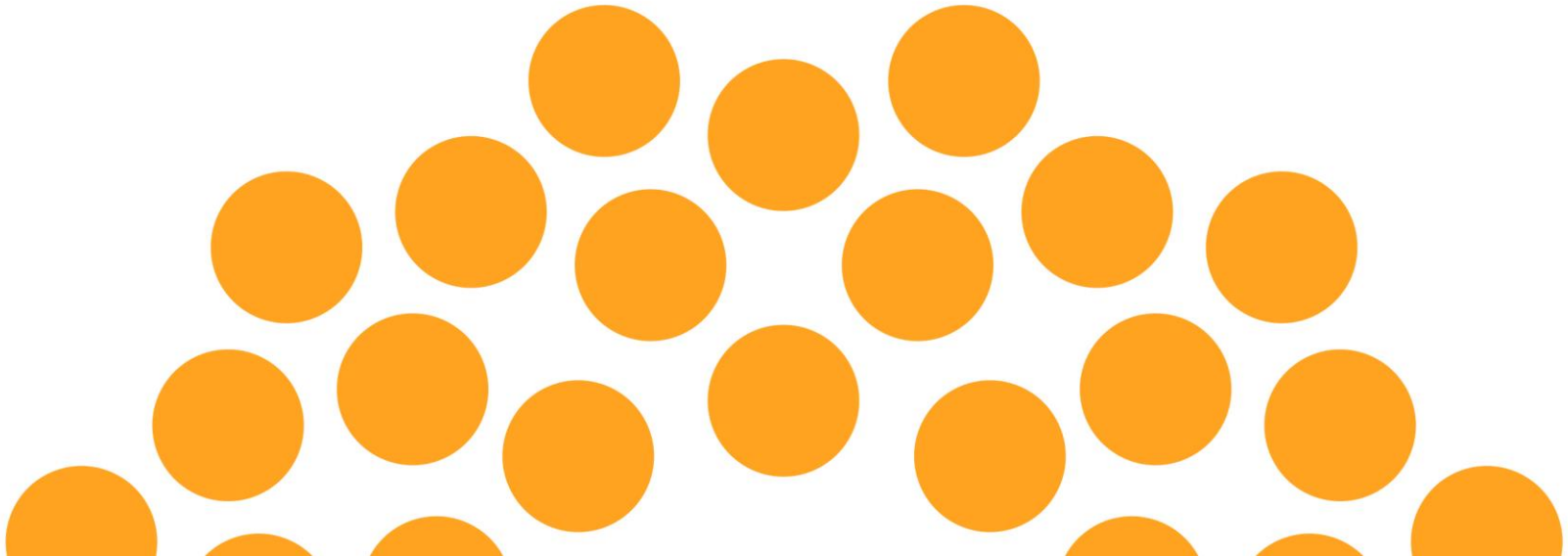
Scopo primario di InfoCamere è fornire soluzioni di eccellenza per la gestione e la divulgazione del patrimonio informativo delle Camere di Commercio

Agenda

1. ***Sicurezza delle informazioni***
2. ***Regolamento europeo protezione dati personali***
3. ***Industria e Agricoltura 4.0***

IC
InfoCamere
Innovare è Crescere

Sicurezza delle Informazioni:
un vero problema o prospettiva sbagliata?



Sicurezza Informatica: cosa intendiamo?

WIKIPEDIA
L'enciclopedia libera

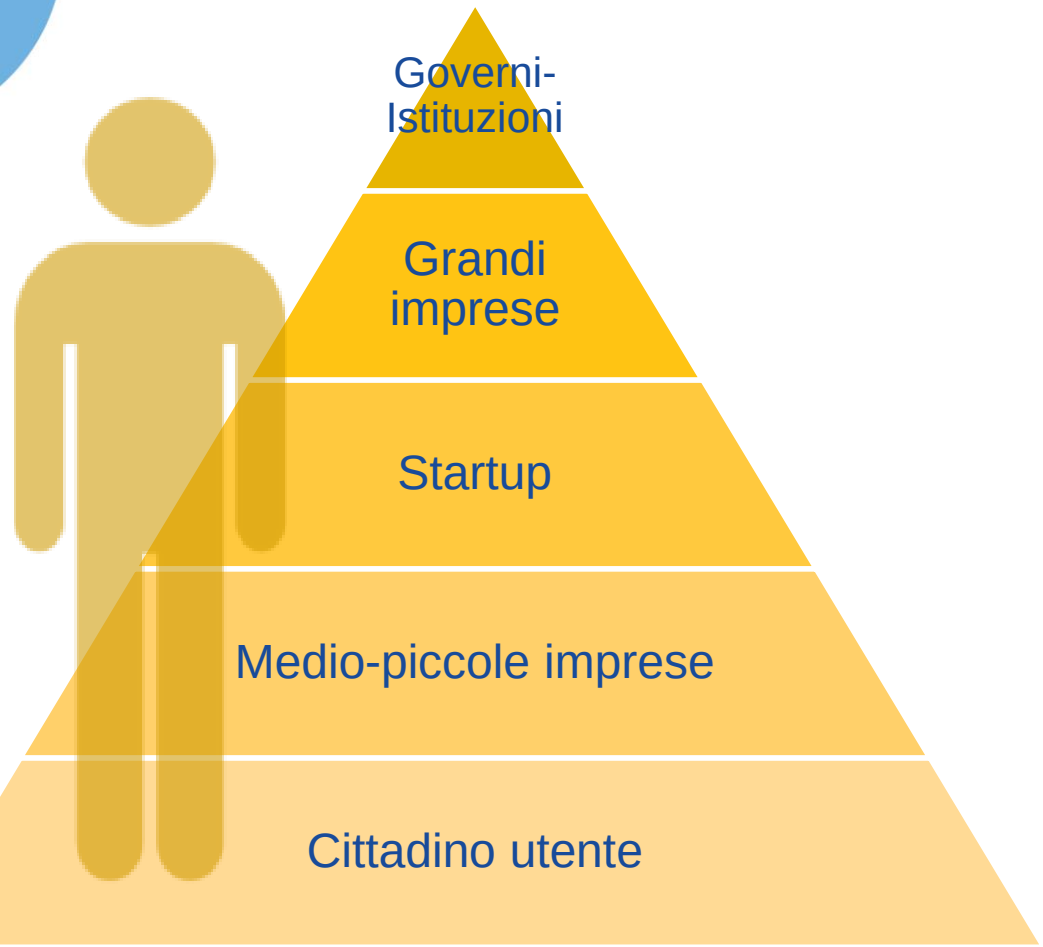
Con il termine **sicurezza informatica** si intende un assieme **di mezzi e tecnologie** tesi alla **protezione** dei sistemi informatici in termini di **disponibilità, confidenzialità e integrità dei beni informatici** (spesso chiamati asset in inglese). A questi tre parametri si tende attualmente ad aggiungere l'autenticità delle informazioni.

Nella sicurezza informatica sono **coinvolti elementi tecnici, organizzativi, giuridici e umani**.

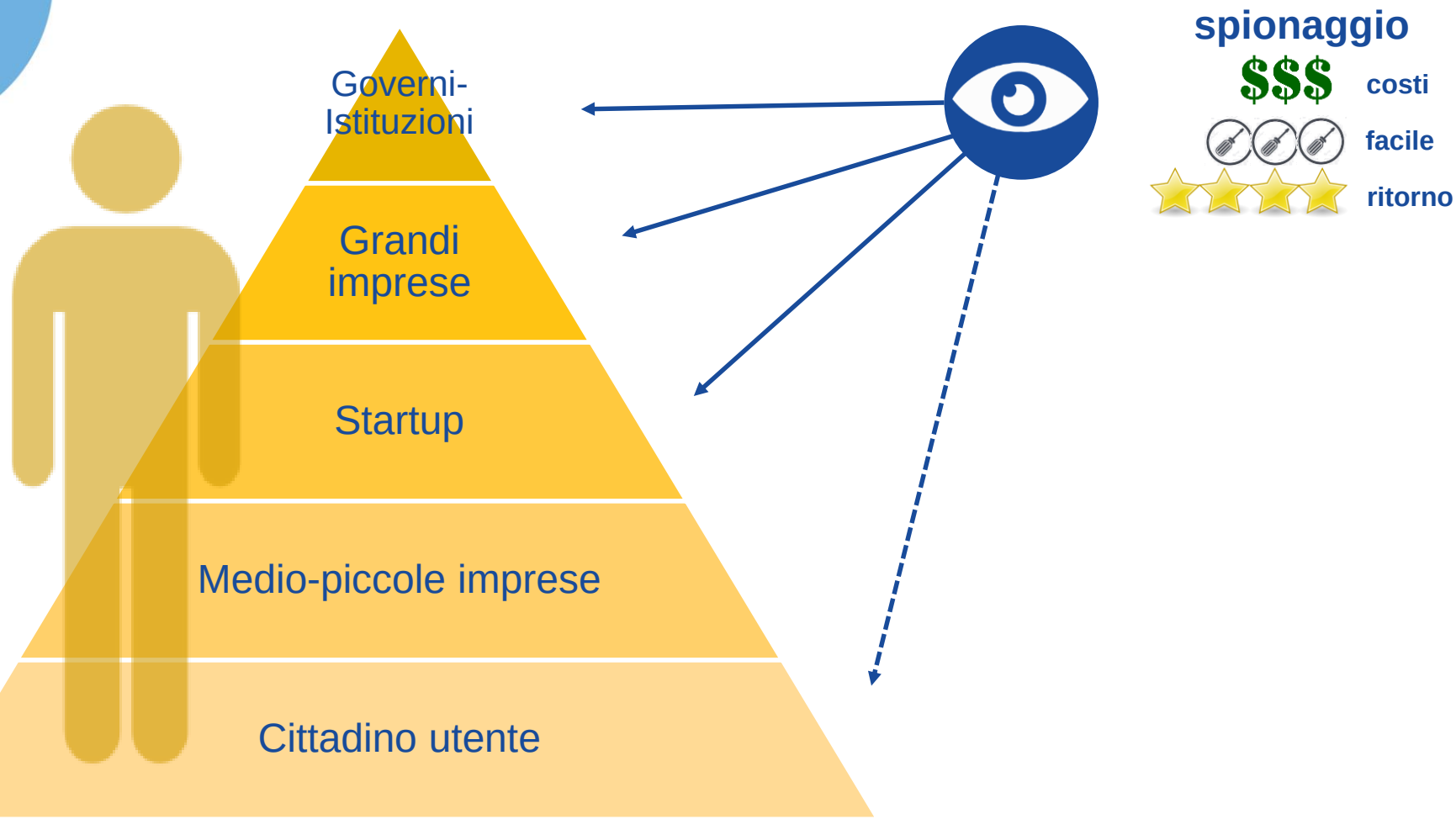
Per valutare la sicurezza è solitamente necessario individuare le minacce, le vulnerabilità e i rischi associati agli asset informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una determinata soglia di tollerabilità (es. economico, politico-sociale, di reputazione, ecc...) ad una organizzazione aziendale.

Il termine è spesso sostituito con il neologismo cybersecurity, che rappresenta una sottoclasse del più ampio concetto di information security. **Per cybersecurity si intende infatti quell'ambito dell'information security prettamente ed esclusivamente dipendente dalla tecnologia informatica.**

Sicurezza Informatica: obiettivi, tecniche e valori



Sicurezza Informatica: obiettivi, tecniche e valori



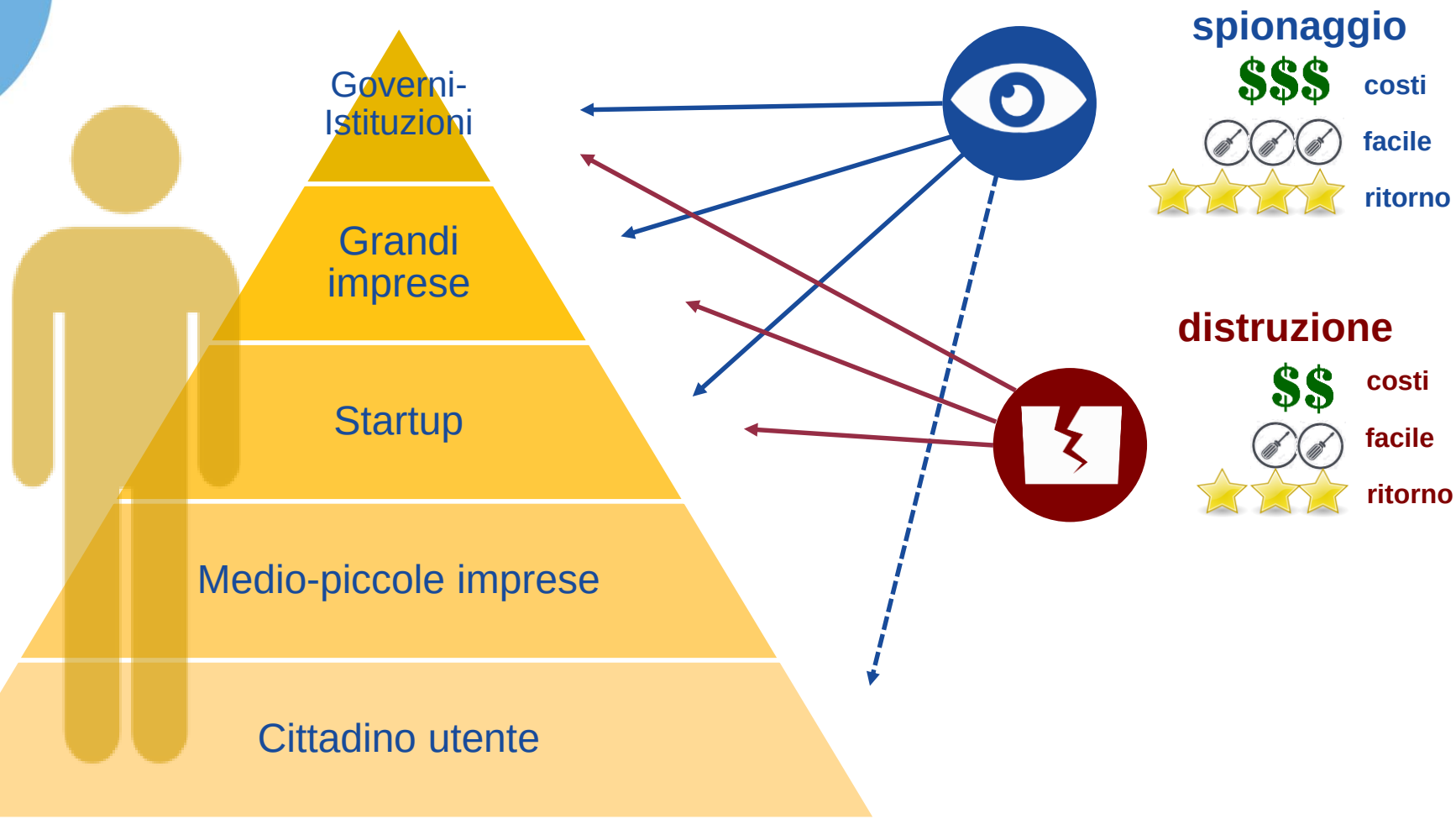
spionaggio

$$$ **costi**

facile

ritorno

Sicurezza Informatica: obiettivi, tecniche e valori



spionaggio

$$$ costi

facile

ritorno

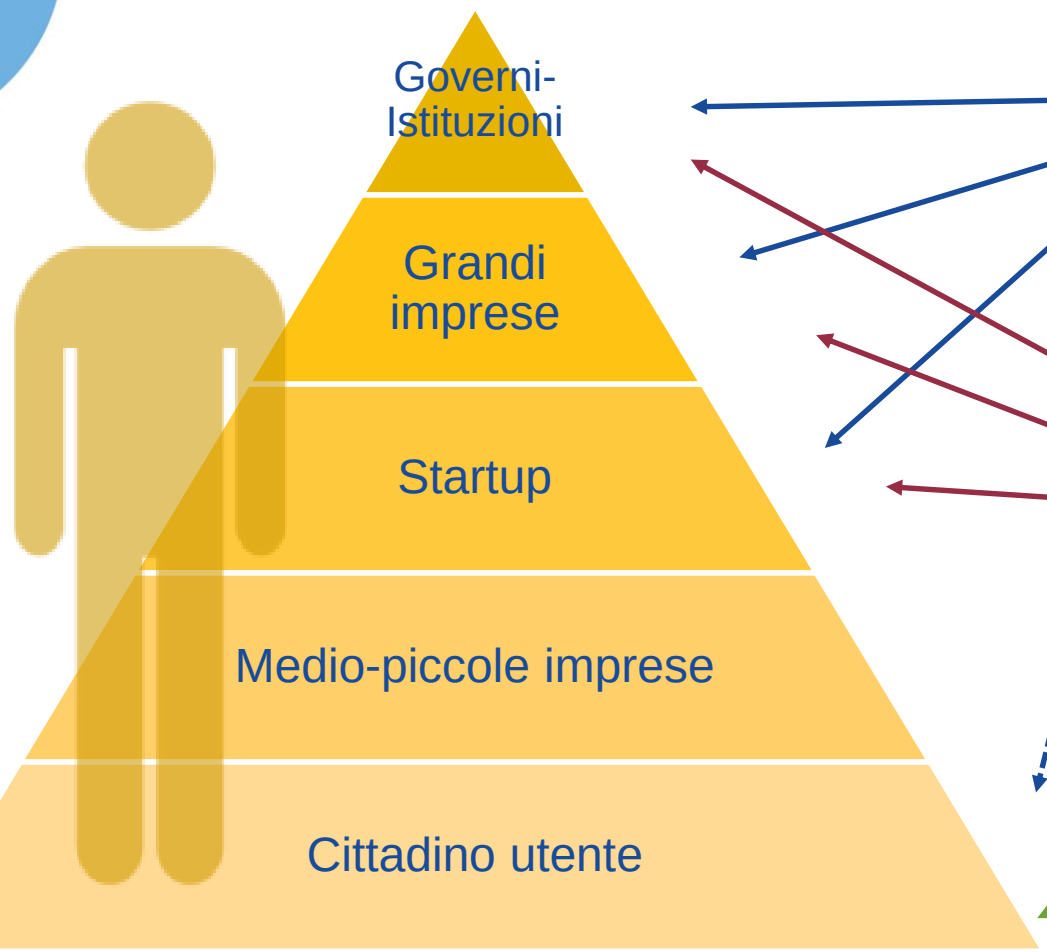
distruzione

$$ costi

facile

ritorno

Sicurezza Informatica: obiettivi, tecniche e valori



spionaggio

$$$ costi

facile

ritorno

distruzione

$$ costi

facile

ritorno

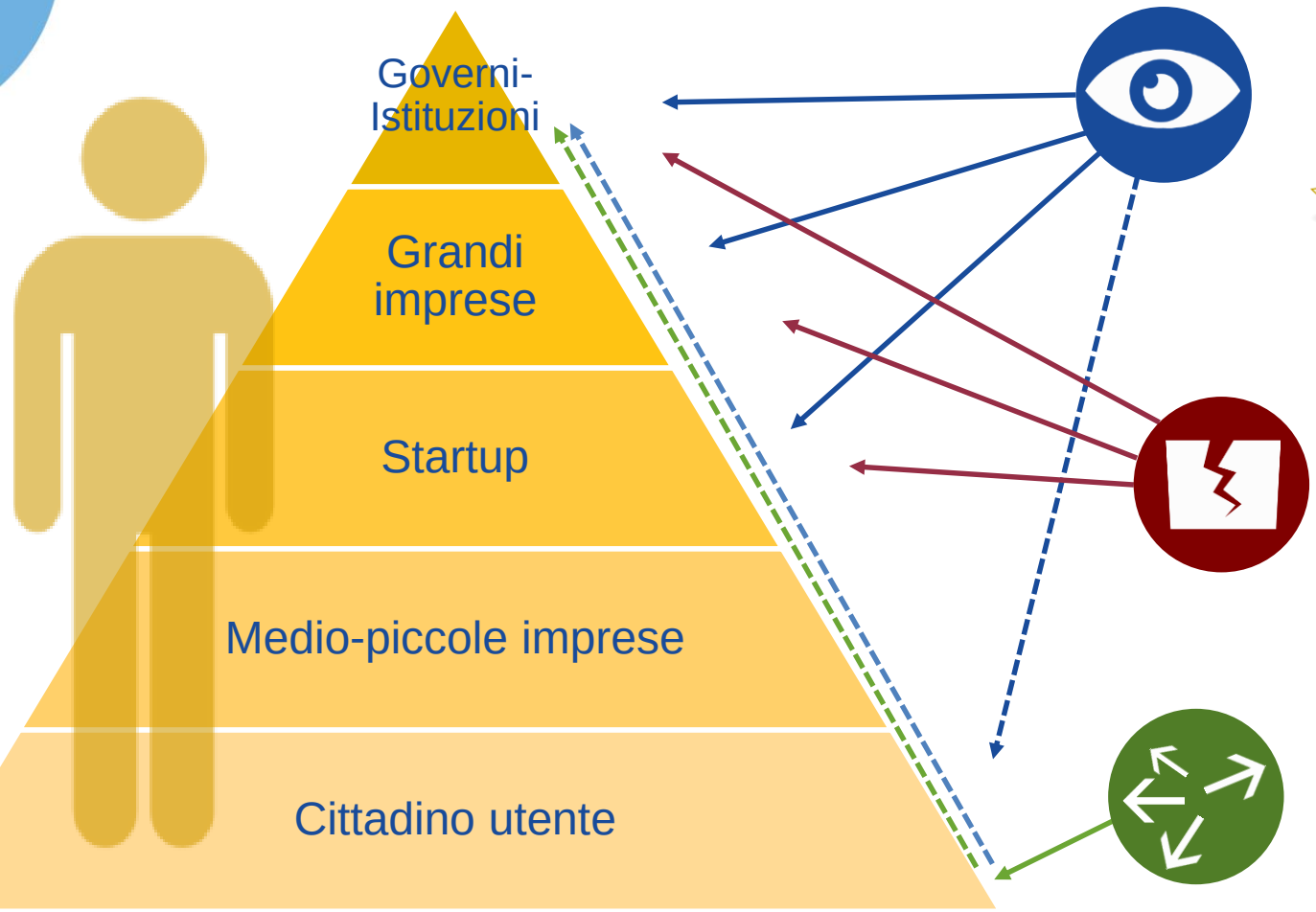
attacco indistinto

$ costi

facile

ritorno

Sicurezza Informatica: obiettivi, tecniche e valori



spionaggio

$$$ costi

facile

ritorno

distruzione

$$ costi

facile

ritorno

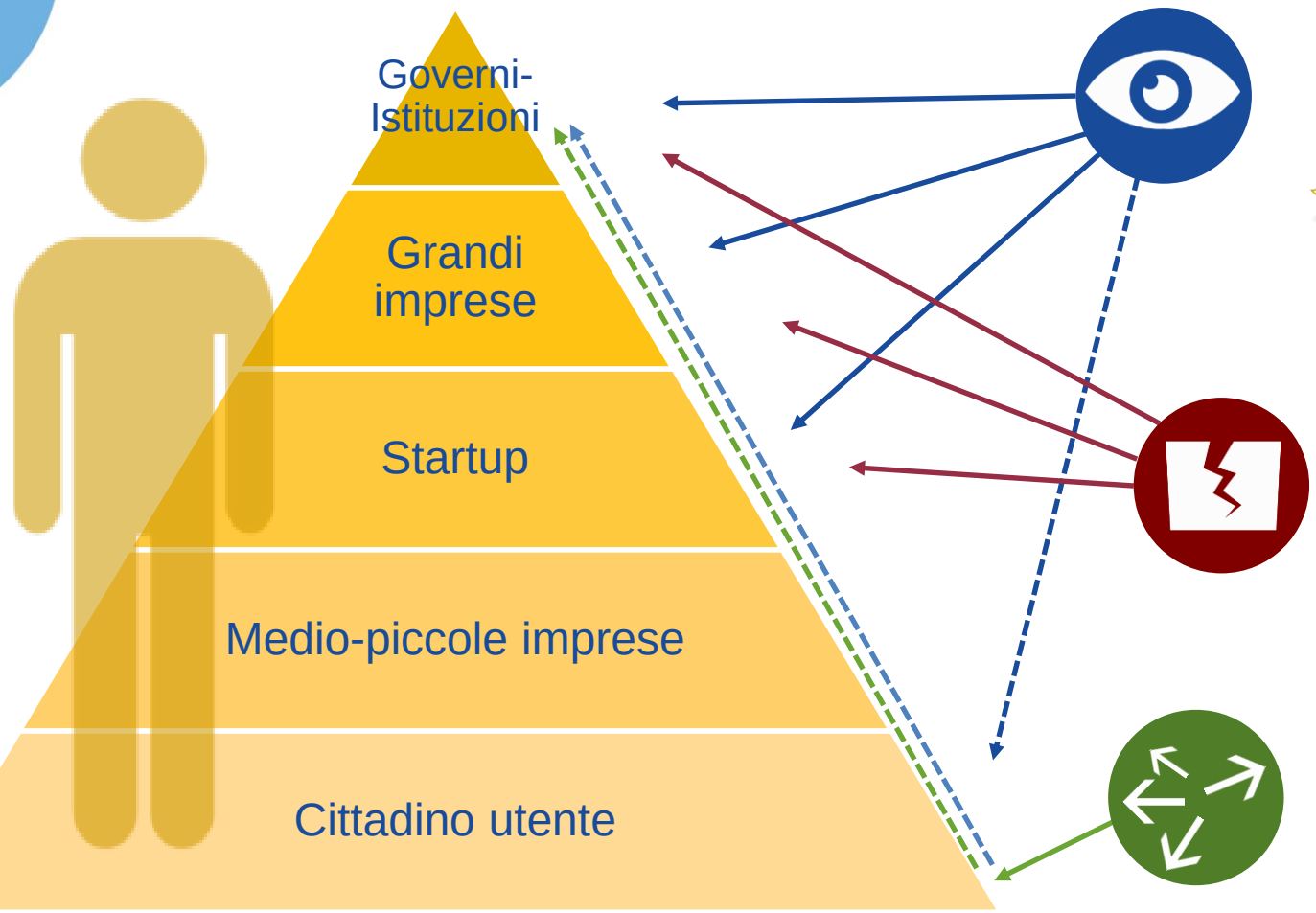
attacco indistinto

$ costi

facile

ritorno

Sicurezza Informatica: obiettivi, tecniche e valori



spionaggio

$$$ costi

facile

ritorno

distruzione

$$ costi

facile

ritorno

attacco indistinto

$ costi

facile

ritorno

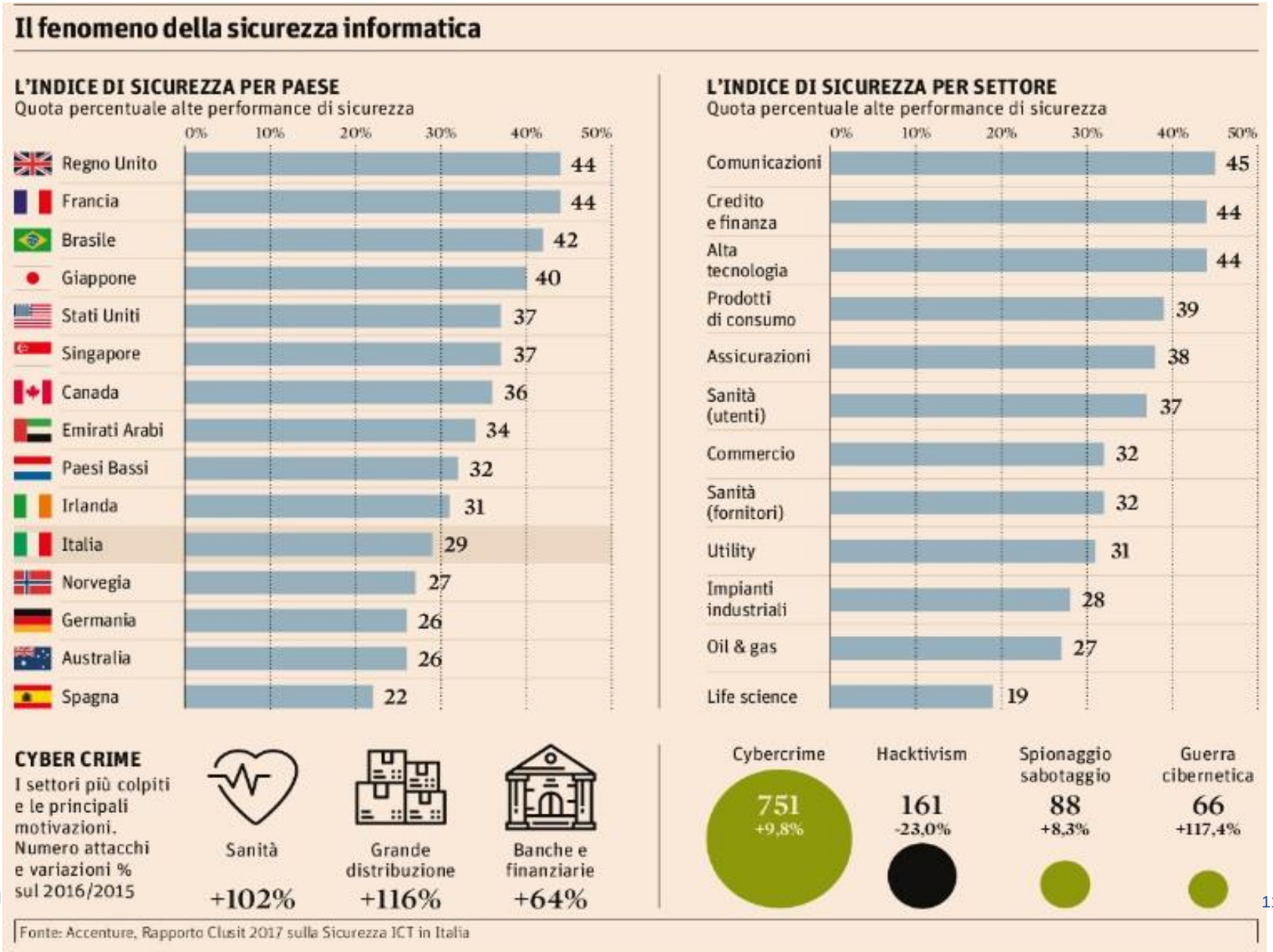
Social Engeneering

$$$$$ costi

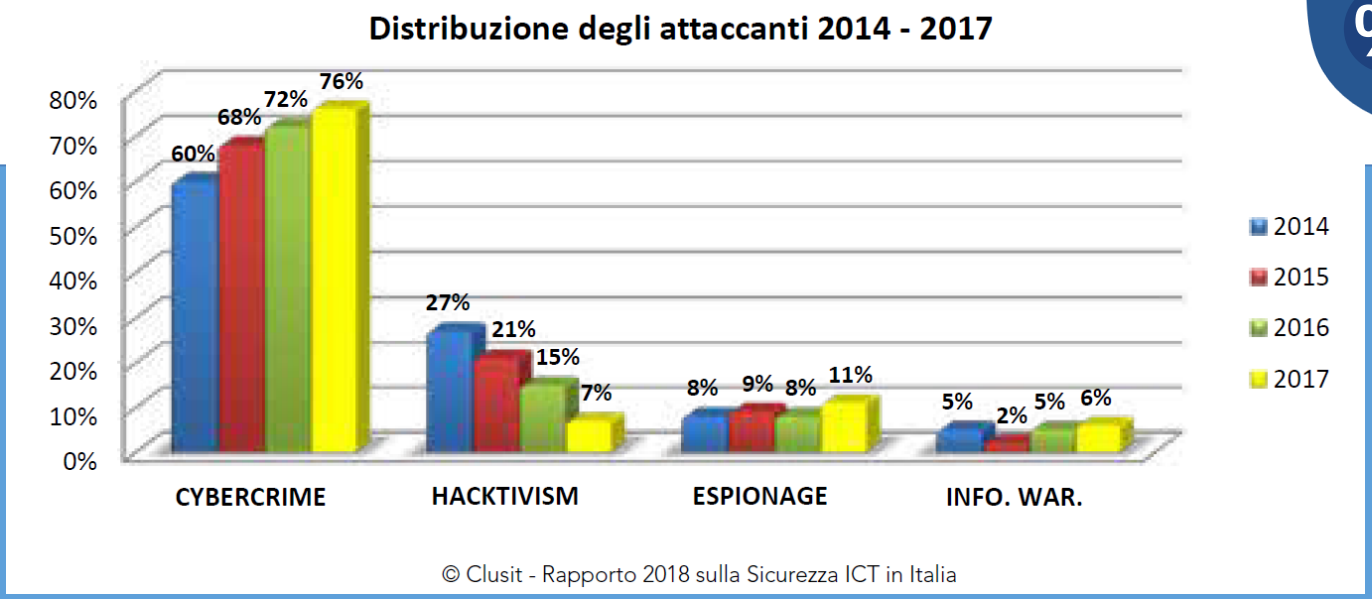
facile

ritorno

Sicurezza – principali minacce - CONTESTO



Sicurezza – principali minacce - CONTESTO

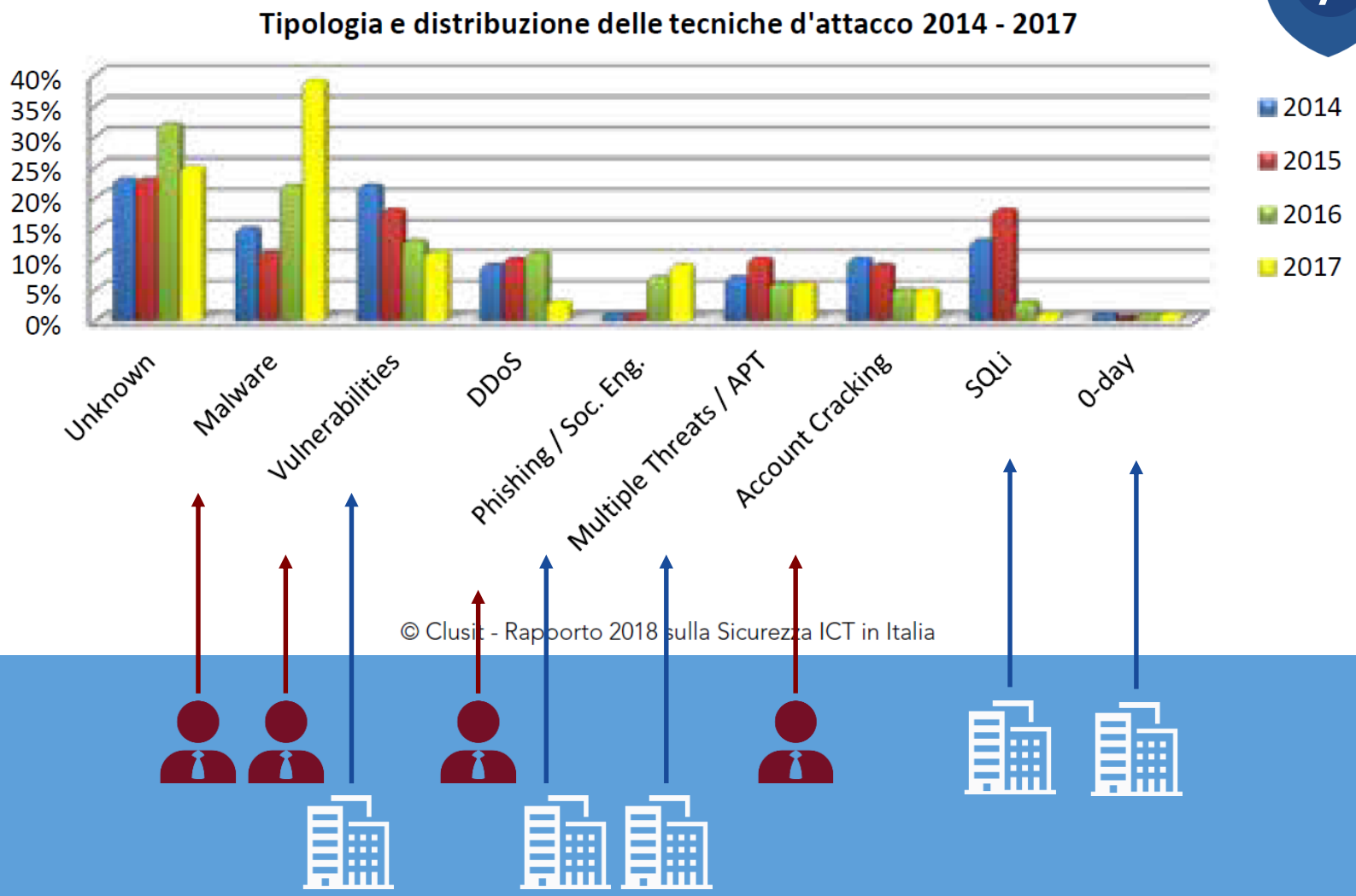


Fatturato 2018 stimato

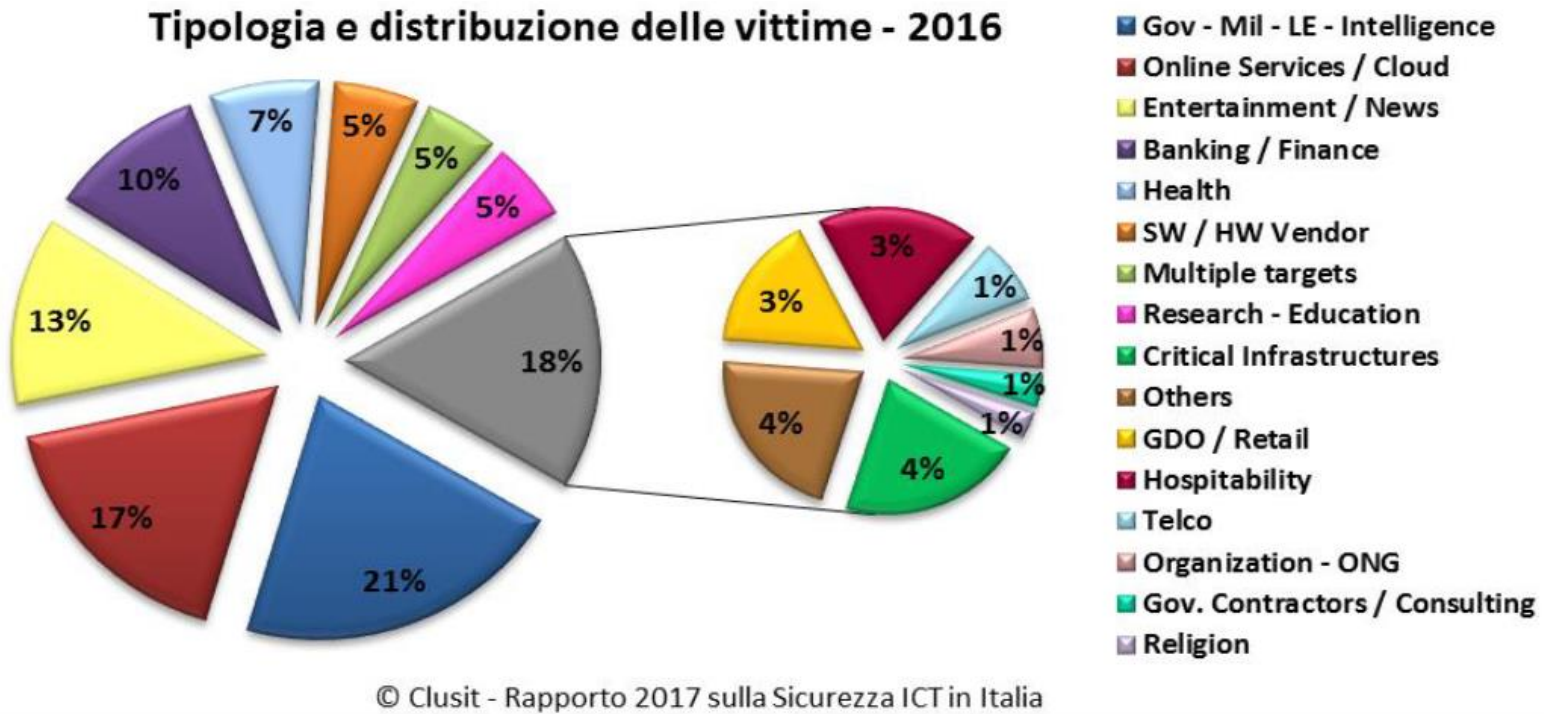
800 miliardi di dollari

"secondo" solo al narcotraffico

Sicurezza – principali minacce - CONTESTO



Sicurezza – principali minacce - CONTESTO



Sicurezza – principali minacce - CONOSCENZA

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co.. tecniche che utilizzando software malevolo hanno l'obiettivo di rubare informazioni o interagire con i sistemi bloccandoli o attivando processi non previsti

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
o attivando
pr

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze o per sfruttare ambiti da cui sferrare gli attacchi

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivand

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti errare gli cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte o comportamenti non previsti/autorizzati

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivando

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti
errare gli
cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte e comportamenti
non

DDos: tecniche che mirano a rendere non raggiungibile o con tempi di risposta altissimi un sito web o una rete intera

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivand

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti errare gli cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte e comportamenti non

DDos: tecniche che mirano a rendere non raggiungibile o con un

Botnet: tecniche di attacco basate su device (o insieme di device) hardware non presidiati da cui lanciare una azione di quelle sopra descritte sincronizzata su vasta scala

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivando

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti

errare gli
cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte e comportamenti
non

DDos: tecniche che mirano a rendere non raggiungibile o
con
un

Botnet: tecniche di attacco basate su device (o insieme di device) hardware non presidiati da cui lanciare una azione di quelle sopra descritte sincronizzata su vasta scala

Data Breach: furto, modifica, accesso, cancellazione di dati; assume particolare significatività nel momento in cui l'azione viene fatta su dati personali e/o sensibili per le organizzazioni e la società.

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivando

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti per deviare gli scambi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte e comportamenti non

DDos: tecniche che mirano a rendere non raggiungibile o con
un

Botnet: tecniche di attacco basate su device (o insieme di device) hardware non presidiati da cui lanciare una azione di quelle sopra descritte sincronizzata su vasta scala

Data Breach: f
modifica, acce
cancellazione d
assume partic
significatività nel m
in cui l'azione viene
dati personali e/o s
per le organizzazioni e la società.

Furti di Identità: tecniche che agiscono sull'acquisizione fraudolenta dei dati di un soggetto per agire in vece sua o per limitarne le capacità decisionali/operative

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
e attivand

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze e per sfruttare ambiti errare gli cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte e comportamenti non

DDos: tecniche che mirano a rendere non raggiungibile o con un

Botnet: tecniche di attacco basate su device (o insieme di device) hardware non presidiati da cui lanciare una azione di quelle sopra descritte sincronizzata su vasta scala

Data Breach: f
modifica, acce
cancellazione d
assume partic
significatività nel m
in cui l'azione viene
dati personali e/o s
per le organizzazioni e la società.

Social Engeneering: tecniche di raccolta informazioni per effettuare un attacco verso un singolo o una società

Furti di Identità: tecniche che agiscono sull'acquisizione fraudolenta dei dati di un soggetto per agire in vece sua o per limitarne le capacità decisionali/operative

Sicurezza – principali minacce - CONOSCENZA

Malware: virus & co..
tecniche che utilizzando
software m
l'obiettiv
informazio
con i siste
o attivand

Web Based Attacks: tecniche che si basano sui siti web per trovare debolezze o per sfruttare ambiti errare gli cchi

Web Application Attacks: tecniche che entrano via web nelle applicazioni per ottenere risposte o comportamenti non

DDos: tecniche che mirano a rendere non raggiungibile o con un

Botnet: tecniche di attacco basate su device (o insieme di device) hardware non presidiati da cui lanciare una azione di quelle sopra descritte sincronizzata su vasta scala

Social Engeneering
tecniche di racco
informazioni pe
effettuare un
attacco verso u
singolo o una
società

Cyber Spionaggio: tecniche sofisticate per carpire in maniera continuativa o mirata informazioni ad un soggetto / organizzazione

Furti di Identità: tecniche che agiscono sull'acquisizione fraudolenta dei dati di un soggetto per agire in vece sua o per limitarne le capacità decisionali/operative

Data Breach: f
modifica, acce
cancellazione d
assume partic
significatività nel m
in cui l'azione viene
dati personali e/o s
per le organizzazioni e la società.

Sicurezza – principali minacce - CONOSCENZA

- **Attacchi esterni:**

  - Malware
  - Web based attacks
  - Web application attacks
  - DDos
  - Botnet
  - Data Breach
  - Furti identità
  - Social Engeneering
  - Cyber spionaggio

- **Attacchi interni:**

  - Malware
  - Web based attacks
  - Web application attacks
  - Data Breach
  - Furti identità
  - Social Engeneering
  - Cyber spionaggio

Molte fonti riportano che, **statisticamente, oltre il 75% degli attacchi andati a buon fine possono contare su una *base interna* o una *debolezza del sistema***
che compromette la solidità di tutto l'insieme.

Cybersecurity problema vero, sbagliata la prospettiva

Abbiamo imparato a…

Cybersecurity problema vero, sbagliata la prospettiva

Abbiamo imparato a…

- **Leggere e scrivere**
  andando a scuola

Cybersecurity problema vero, sbagliata la prospettiva

Abbiamo imparato a…

- **Leggere e scrivere**
  andando a scuola
- **Correre in bicicletta,**
  sbucciandoci le ginocchia

Cybersecurity problema vero, sbagliata la prospettiva

Abbiamo imparato a…

- **Leggere e scrivere**
  andando a scuola
- **Correre in bicicletta,**
  sbucciandoci le ginocchia
- **Guidare l'auto,**
  studiando e affrontando gli esami

Cybersecurity problema vero, sbagliata la prospettiva

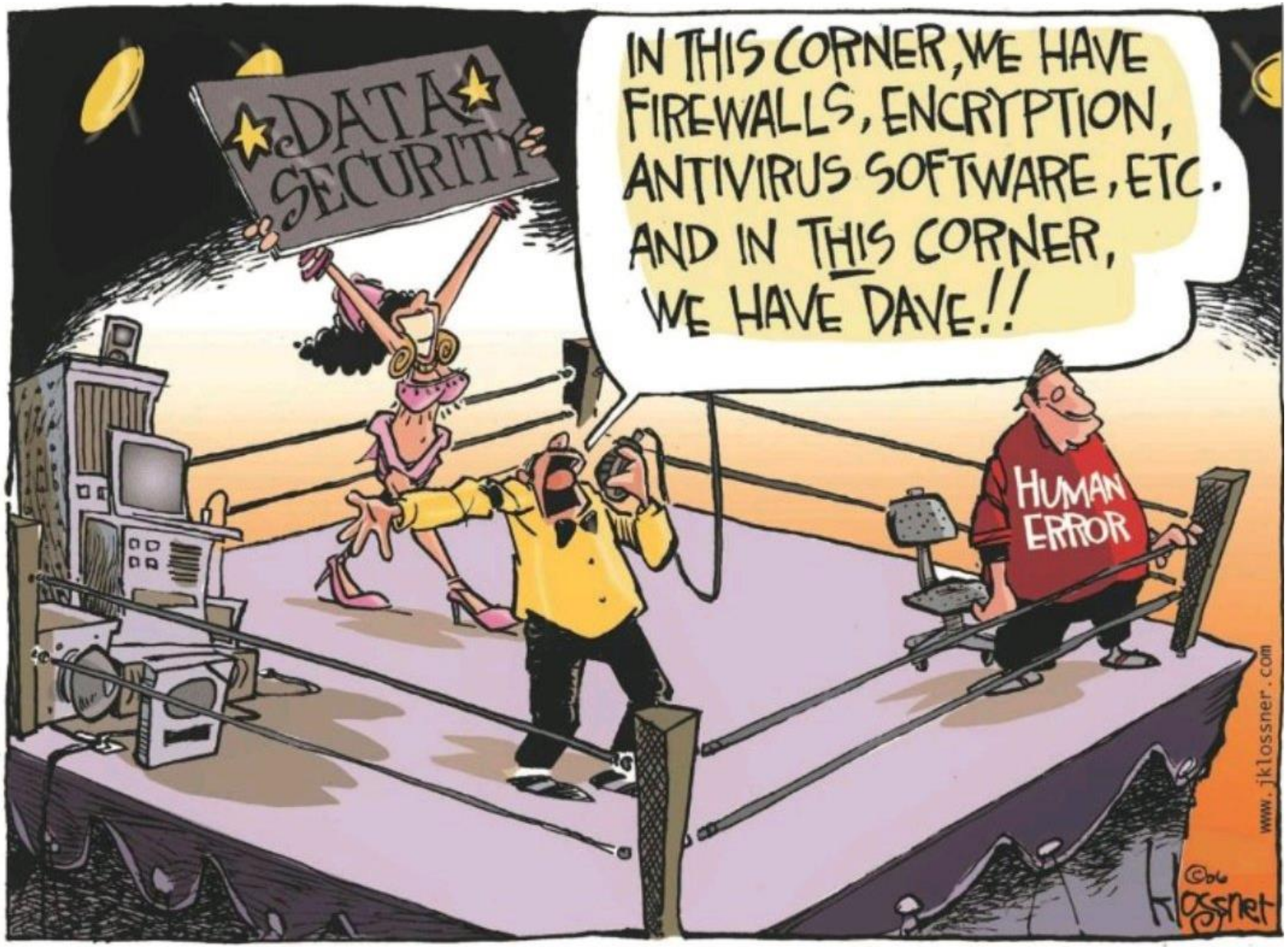
Abbiamo imparato a…

- **Leggere e scrivere**
  andando a scuola
- **Correre in bicicletta,**
  sbucciandoci le ginocchia
- **Guidare l'auto,**
  studiando e affrontando gli esami

Ma come abbiamo imparato ad usare il computer?

…lo abbiamo acceso!

Cybersecurity problema vero, sbagliata la prospettiva

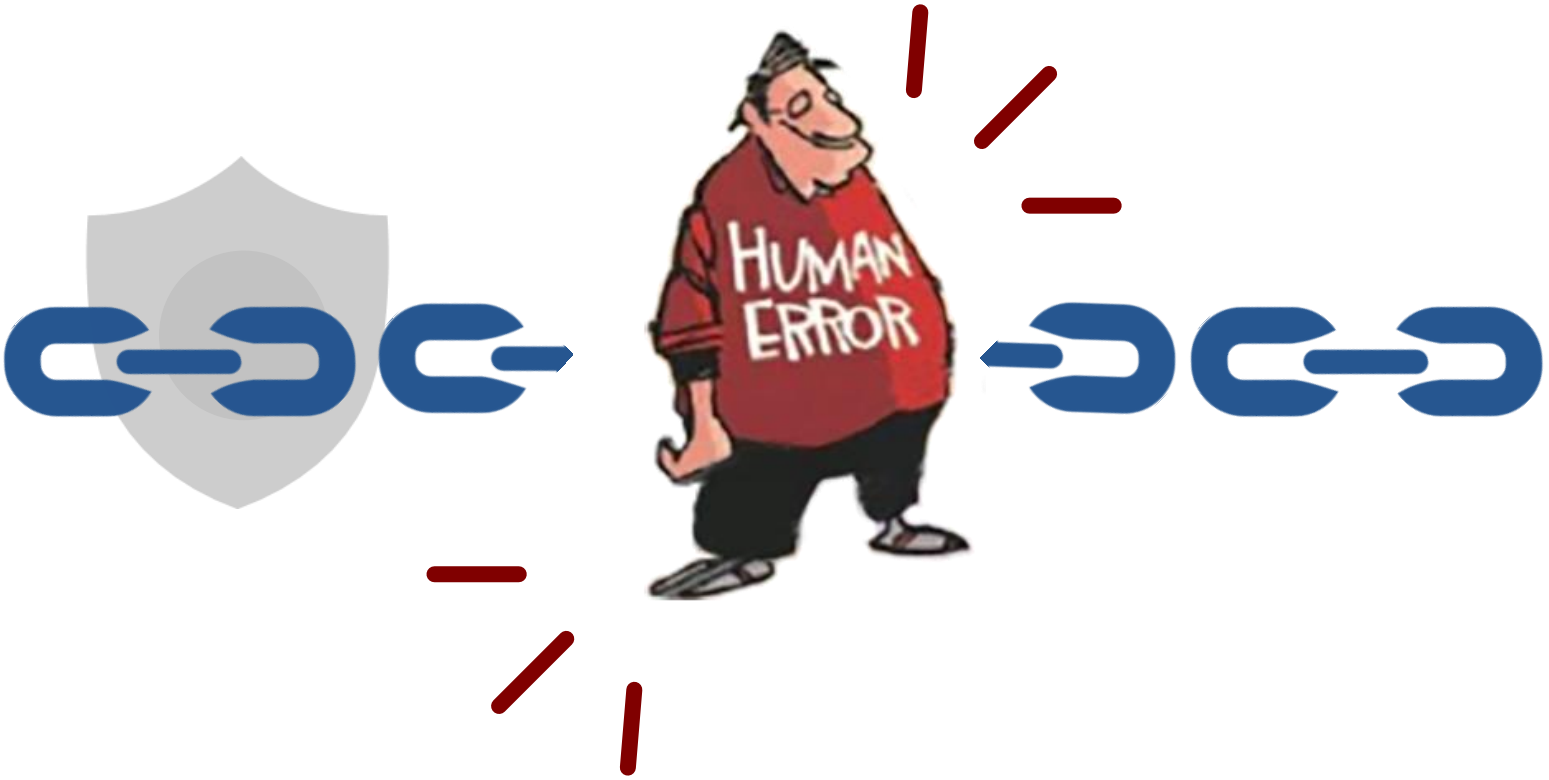


Cosa combina "*Dave*"?

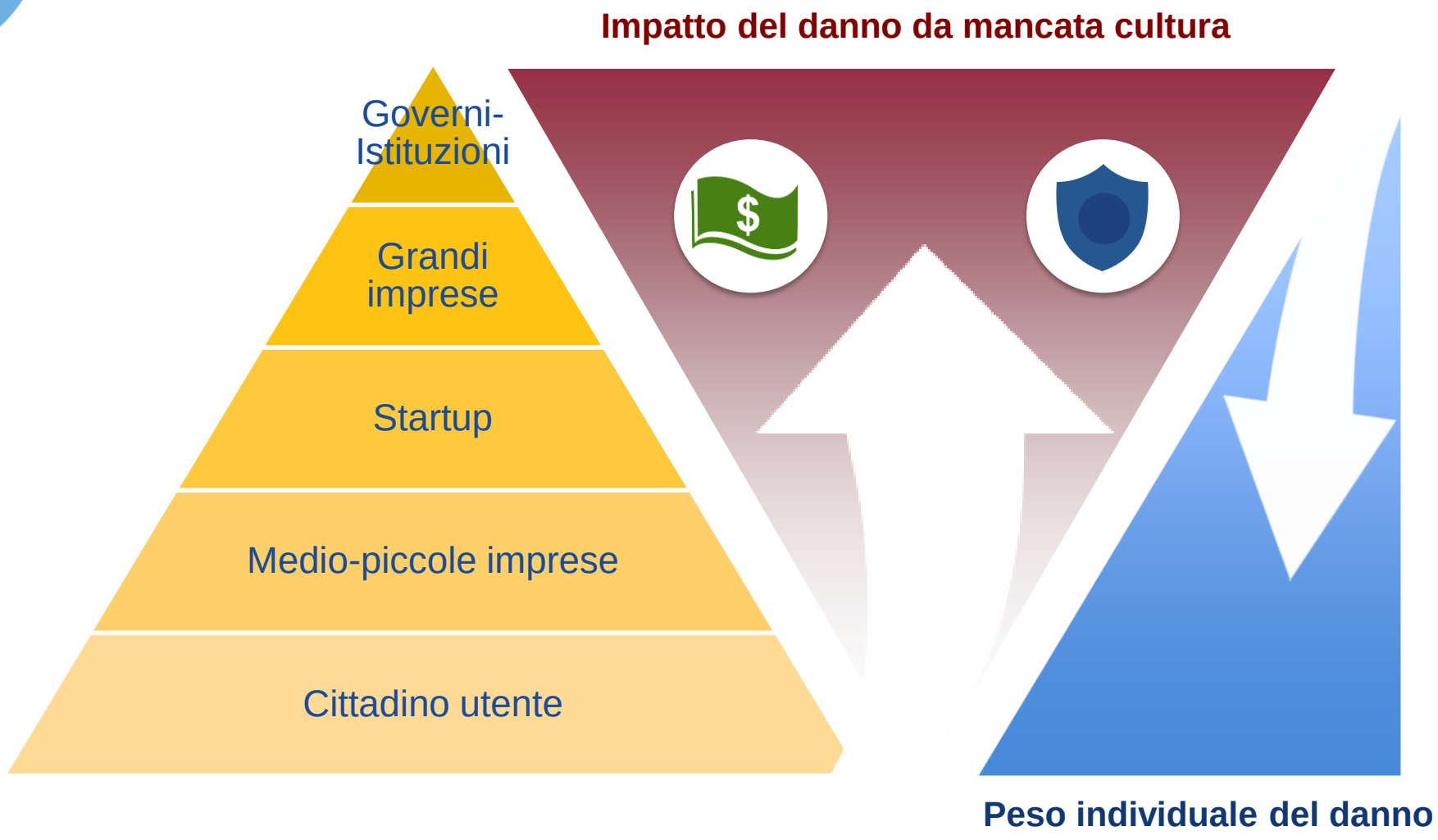
Password più usate in Italia:

Rank	Password	Frequency
1	123456	706,689
2	123456789	237,898
3	12345	107,211
4	000000	78,924
5	111111	62,445
6	12345678	61,658
7	azerty	56,688
8	paSSword	54,128
9	1234567	53,003
10	badoo	49,918
11	123123	37,082
12	1234567890	33,945
13	654321	28,728
14	qwerty	25,736
15	666666	25,000
16	juventus	23,659
17	antonio	21,679
18	andrea	21,153
19	121212	19,960
20	010203	18,632
21	987654321	18,590

"*Dave*" non deve essere l'anello debole della catena!



Mancata cultura – danno di scala



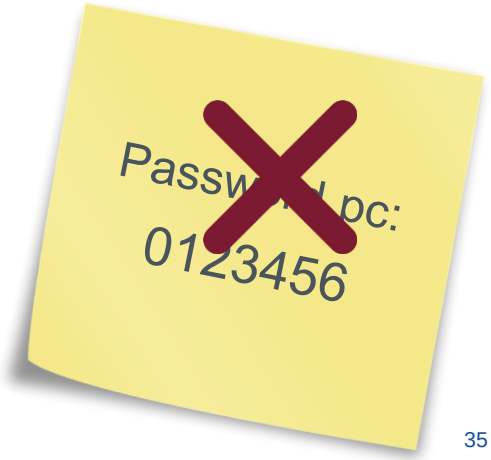
Per metterci in sicurezza cosa fare: FASE 1

- **A casa mia entra chi voglio io:** sistemi di controllo e validazione degli accessi sono il primo passo di sicurezza da mettere in atto; accedere a pc/server/smartphone solo dopo aver digitato una **password o** un **codice di accesso** *(non deve essere scritto su un post-it attaccato al monitor…).*

- **Educazione innanzitutto:** evitare di accendere il computer e lasciarlo incustodito.

- **Cosa ho in casa:** conoscere lo stato in essere degli strumenti; la gestione del cespite non deve essere vista solo come un componente da ammortizzare.

- **Cosa rischio:** avere un quadro degli ambiti a rischio per l'azienda e operare per ridurlo o abbatterlo.



Per metterci in sicurezza cosa fare: FASE 2

- **Chi meno spende meno ha:** è un vecchio detto che mai come oggi dobbiamo tenere presente soprattutto se abbiamo a che fare con risorse scarse.
  Per assistenza, outsourcing e manutenzioni vanno valutati **partner che garantiscano le proprie capacità**.

- **Sono aggiornato?:** non poniamoci la domanda come persone ma come ***organizzazione***. Avere la certezza che le persone che operano in ambiti delicati/sensibili siano formate adeguatamente e che i sistemi operativi (anche SCADA) siano **aggiornati** alle ultime release di software.

- **Il SW scade?:** sì, non va a male ma può far male!
  Scadono le manutenzioni dei sistemi operativi,
  scadono le funzionalità dei sistemi applicativi,
  scadono le garanzie dei vecchi software (a cui siamo *affezionati…*)
  che nessuno aggiorna più e che possono diventare
  porte di entrata pericolose.

Per metterci in sicurezza cosa fare: FASE 3

- **Vaccinati sempre:** evitare situazioni di scarsa copertura antivirus e tenere conto che più alto è il rischio più elevata dovrà essere la copertura da tale rischio.
- **Aggiornati sempre:** oltre alle persone vanno aggiornati tutti i sistemi con le ultime correzioni: ciò vale per il pc ma anche per lo smartphone.
- **Mi salvo sempre:** backup dei sistemi, dei dati, della mia rete… più alto è il rischio e più alta dovrà essere la copertura. Le soluzioni «cloud free» vanno valutate attentamente: non sempre i contratti sono pensati per tutelare gli utenti (*soprattutto sulla proprietà dei dati*).
- **Cripto o non cripto:** la criptazione dei dati, soprattutto se sensibili, garantisce maggiore sicurezza.
- **Mi fido poco:** Pretendere servizi reali, misurabili, oggettivi e con livelli di servizio garantiti… se serve anche con penali.

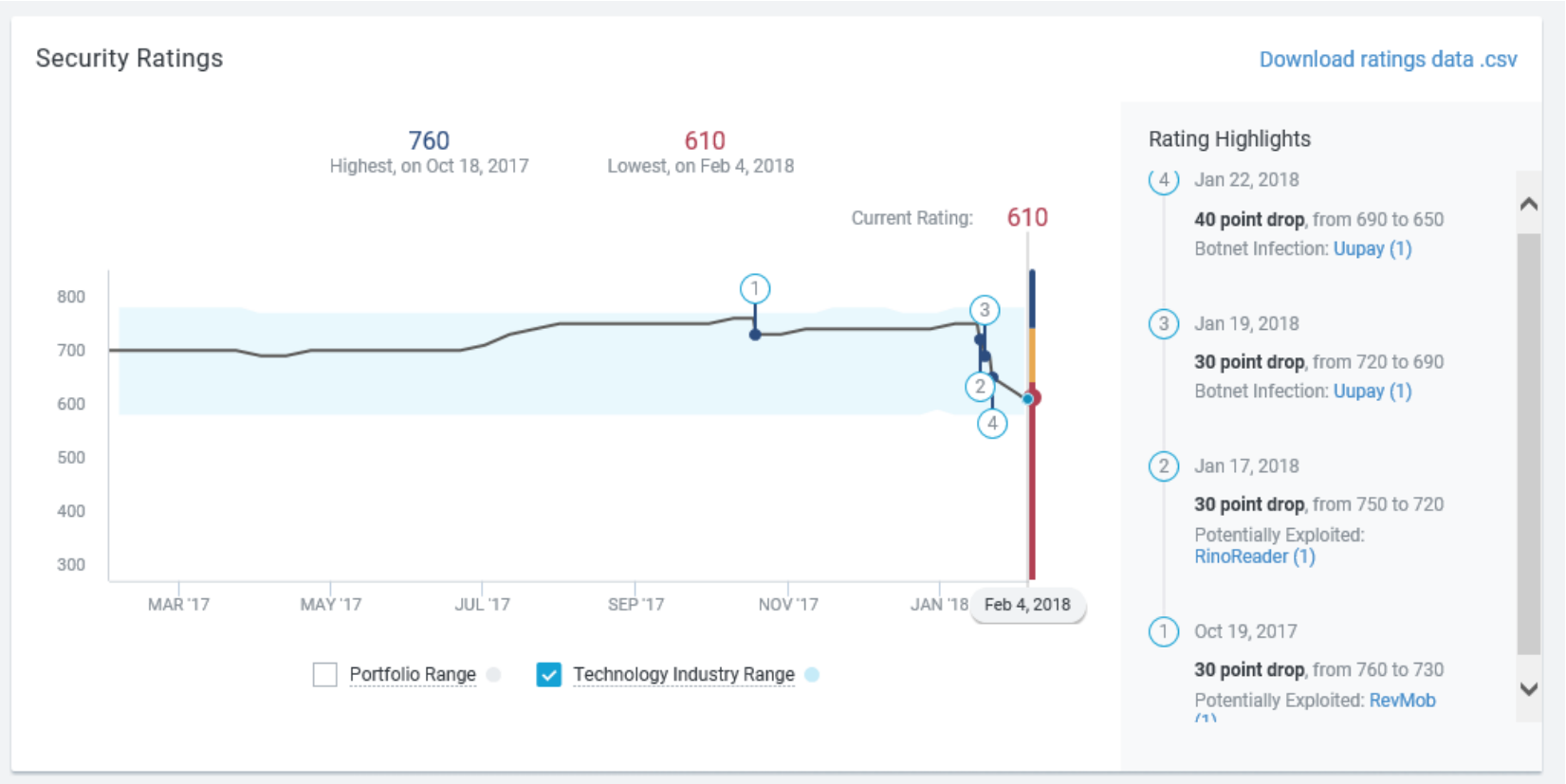
Per metterci in sicurezza cosa fare: FASE 4

- **Assicurarsi… perché no?:** sul mercato ci sono soluzioni che permettono, conoscendolo, di assicurare il rischio anche in ambito cyber.
  Per avere potere contrattuale reale è necessario **conoscere il rischio**.

NB: ai sensi dell'art 1418 c.c. le sanzioni NON sono assicurabili!

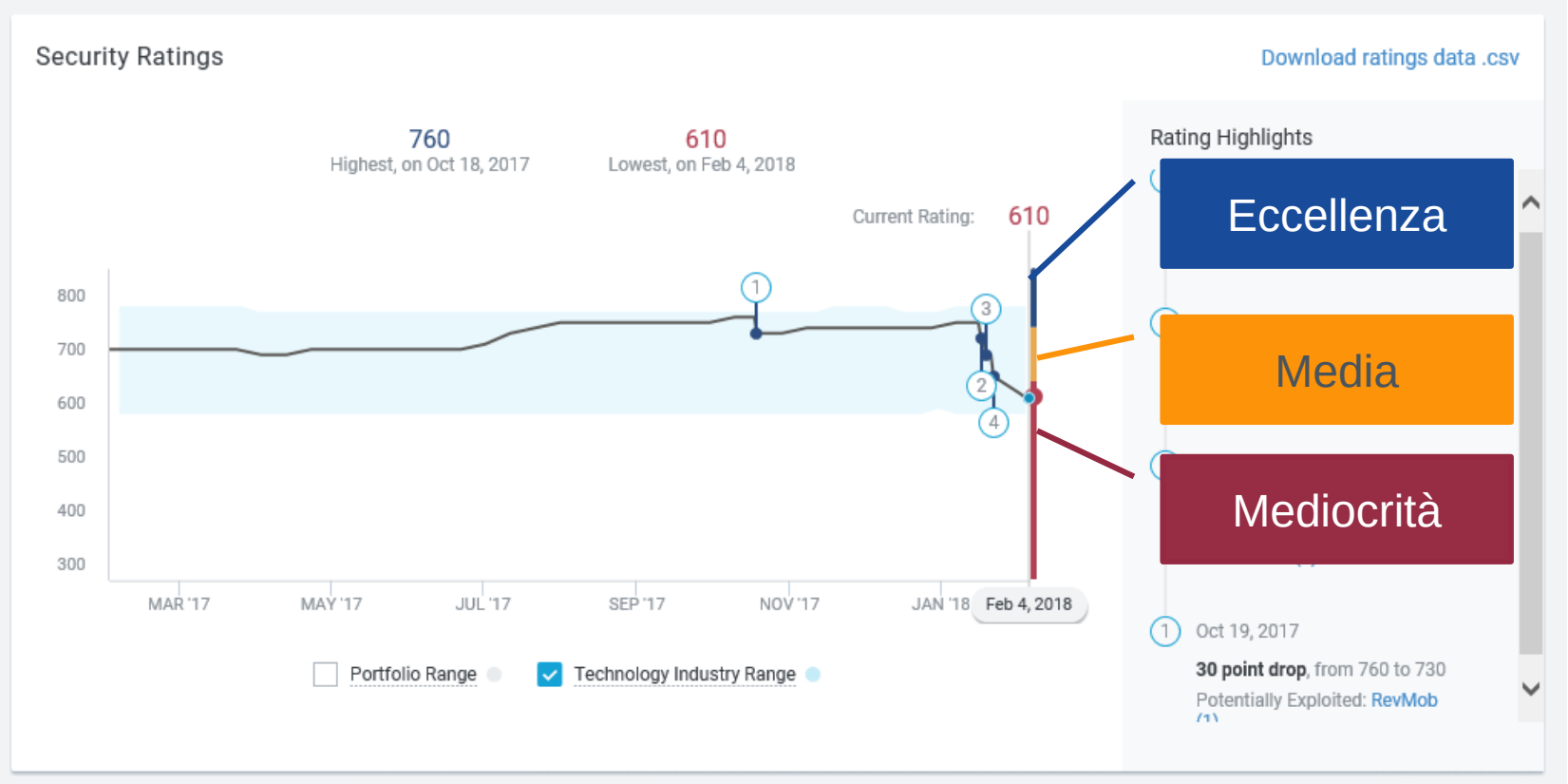
Per metterci in sicurezza cosa fare: FASE 5

- **Rischio reputazionale**: un rischio reale che, se non governato e conosciuto, può rappresentare un'arma in più da usare nei confronti di obiettivi e/o bersagli magari in abbinata con una bella azione di Social Engineering



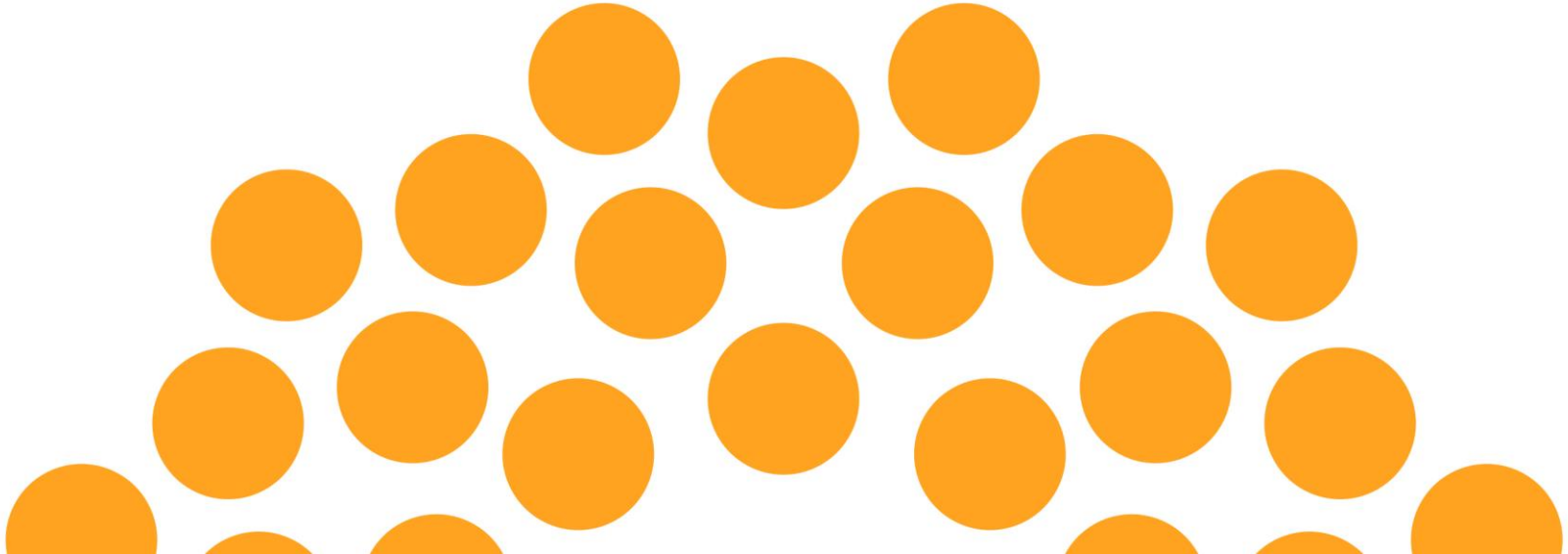
Per metterci in sicurezza cosa fare: FASE 5

- **Rischio reputazionale**: un rischio reale che, se non governato e conosciuto, può rappresentare un'arma in più da usare nei confronti di obiettivi e/o bersagli magari in abbinata con una bella azione di Social Engineering



IC
InfoCamere
Innovare è Crescere

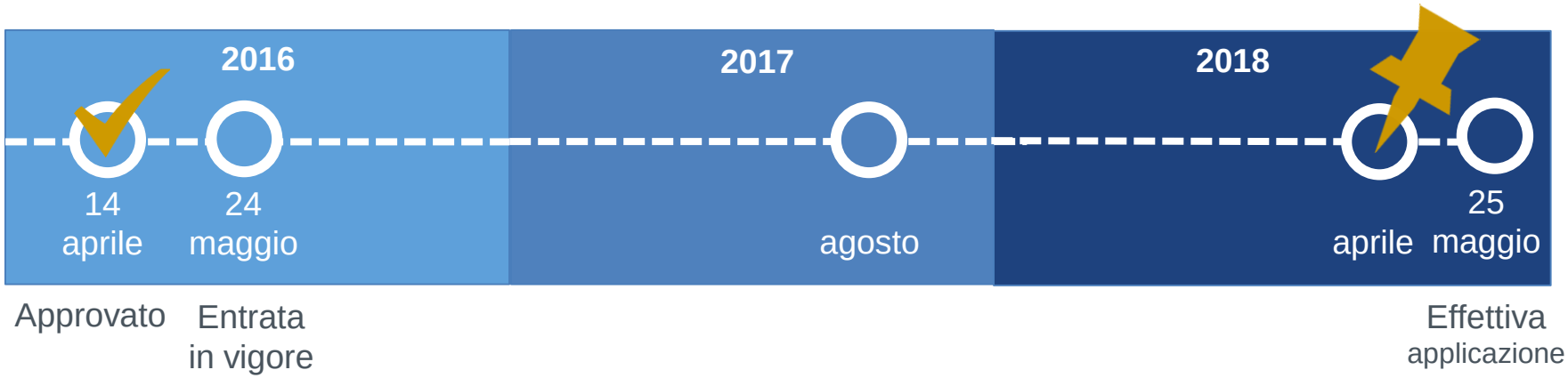
Regolamento Europeo sul trattamento dei dati personali – GDPR – 679/2016



Concetti che svilupperemo

- Regolamento Europeo 2016/679
- I nuovi ambiti di attenzione
- TITOLARE e RESPONSABILE
- Avvisi ai naviganti
- Il Registro dei Trattamenti

Regolamento Europeo 2016/679 - GDPR



Disposizioni generali

Articolo 1:

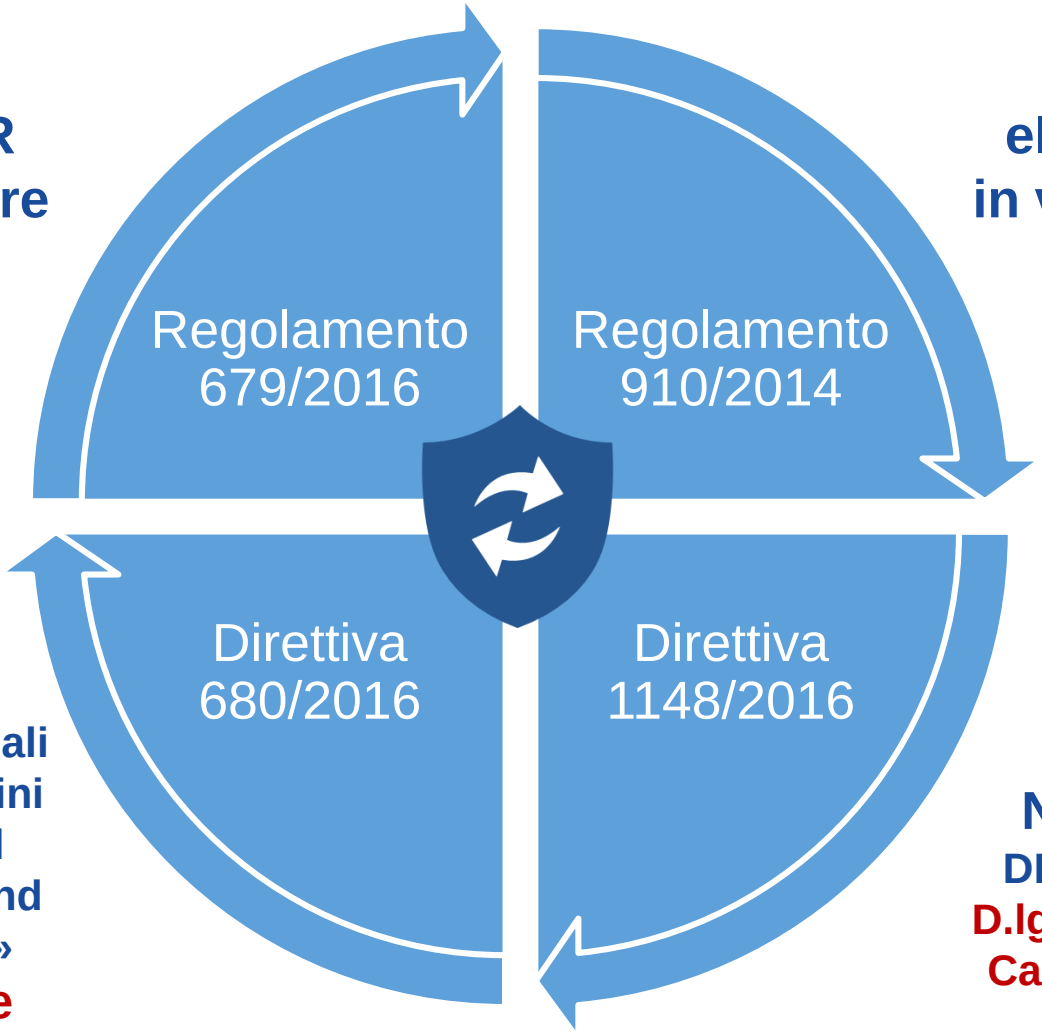
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla **protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché norme relative alla **libera circolazione di tali dati**.
2. Il presente regolamento **protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.**
3. **La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

EU SECURITY FRAMEWORK 2018

GDPR in vigore

eIDAS in vigore



Dati personali nelle Indagini «Criminal Offences and Penalties»
D.lgs alle Camere

NIS
DPCM
D.lgs alle Camere

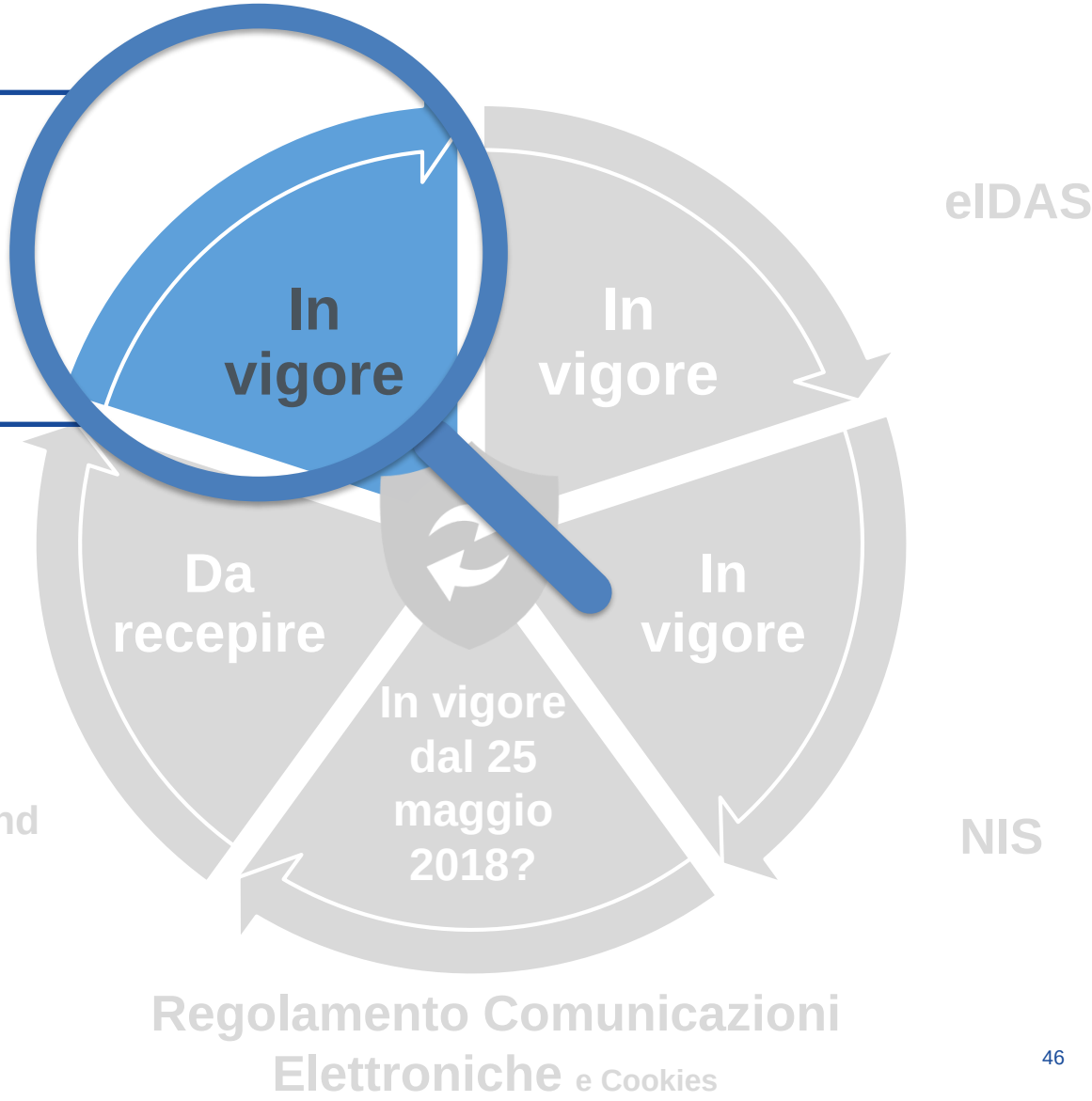
EU SECURITY FRAMEWORK 2018
Misure tecniche e organizzative

Regolamento Comunicazioni Elettroniche e Cookies

EU SECURITY FRAMEWORK 2018
Misure tecniche e organizzative

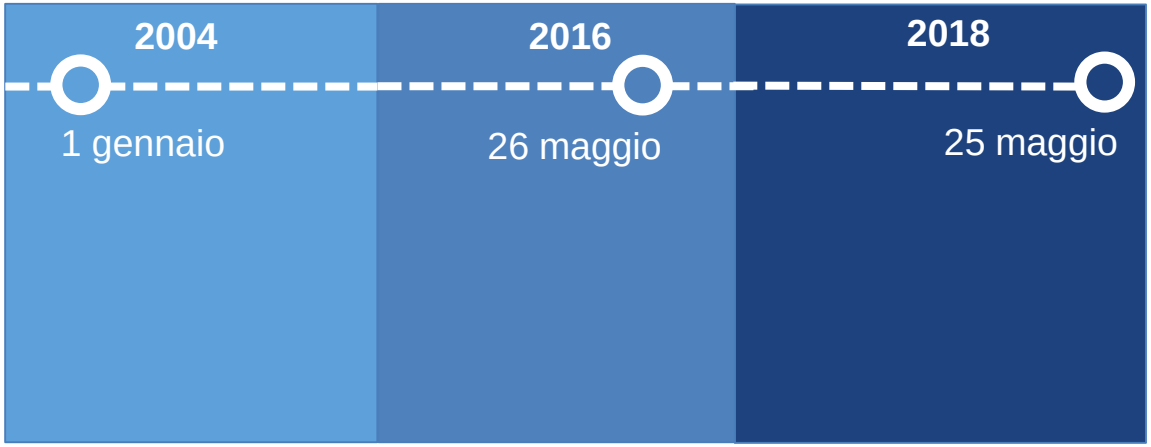
Ci focalizziamo ora su:

GDPR



Regolamento Europeo 2016/679 - GDPR

Le fasi



Regolamento Europeo 2016/679 - GDPR
Le fasi