



POLITECNICO
MILANO 1863

SCHOOL OF MANAGEMENT



GDPR e Security: un percorso impervio... a trazione integrale

Osservatorio Information Security & Privacy

03.05.2018

www.osservatori.net



La mission e il target dell'Osservatorio



L'Osservatorio intende rispondere al bisogno di conoscere, comprendere e affrontare le principali problematiche dell'Information Security & Privacy e monitorare l'utilizzo di nuove tecniche e tecnologie a supporto di tale area da parte delle aziende end user



L'Osservatorio si rivolge a tutti coloro che si occupano di Security, da diversi punti di vista: CIO, CSO, CISO, DPO, Internal Audit, Compliance Manager e Risk Manager delle principali imprese italiane

Gli obiettivi dell'Osservatorio

- ❑ Quantificare il **mercato** della sicurezza informatica in Italia
- ❑ Comprendere l'impatto del **Regolamento UE** sulla protezione dei dati e sulle nuove professionalità
 - ❑ Indagare come i **trend dell'innovazione digitale** impattano sulla gestione dell'information security e della privacy
 - ❑ Identificare **le competenze e i ruoli** coinvolti nella gestione dell'information security e le modalità di gestione del **fattore umano**
 - ❑ Analizzare le modalità di gestione del **rischio cyber**
 - ❑ Monitorare lo stato di **adozione di sistemi** di information security e privacy nelle organizzazioni italiane
- ❑ Studiare gli impatti sulle **grandi imprese** e sulle **PMI**
- ❑ Identificare i **casi di successo**



Le evidenze della Ricerca

La rilevanza e il mercato

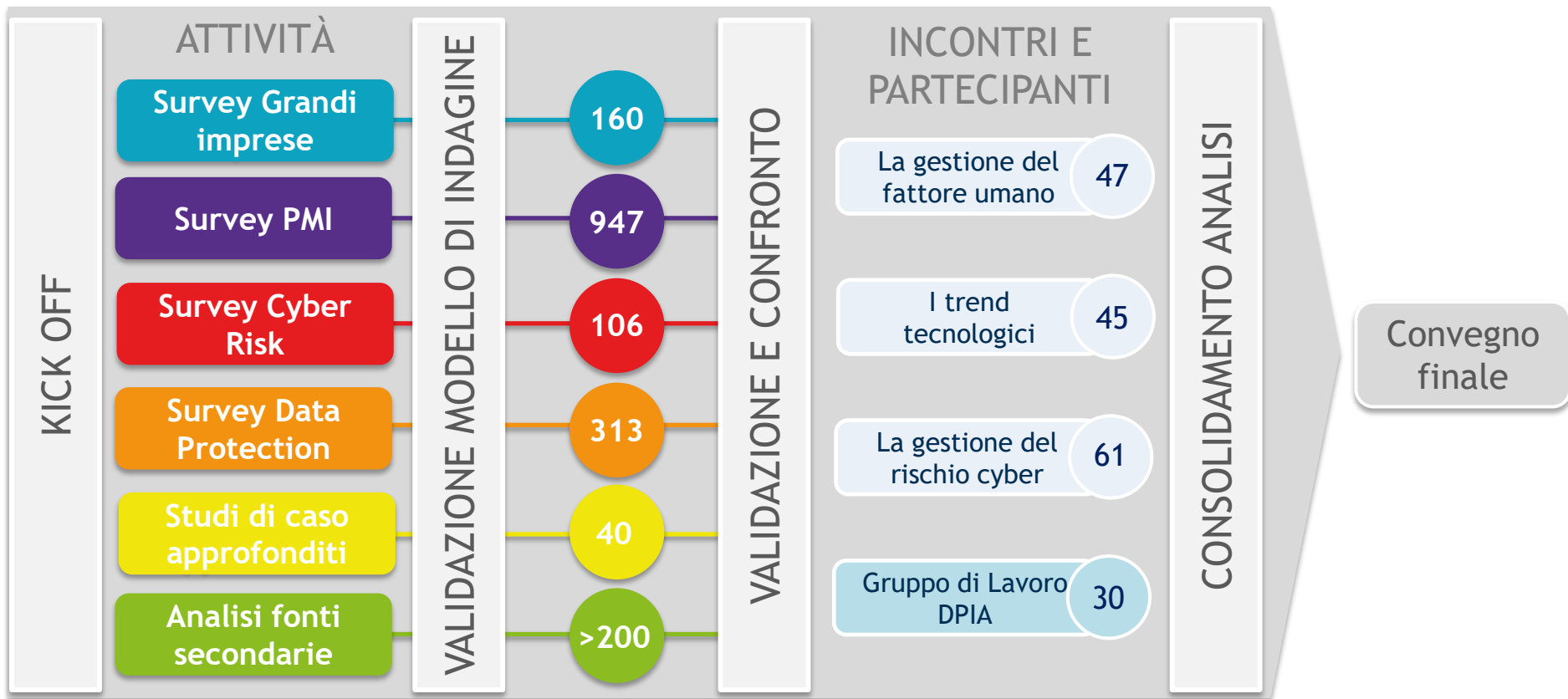
La figura del CISO e le
competenze

Il percorso di
adeguamento al GDPR

Il Cyber Risk

Le PMI

La metodologia di Ricerca



Le priorità di investimento dell'innovazione digitale

2017



Survey Innovation dell'Osservatorio Digital Transformation Academy che ha visto il coinvolgimento di oltre 200 Innovation Manager e CIO di grandi organizzazioni italiane nel 2016 e 2017

Le priorità di investimento dell'innovazione digitale

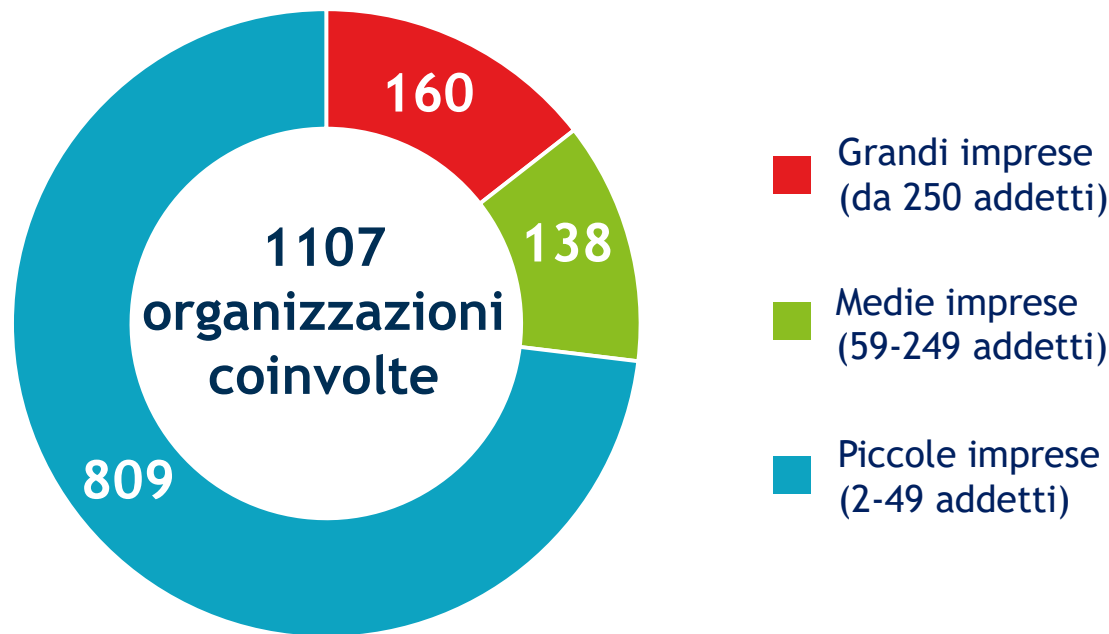
2017



2018

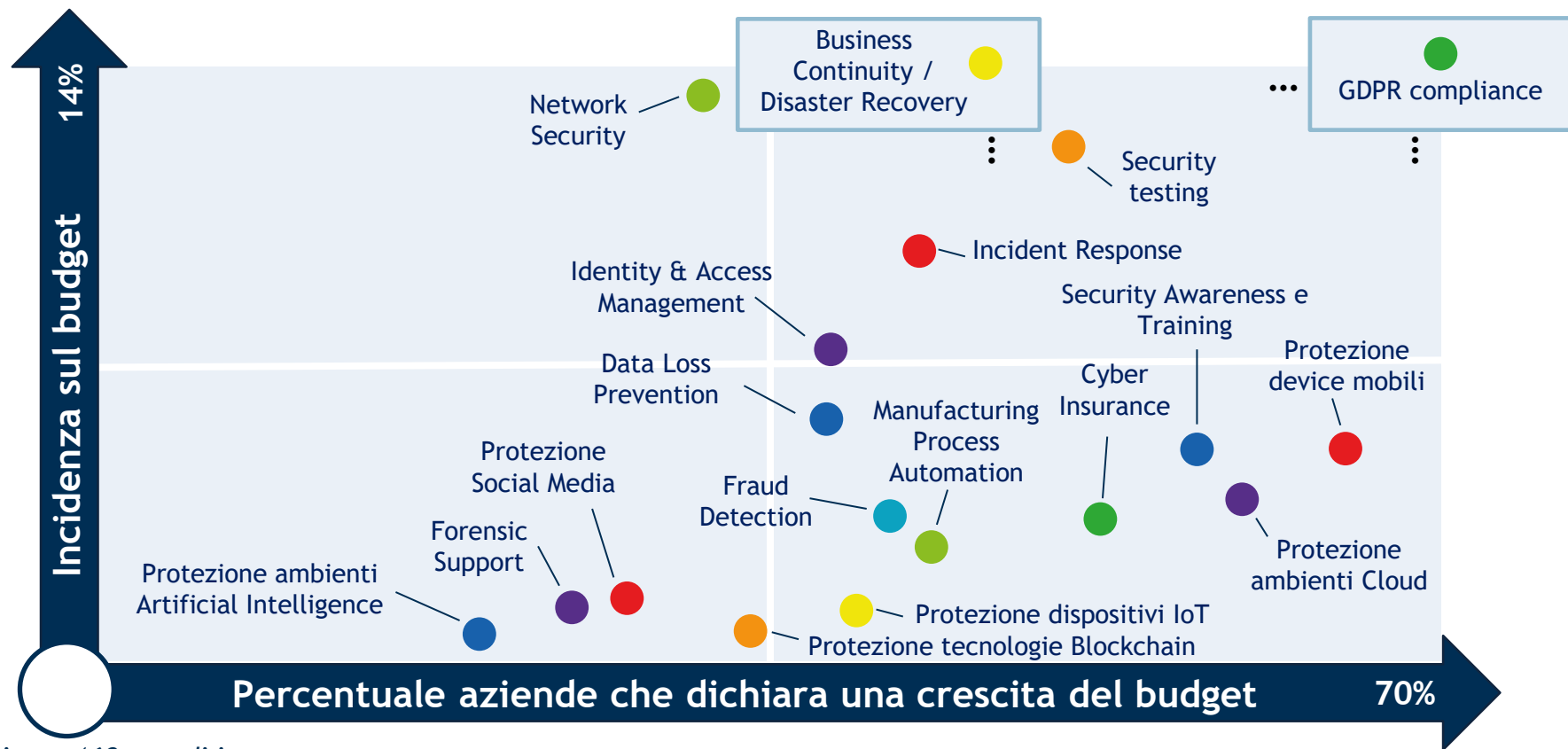


Survey Innovation dell'Osservatorio Digital Transformation Academy che ha visto il coinvolgimento di oltre 200 Innovation Manager e CIO di grandi organizzazioni italiane nel 2016 e 2017



Campione: 1107 organizzazioni italiane

La scomposizione del mercato Information Security



Campione: 160 grandi imprese

Le evidenze della Ricerca

La rilevanza e il mercato

La figura del CISO e le
competenze

Il percorso di
adeguamento al GDPR

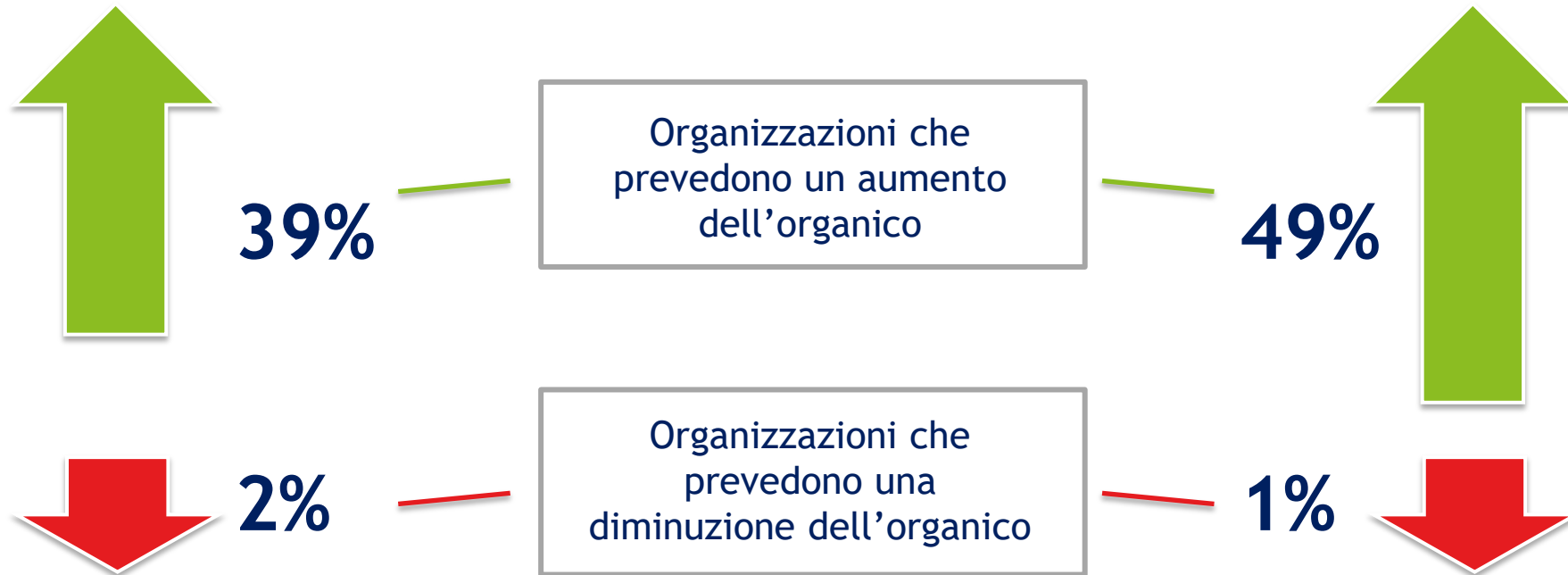
Il Cyber Risk

Le PMI

La crescita dell'organico

Information Security

Privacy



Campione: 160 grandi imprese

La crescita dell'organico

Information Security



39%

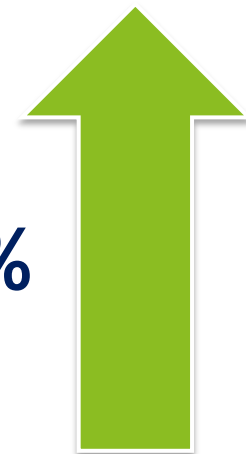


2%



Nel 2016
circa la metà
delle aziende non
aveva ancora
introdotto un CISO
in maniera
formalizzata

Privacy



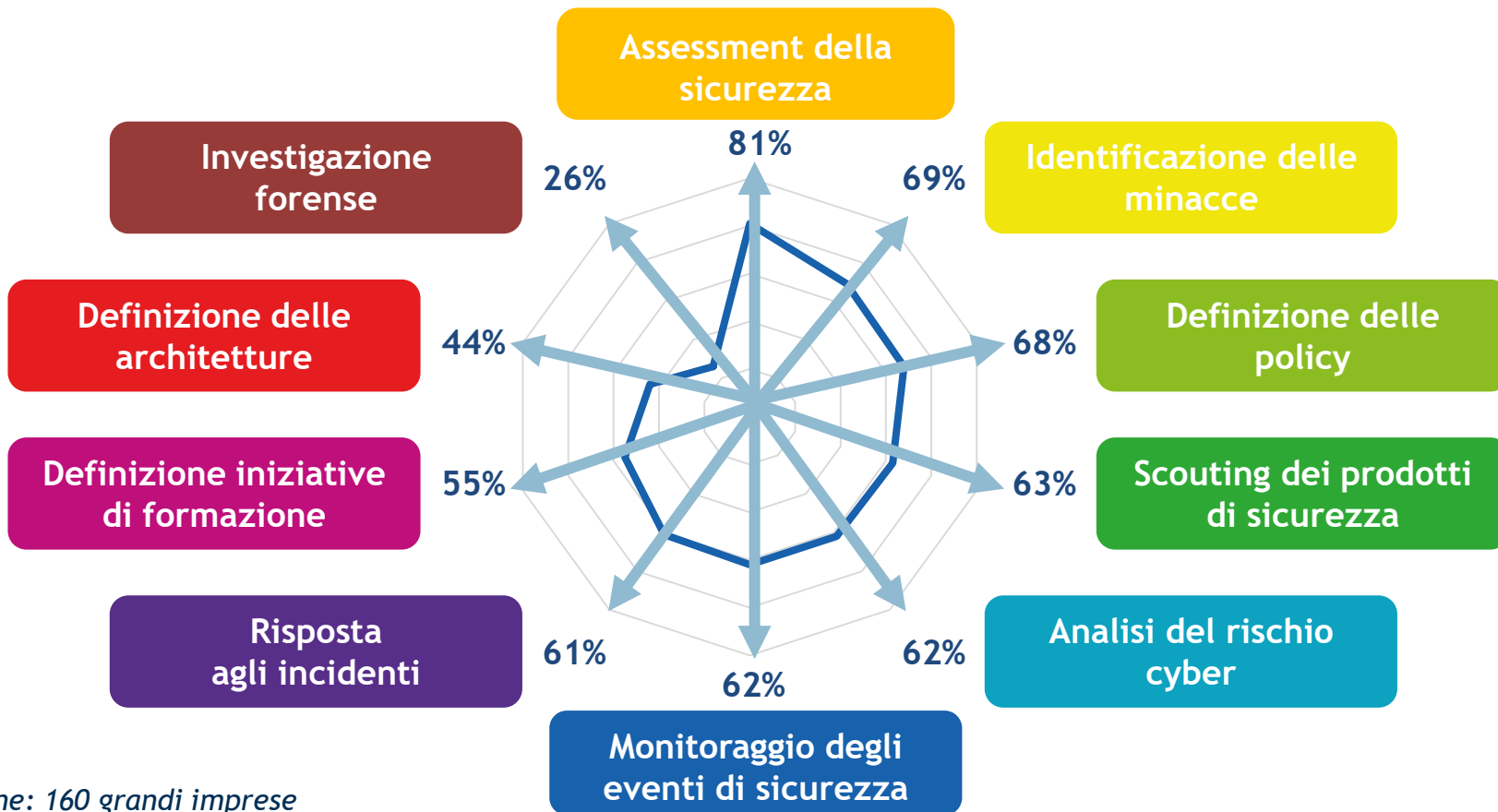
49%



1%

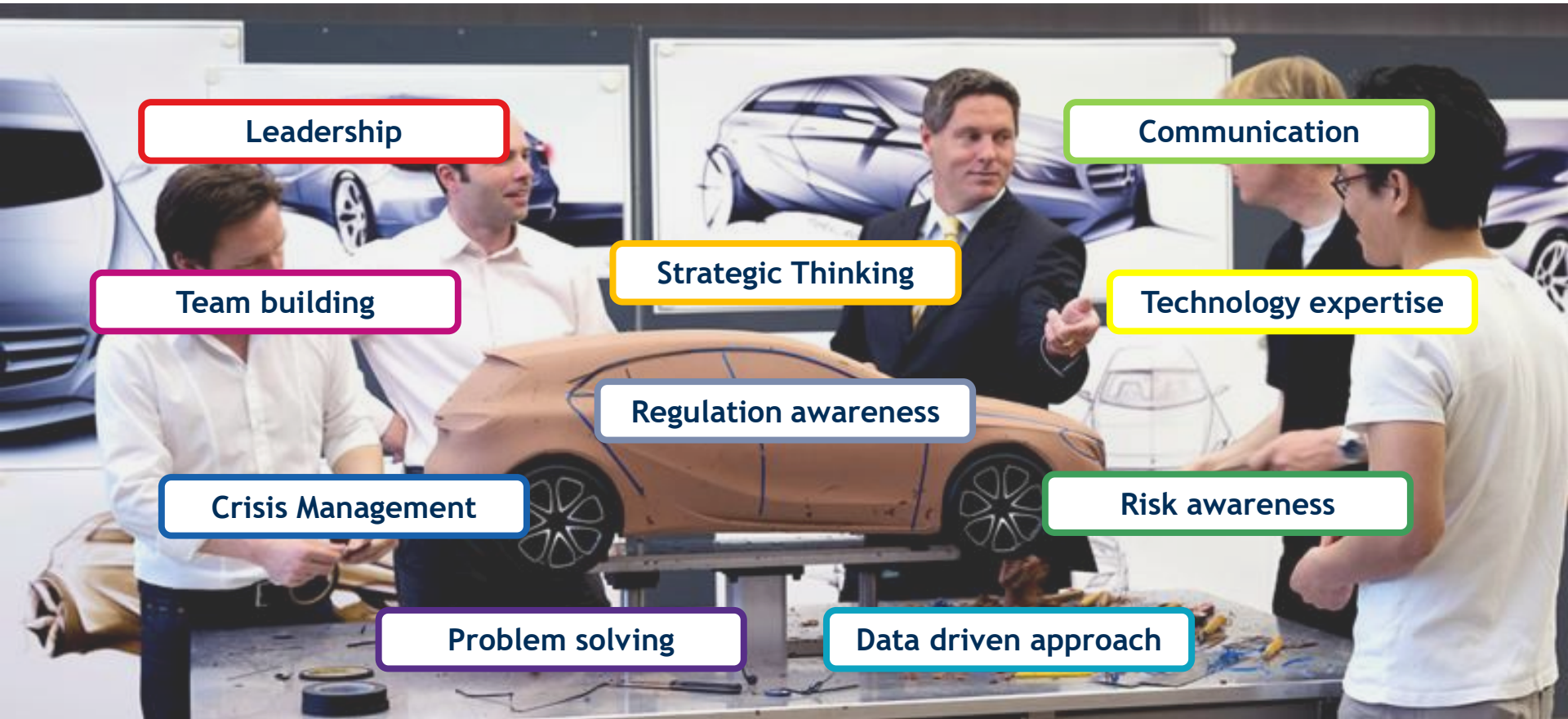
Campione: 160 grandi imprese

Le aree di responsabilità del CISO



Campione: 160 grandi imprese

Le caratteristiche del CISO moderno



Le nuove professionalità in ambito security

76%

SECURITY
ADMINISTRATOR

Rende
operative le
soluzioni
tecnologiche
di security

57%

SECURITY
ARCHITECT

Cura il
disegno
armonico e
coerente
delle
soluzioni di
sicurezza e
delle policy

56%

SECURITY
ENGINEER

Monitora i
sistemi e
propone
soluzioni
relative alla
risposta agli
incidenti

55%

SECURITY
ANALYST

Valuta le
vulnerabilità
che possono
interessare
reti,
apparati,
applicazioni
e servizi

39%

ETHICAL
HACKER

Mette in atto
soluzioni in
grado di
dimostrare le
vulnerabilità
di cui soffre
l'azienda

28%

SECURITY
DEVELOPER

Sviluppa
soluzioni di
security

19%

MACHINE
LEARNING
SPECIALIST

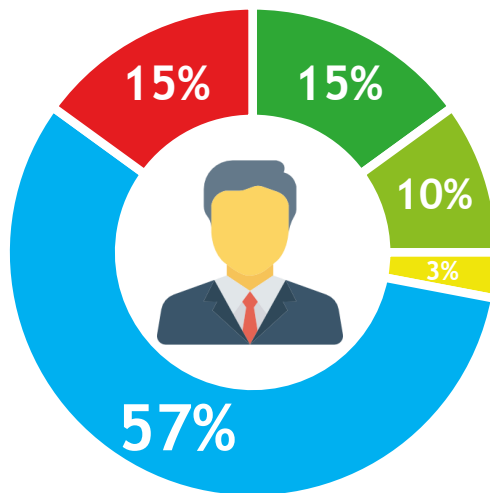
Sviluppa e
monitora
sistemi di
risposta in
real-time

Campione: 160 grandi imprese

Il Data Protection Officer - DPO

Presenza

- Figura formalizzata interna all'azienda
- Figura non formalizzata interna all'azienda
- Responsabilità delegata a una figura esterna
- In introduzione nei prossimi 12 mesi
- Non esiste e non se ne prevede l'introduzione

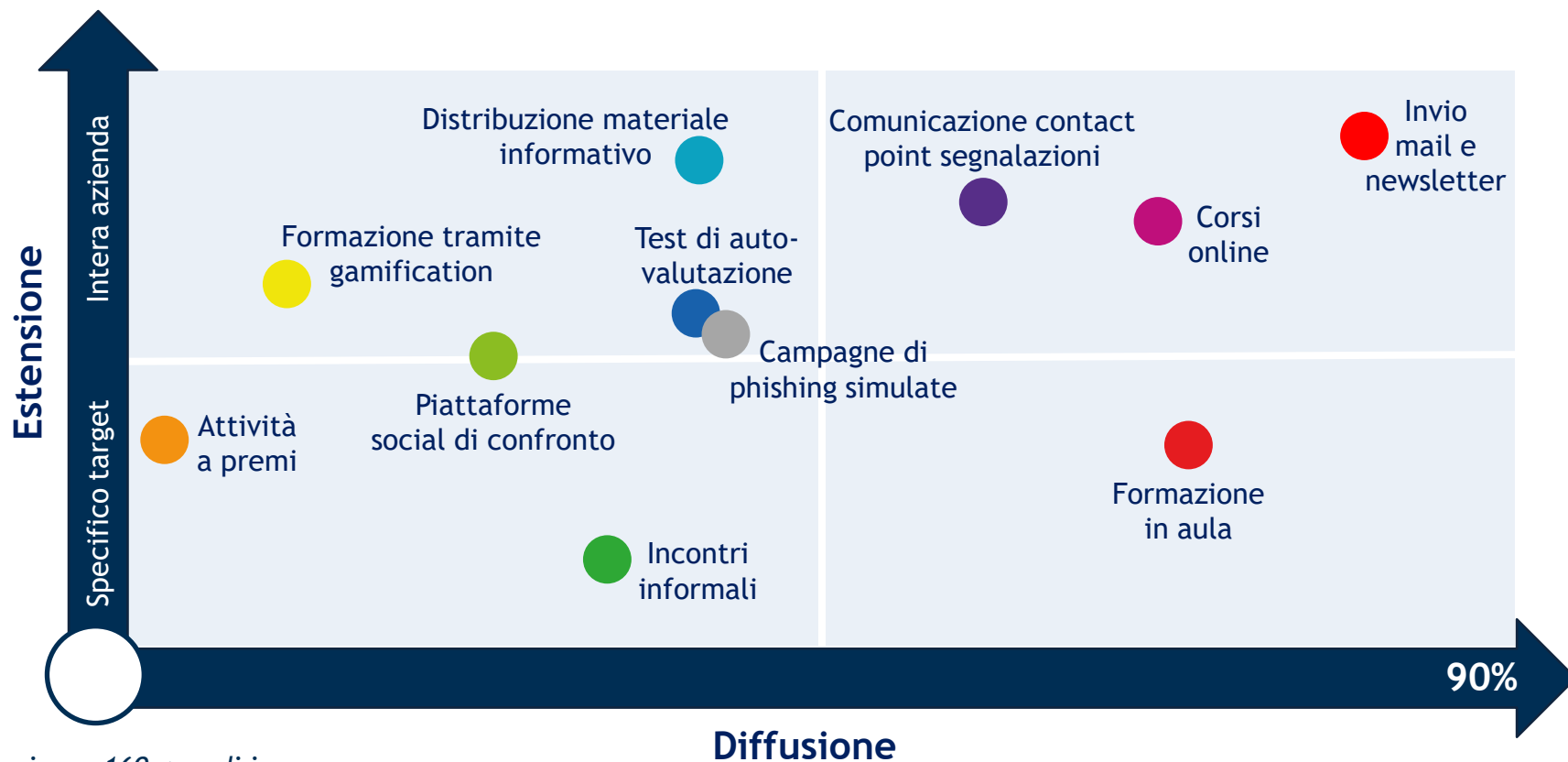


Attività



Campione: 160 grandi imprese

Le iniziative di sensibilizzazione



Campione: 160 grandi imprese

Le evidenze della Ricerca

La rilevanza e il mercato

La figura del CISO e le
competenze

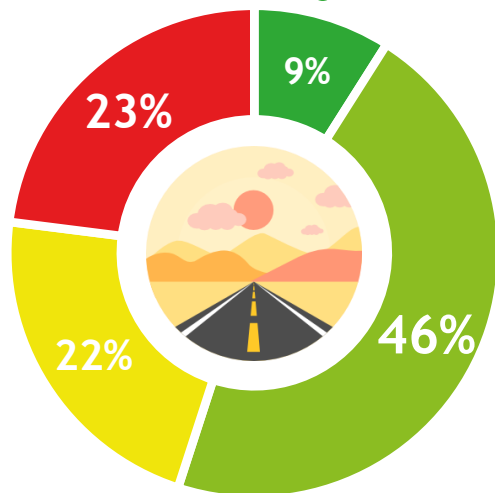
Il percorso di
adeguamento al GDPR

Il Cyber Risk

Le PMI

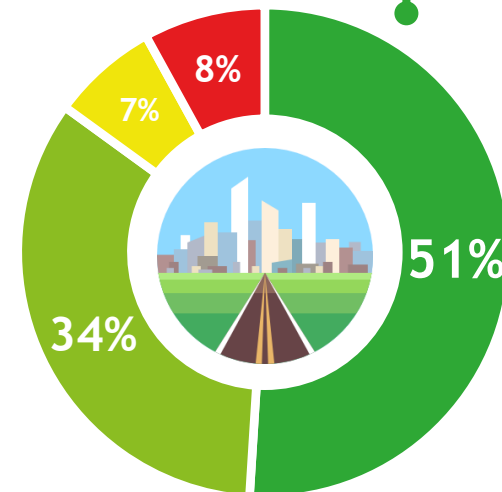
GDPR: l'awareness e le misure di adeguamento

2016



+42 %

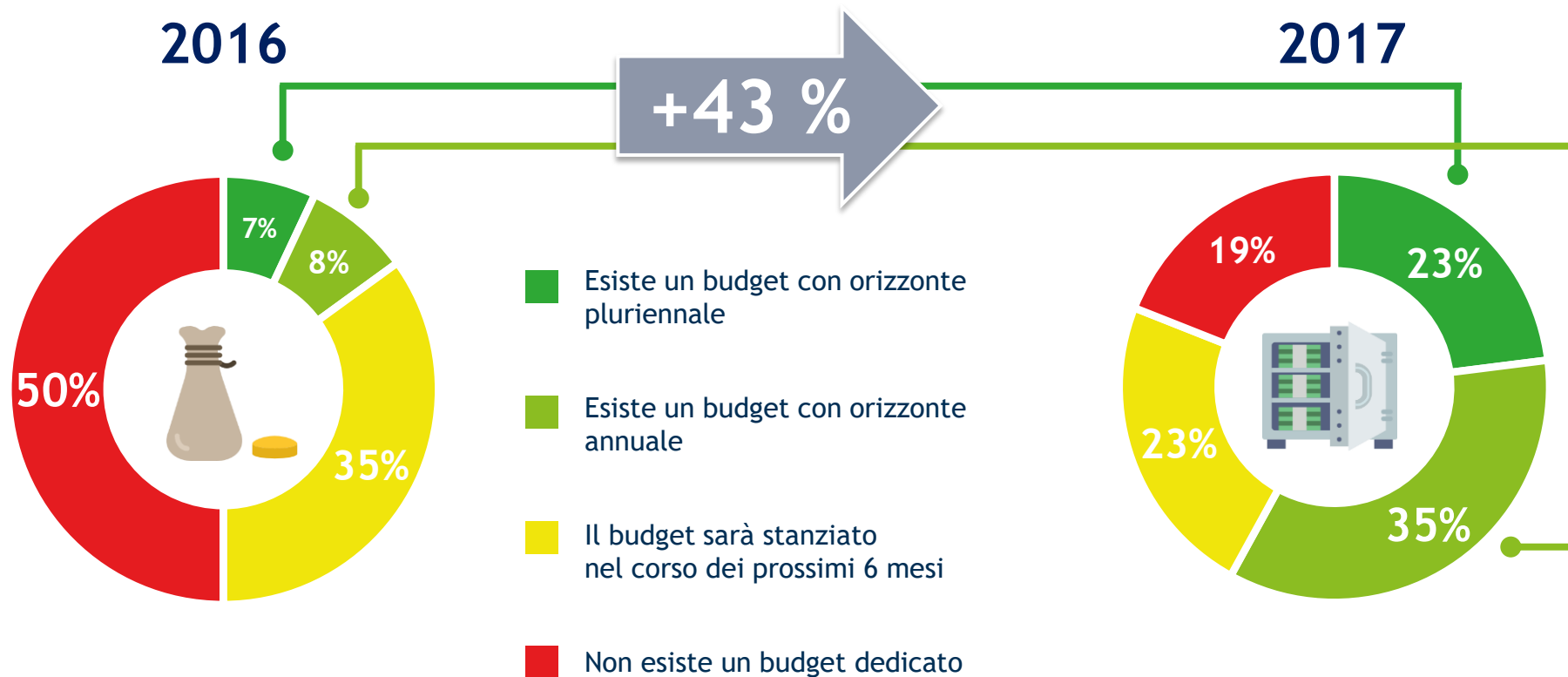
2017



- È in corso un progetto strutturato di adeguamento alla normativa
- È in corso un'analisi dei requisiti richiesti e dei piani di attuazione possibili
- Le implicazioni sono note nelle funzioni specialistiche ma il tema non è all'attenzione del vertice
- Le implicazioni del GDPR non sono note in dettaglio

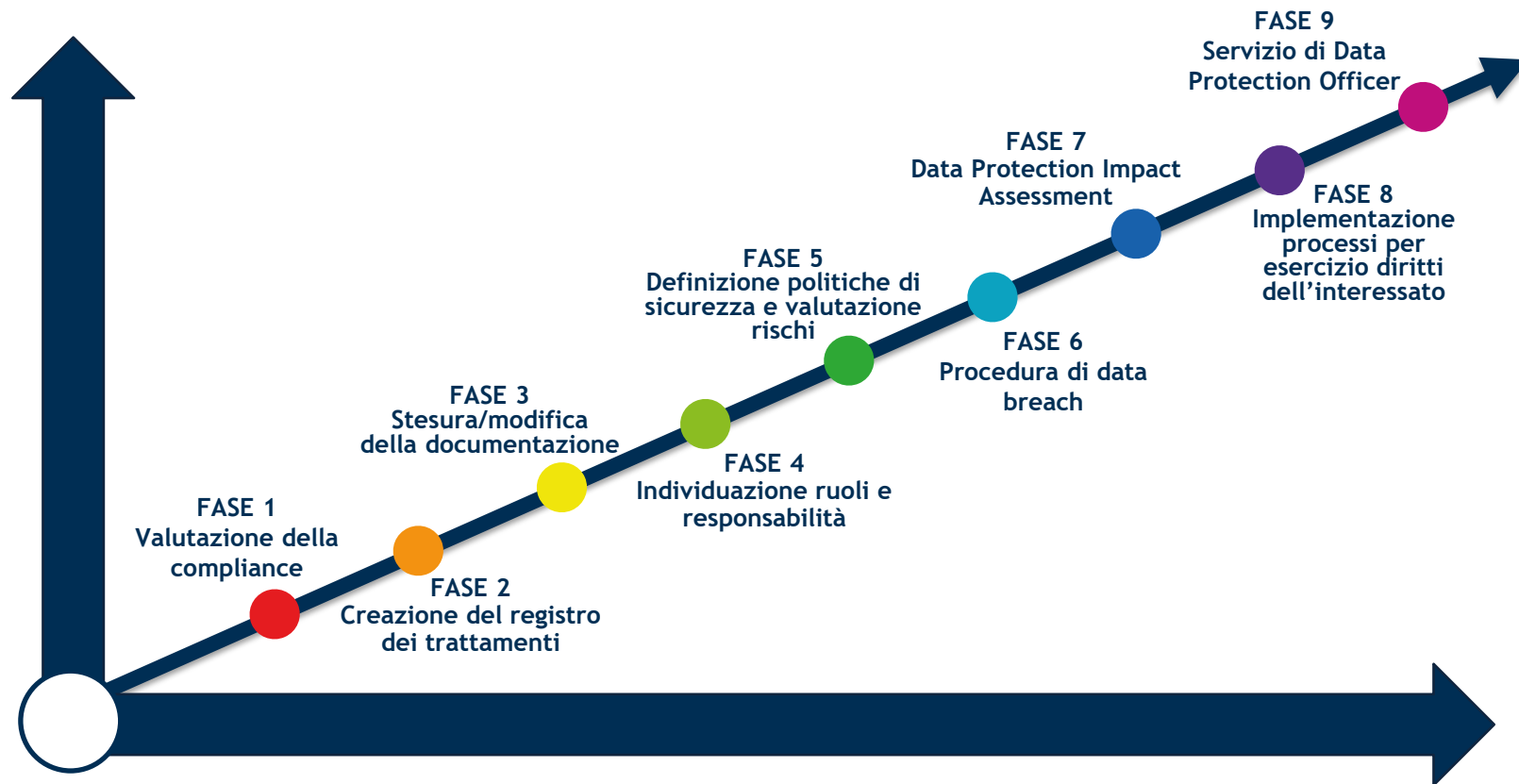
Campione: 160 grandi imprese

GDPR: l'orizzonte di pianificazione



Campione: 160 grandi imprese

Le fasi del percorso di adeguamento



Campione: 160 grandi imprese

Le fasi del percorso di adeguamento

Fase	Stato
Valutazione della compliance	
Individuazione dei ruoli e delle responsabilità	
Definizione delle politiche di sicurezza e valutazione dei rischi	
Creazione del registro dei trattamenti	
Stesura/modifica della documentazione	
Data Protection Impact Assessment	
Procedura di data breach	
Implementazione processi per l'esercizio dei diritti dell'interessato	
Servizio di Data Protection Officer	

Implementata

In corso

Prevista in futuro

Non prevista

Campione: 160 grandi imprese

Le evidenze della Ricerca

La rilevanza e il mercato

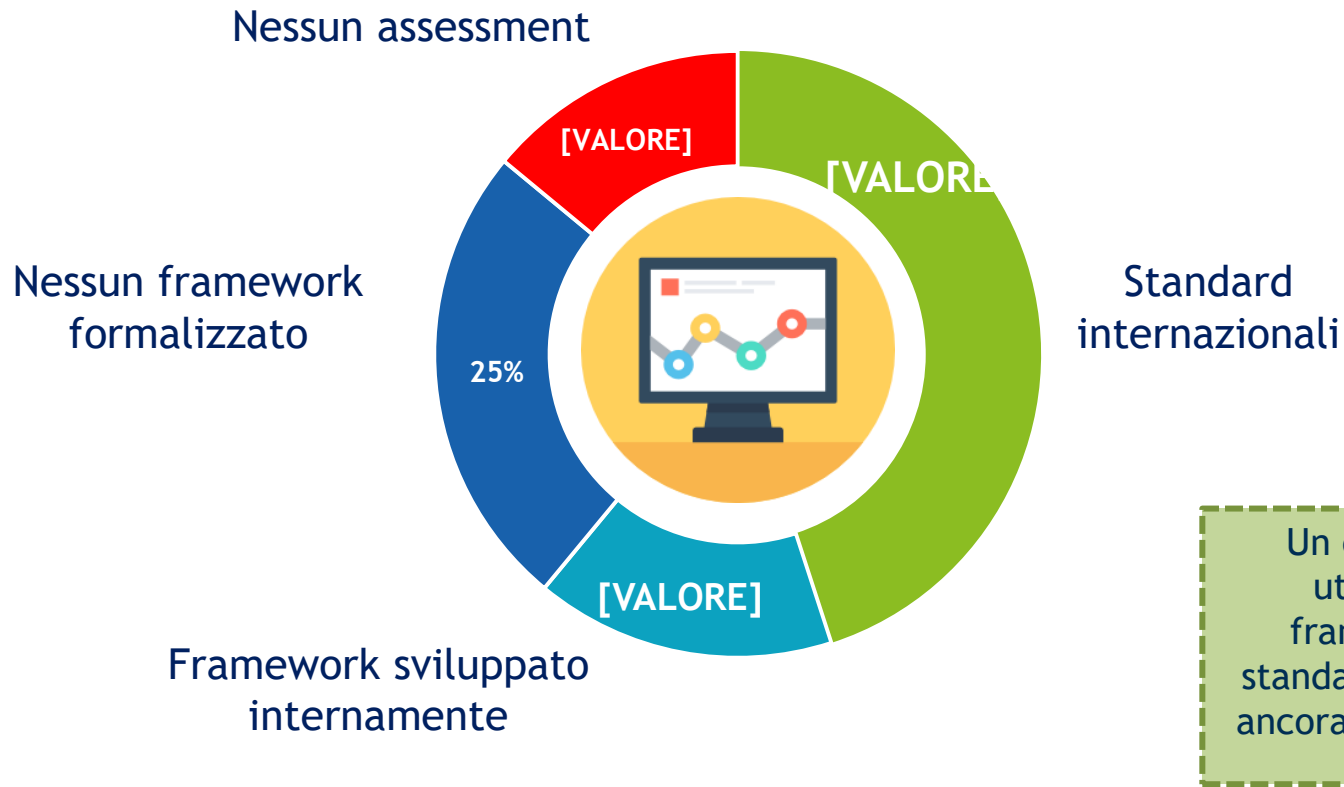
La figura del CISO e le
competenze

Il percorso di
adeguamento al GDPR

Il Cyber Risk

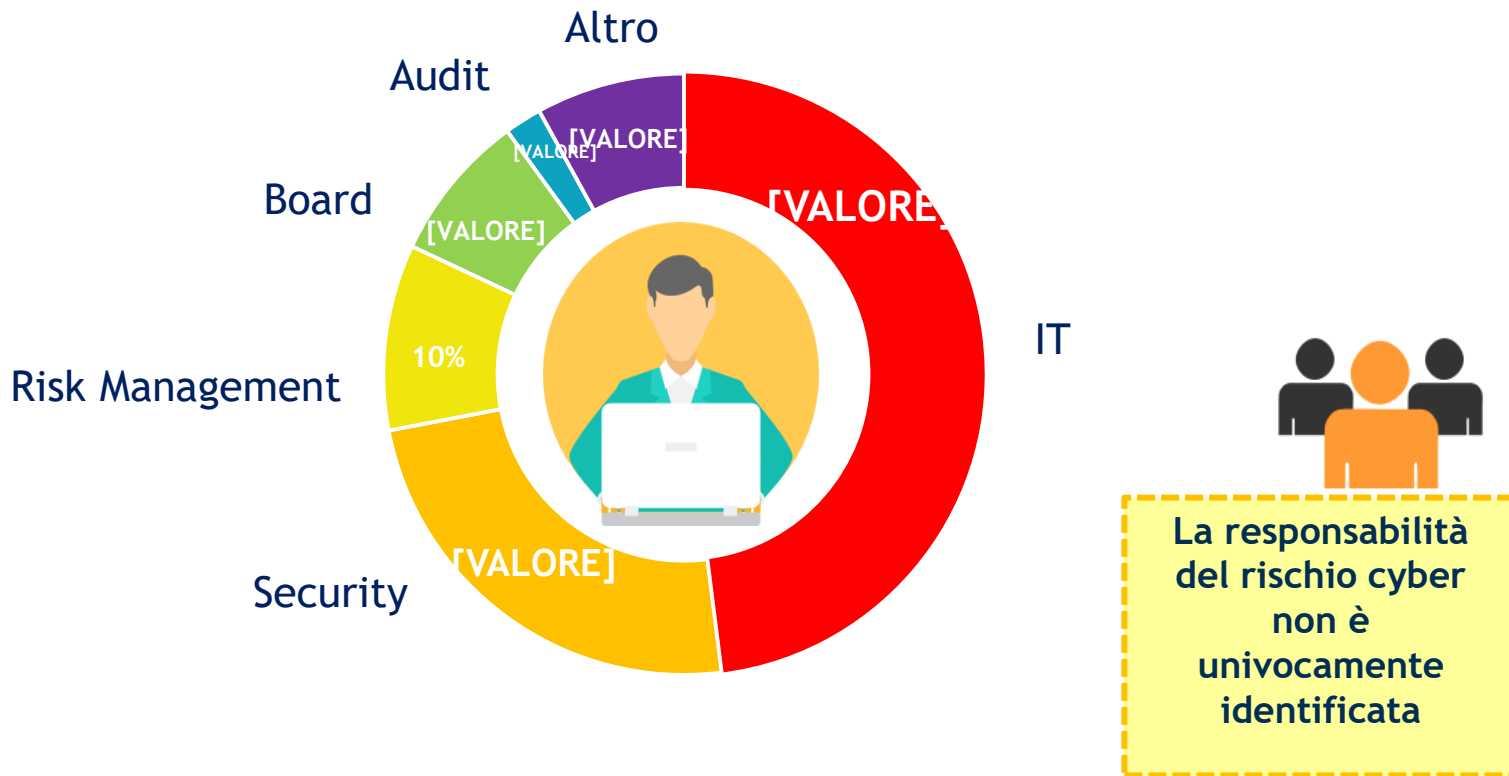
Le PMI

L'assessment del rischio cyber



Campione: 106 organizzazioni italiane

La responsabilità del rischio cyber



Campione: 106 organizzazioni italiane

Gli approcci per la gestione del rischio

Ignorato

Un determinato asset non è considerato critico

Accettato

Sono state valutate le implicazioni del rischio associato a un determinato asset, ma si è ritenuto che non fosse necessario alcun provvedimento

Mitigato

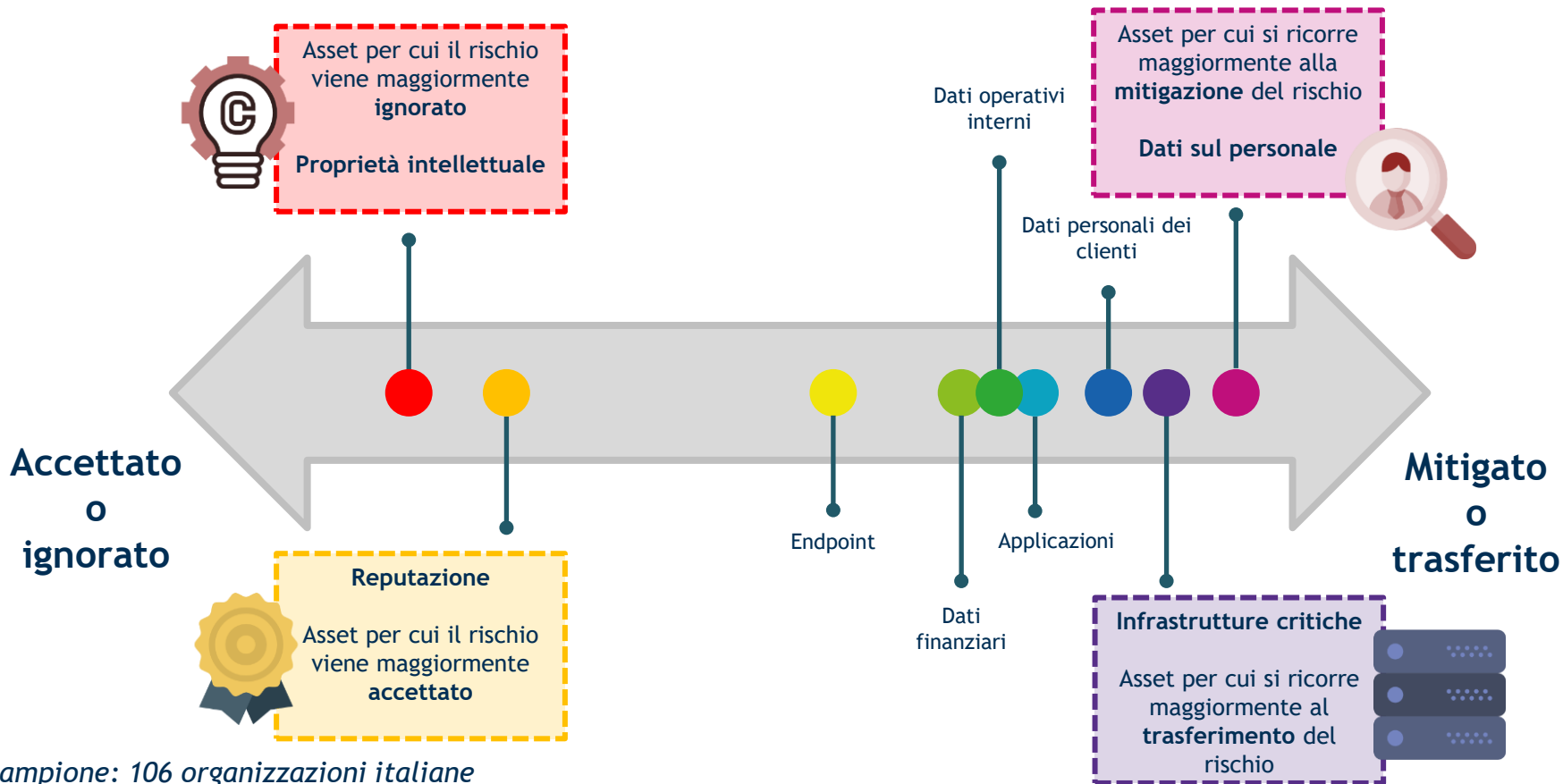
È stato definito un processo strutturato di gestione del rischio associato a un determinato asset, introducendo opportune soluzioni e procedure

Trasferito

Sono state stipulate polizze assicurative che coprono il rischio associato a un determinato asset

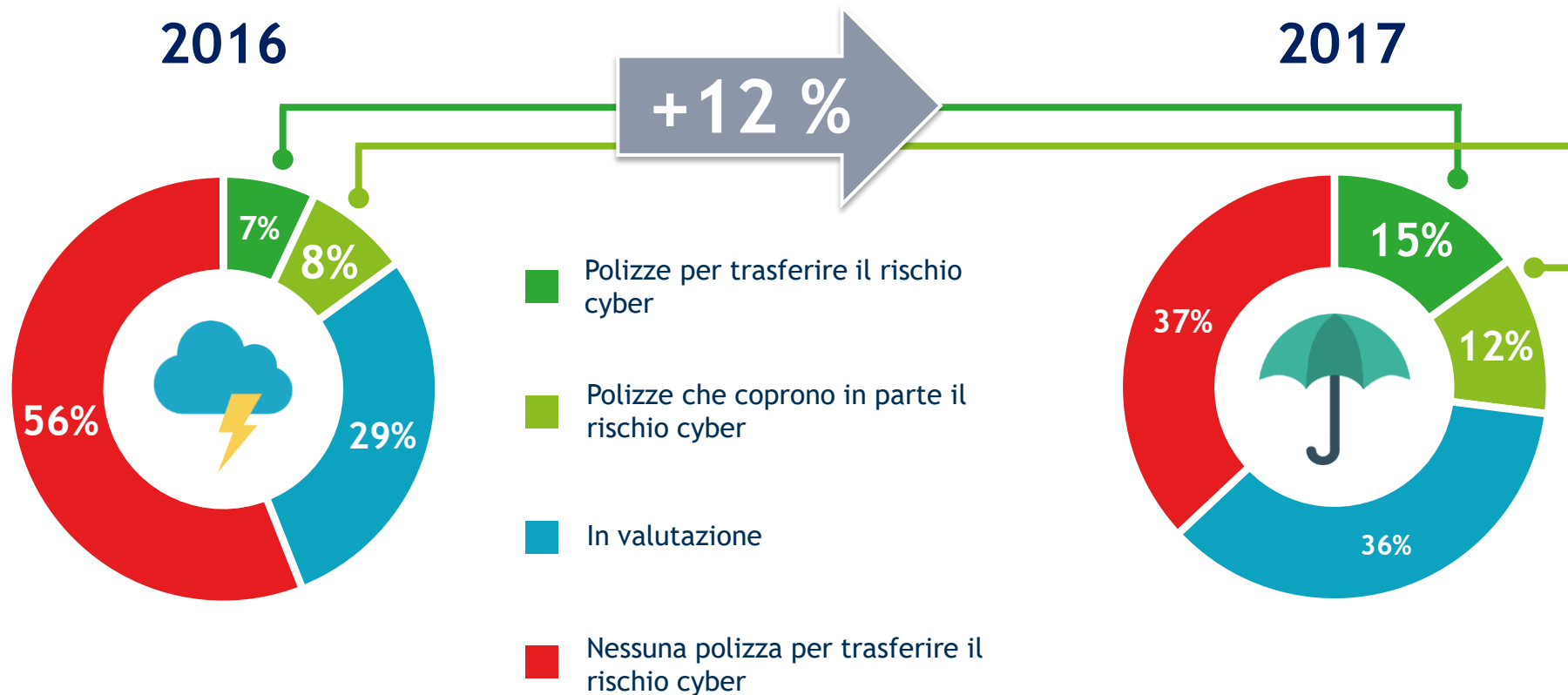
Campione: 106 organizzazioni italiane

Gli approcci per la gestione del rischio



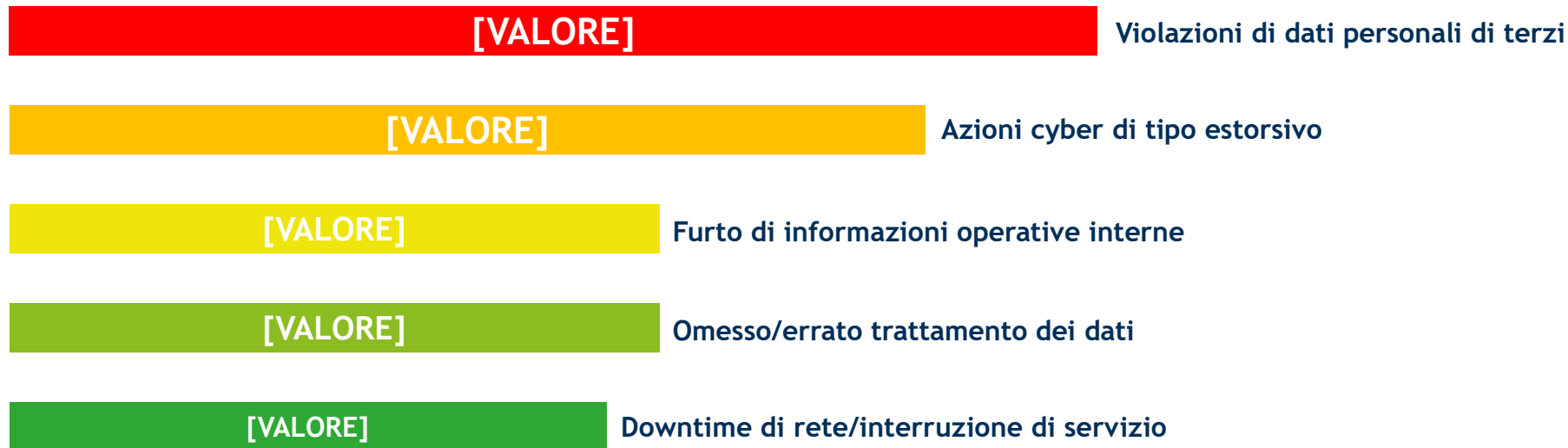
Campione: 106 organizzazioni italiane

Le polizze per trasferire il rischio cyber



Campione: 106 organizzazioni italiane

Le aree di copertura



L'82% delle coperture assicurative stipulate si attiva a seguito di danni legati a violazioni di dati personali di terzi



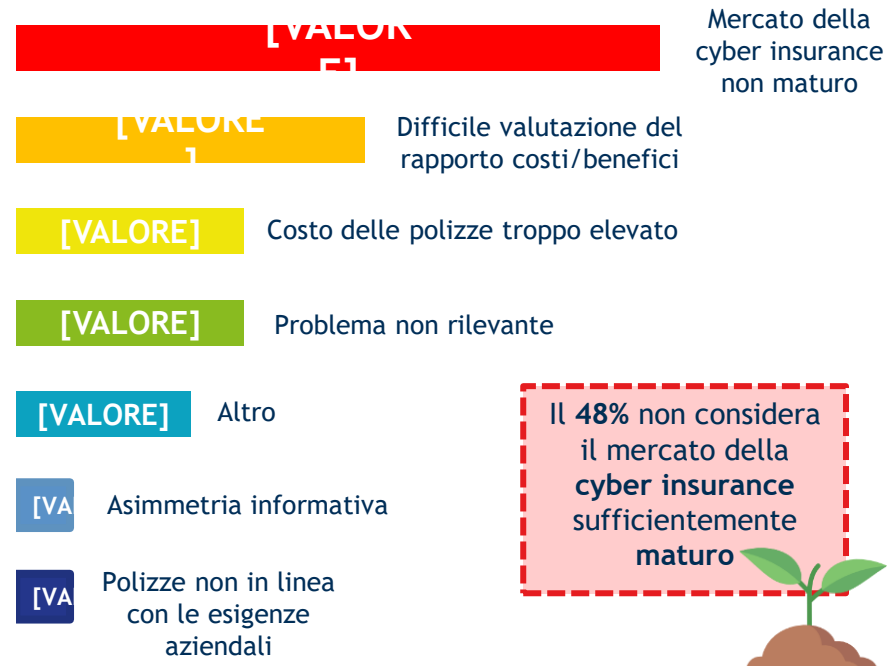
Campione: 106 organizzazioni italiane

La motivazioni che guidano la stipula delle polizze

Le motivazioni per il sì



Le motivazioni per il no



Campione: 106 organizzazioni italiane

Le evidenze della Ricerca

La rilevanza e il mercato

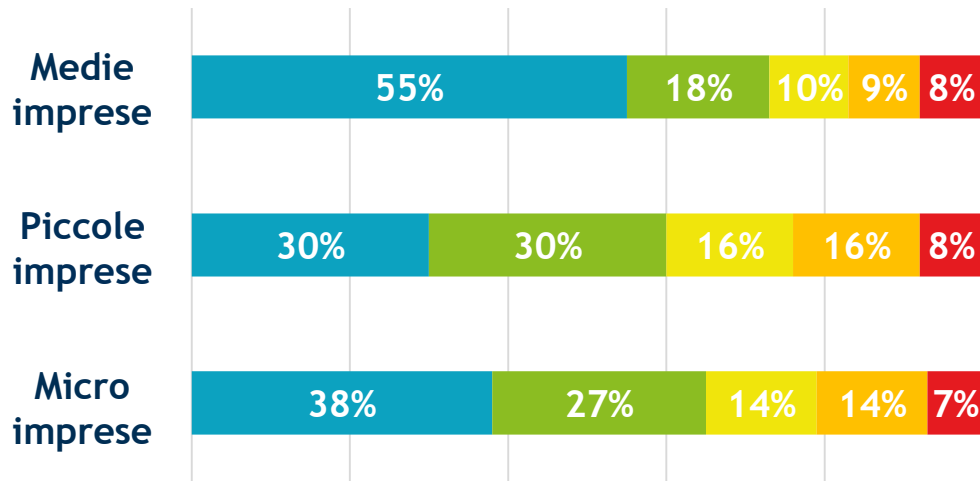
La figura del CISO e le
competenze

Il percorso di
adeguamento al GDPR

Il Cyber Risk

Le PMI

Le PMI: i trend tecnologici e l'impatto sulla security



Principale trend che influenza le scelte di security:

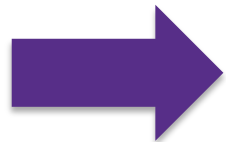


Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

Riassumendo...



Percorso impervio, difficile da percorrere con strumenti tradizionali



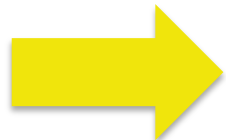
Mercato e investimenti in crescita, crescente attenzione verso i temi dell'innovazione digitale



Percorsi delineati di adeguamento al GDPR, investimenti consistenti e progettualità di ampio respiro



Gestione del rischio cyber e progressiva presa di coscienza degli strumenti per mitigarlo (e trasferirlo)



Progressiva strutturazione organizzativa, con maggiore strategicità della figura del CISO