AGENDA

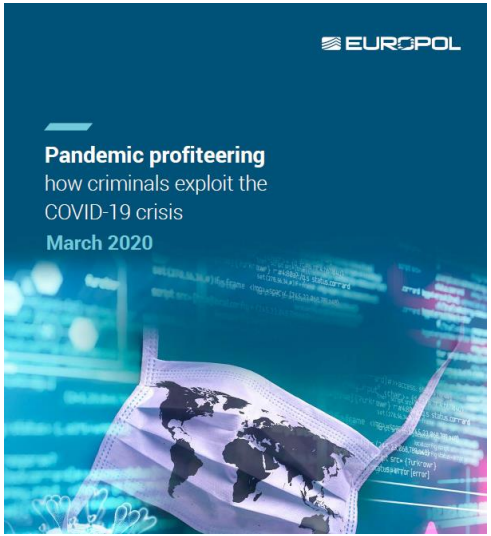
Proteggere dati e informazioni critiche per il business aziendale oggi è più che mai prioritario. Tra tutte le forme di attacco, il Ransomware, che ha l'obiettivo primario di estorcere denaro a fronte di un vero e proprio sequestro di informazioni vitali, è sempre più mirato, evoluto e distruttivo. Mascherando ad arte l'origine delle incursioni, le nuove minacce mettono in discussione l'approccio tradizionale alla cybersecurity, coinvolgendo anche le infrastrutture di backup e data recovery, troppo spesso non sufficientemente protette.

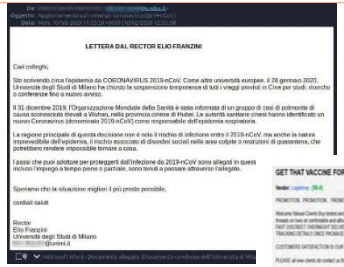
- Cyber resilience: qual è il livello di maturità delle aziende italiane;
- L'evoluzione degli attacchi Ransomware e dei Data Breach;
- I sistemi di sicurezza che blindano il dato e assicura la continuità del business;
- La gestione di un attacco ransomware e il corretto recovery dei dati;
- La ripartenza dopo un attacco ai sistemi di backup;
- La gestione della crisi e l'applicazione dell'analisi forense;
- Il data recovery GDPR compliant.

Ne parleremo con:

- 11:30 – 11.45 **Elena Vaciago**, Associate Research Manager di **The Innovation Group**
- 11.45 – 12.00 **Fabio Bucciarelli**, Senior Security Advisor di **Lutech**
- 12.00 – 12.15 **Emiliano Campagnoli**, Data Protection Solution Presales System Engineer di **Dell Technologies**
- 12:15 – 12:30 **Domande & Risposte**

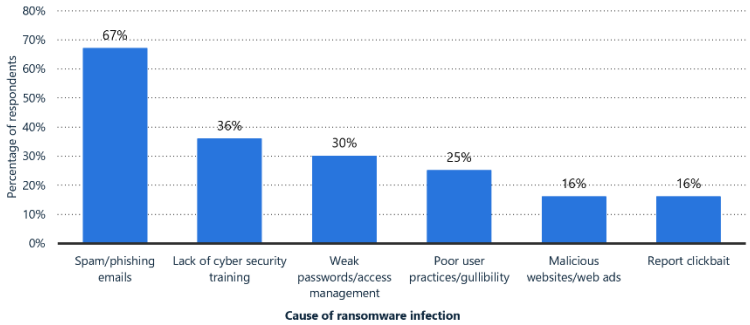
ALERT: crescita dei Rischi Cyber nei giorni dell'epidemia da Covid-19



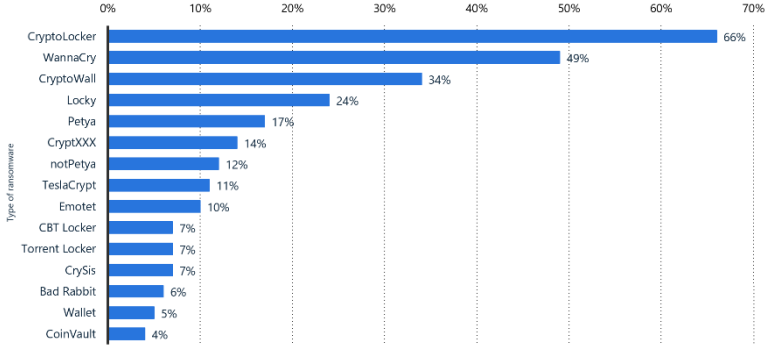


Attacchi Ransomware: sempre più sofisticati, con richieste di riscatto che superano i milioni di euro

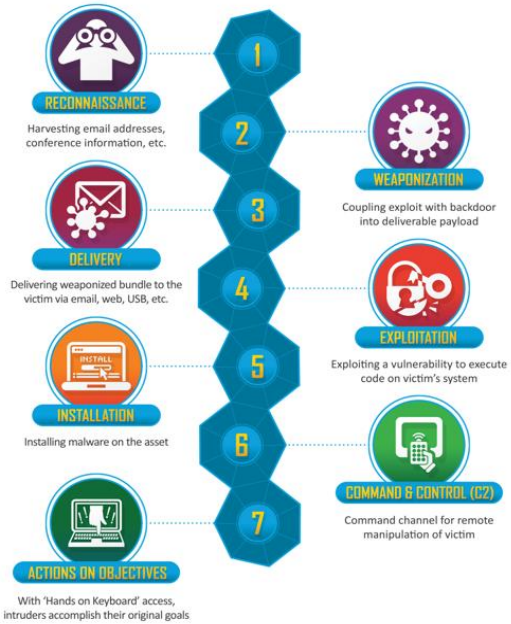
Leading cause of ransomware infection 2019



Share of MSP clients who experienced a ransomware attacks 2019, by strain



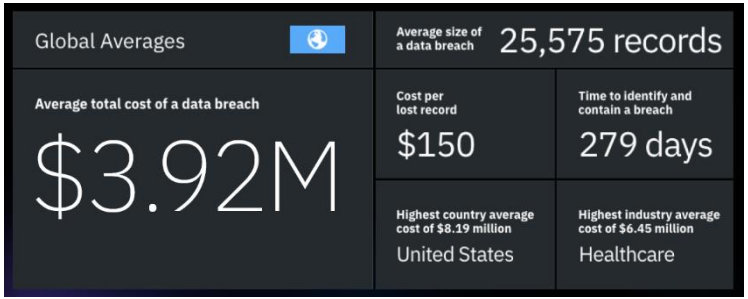
Quali sono le fasi di un attacco Ransomware avanzato?



Fonte: Lockheed Martin, The Cyber Kill Chain Framework

Fonte: Datto , Worldwide; Oct 2019, Global State of the Channel Ransomware Report, 1,400 managed services providers

Data Breach: aumenta il costo, il tempo per la risoluzione dell'incidente, il numero di aziende colpite



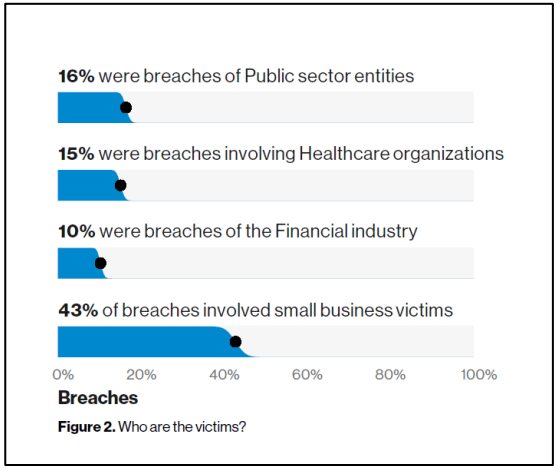
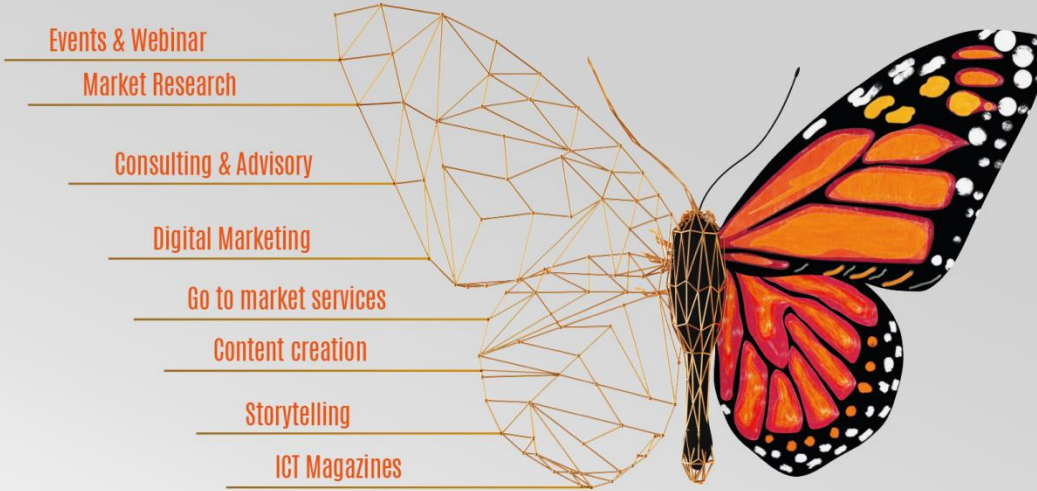


Figure 2. Who are the victims?

- Il **costo medio** di un data breach è oggi di 3,9 milioni di dollari (era di 3,6 milioni di dollari 2 anni fa), e la dimensione di un data breach è in media di 25.575 record (rispetto ai 24.000 record di 2 anni fa).
- Il **tempo medio** che intercorre tra il momento in cui avviene l'incidente e il contenimento dello stesso, è cresciuto del 4,9% tra il 2018 e il 2019: oggi si attesta su **279 giorni**, di cui 206 per la fase iniziale di individuazione del breach e 73 giorni per la risoluzione dell'incidente.
- I **settori** che registrano un maggior numero di data breach sono il settore pubblico, sanitario, finanziario.

Fonte: 2019 Data Breach Study, di Ponemon Institute e IBM Security, Verizon 2019 Data Breach Investigations Report



TIGSURVEY

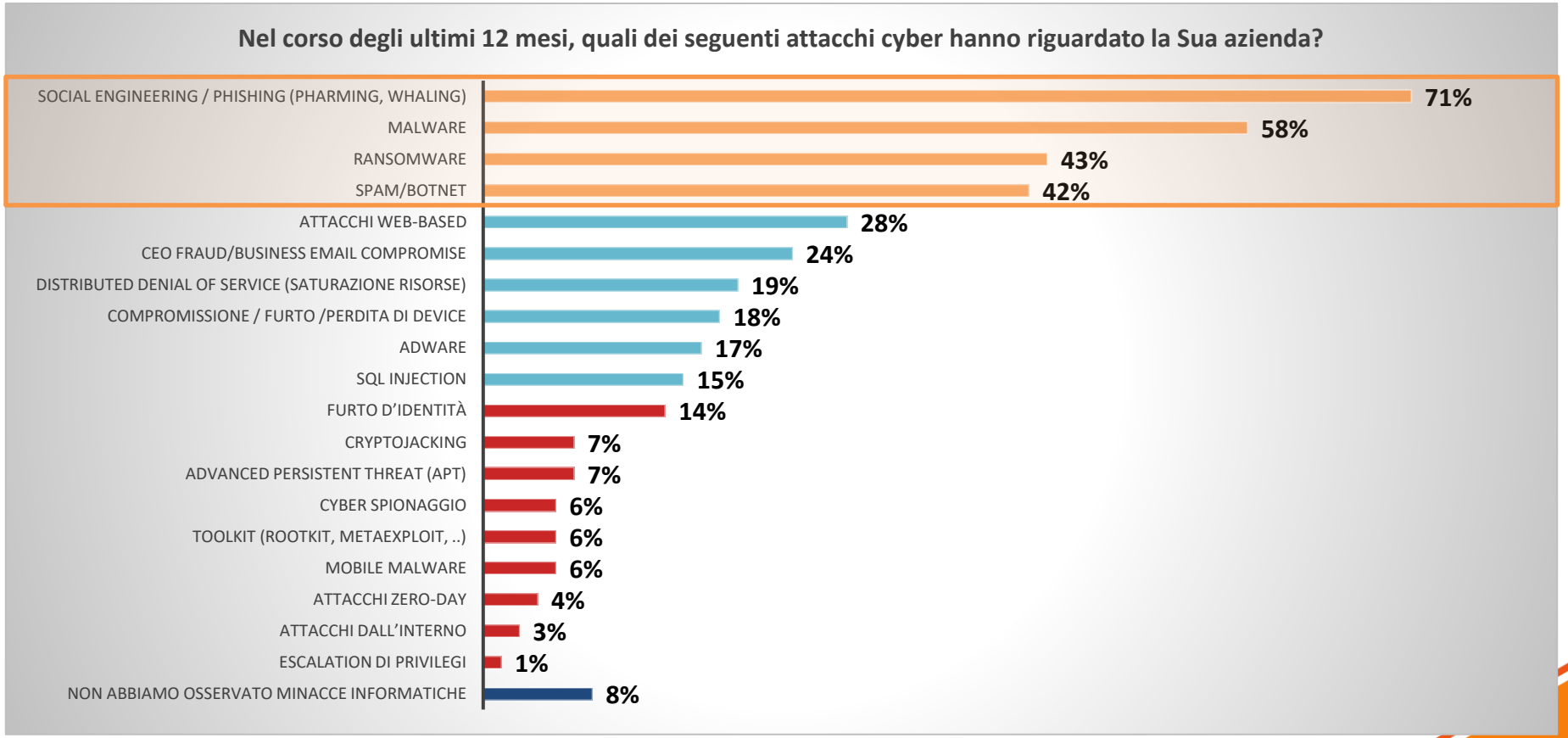
Cyber Risk Management 2020

A cura di: **Elena Vaciago,**
Associate Research Manager, The Innovation Group

The Innovation Group
Innovating business and organizations through ICT

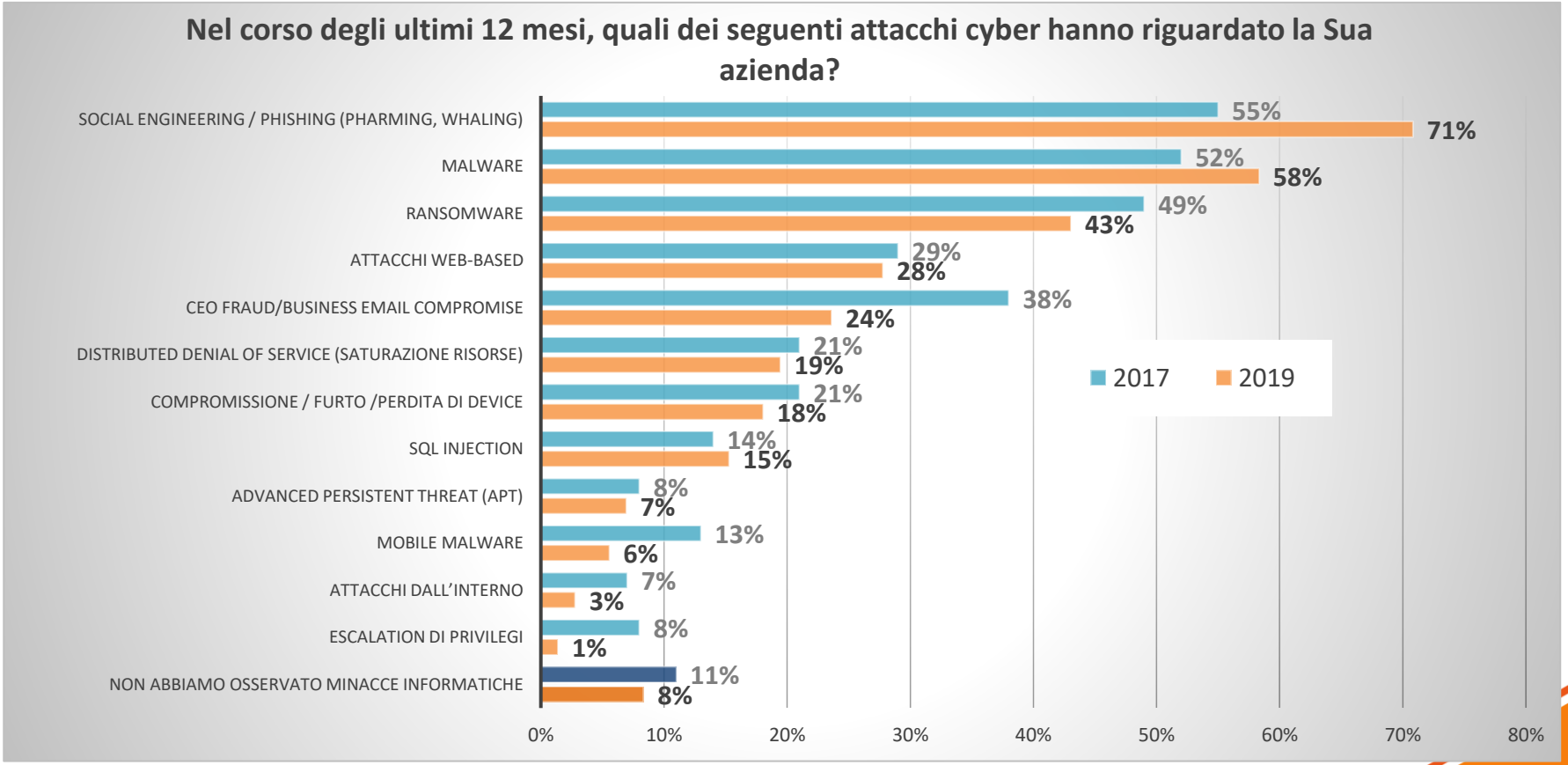
INDIGO COMMUNICATION

Il Phishing è oggi la minaccia cyber osservata con maggiore frequenza, seguita da malware, ransomware, spam



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 72 aziende italiane

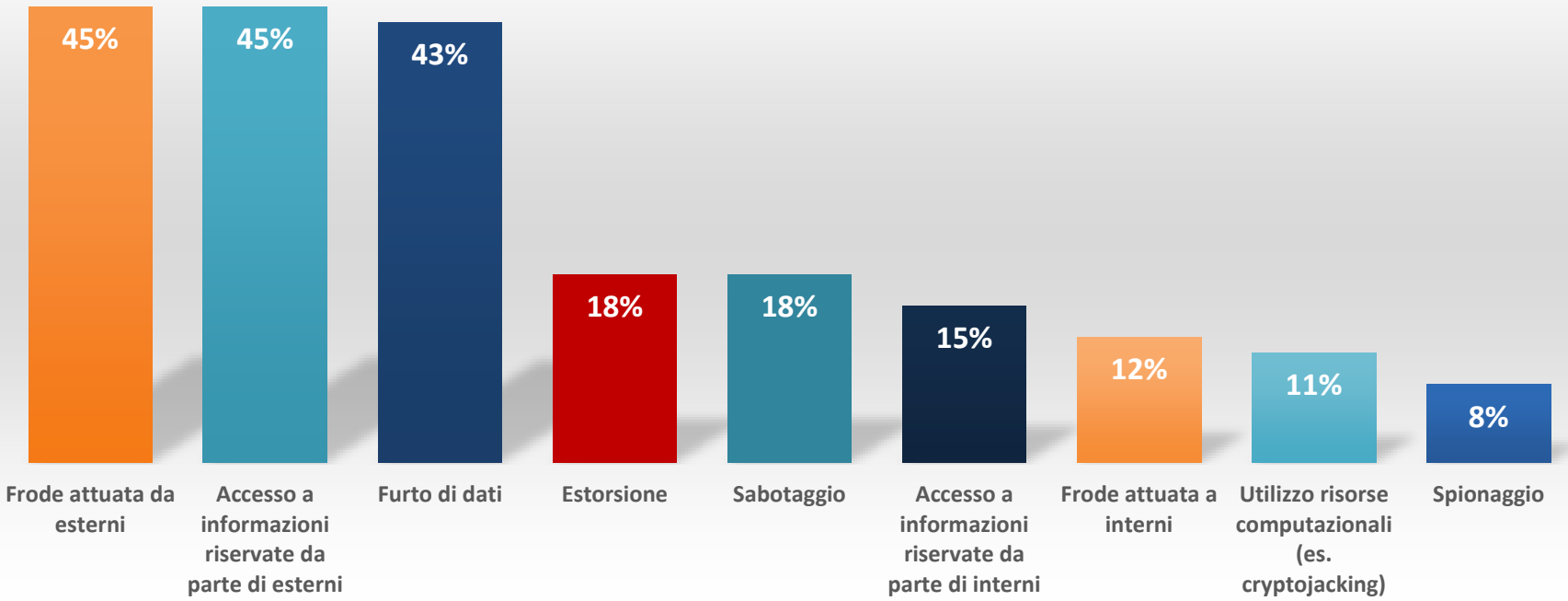
Negli ultimi 2 anni, lo scenario è rimasto simile in termini di classifica delle minacce. Diminuisce chi non osserva alcuna minaccia



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 72 aziende italiane VS. CRM Survey 2018

Le motivazioni che spingono il cyber crime sono molteplici, ma prevalgono nettamente quelle a scopo economico

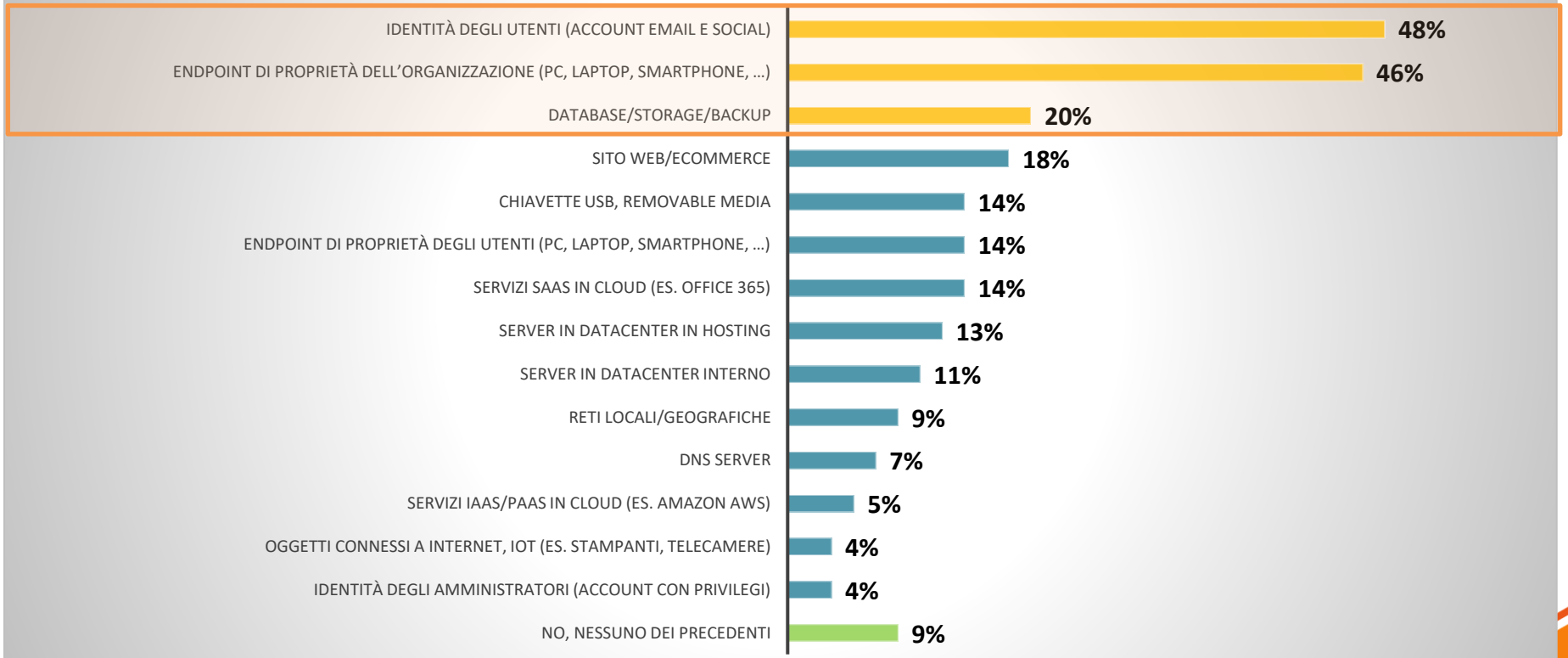
Quali erano le finalità degli attacchi osservati?



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 65 aziende italiane

Gli ambienti più colpiti sono le identità degli utenti, gli Endpoint e lo Storage dell'azienda, ma non sono i soli: compare anche il Cloud

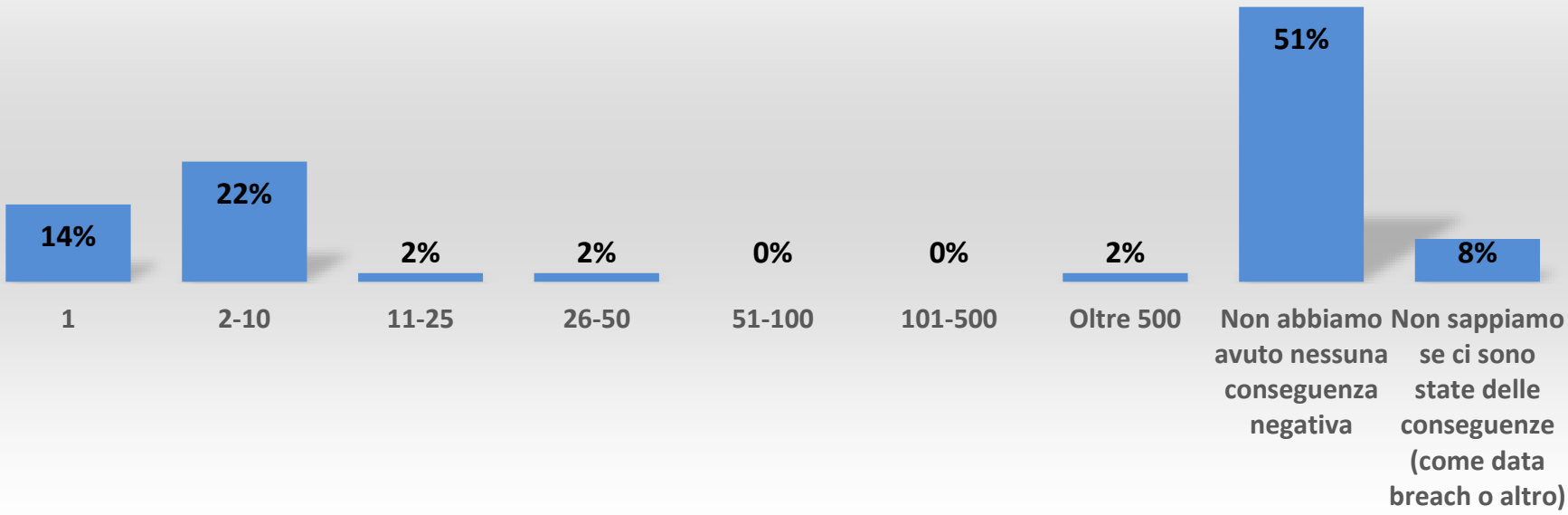
Gli attacchi osservati nel 2019 hanno comportato incidenti informatici per i seguenti ambienti/sistemi ICT?



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 56 aziende italiane

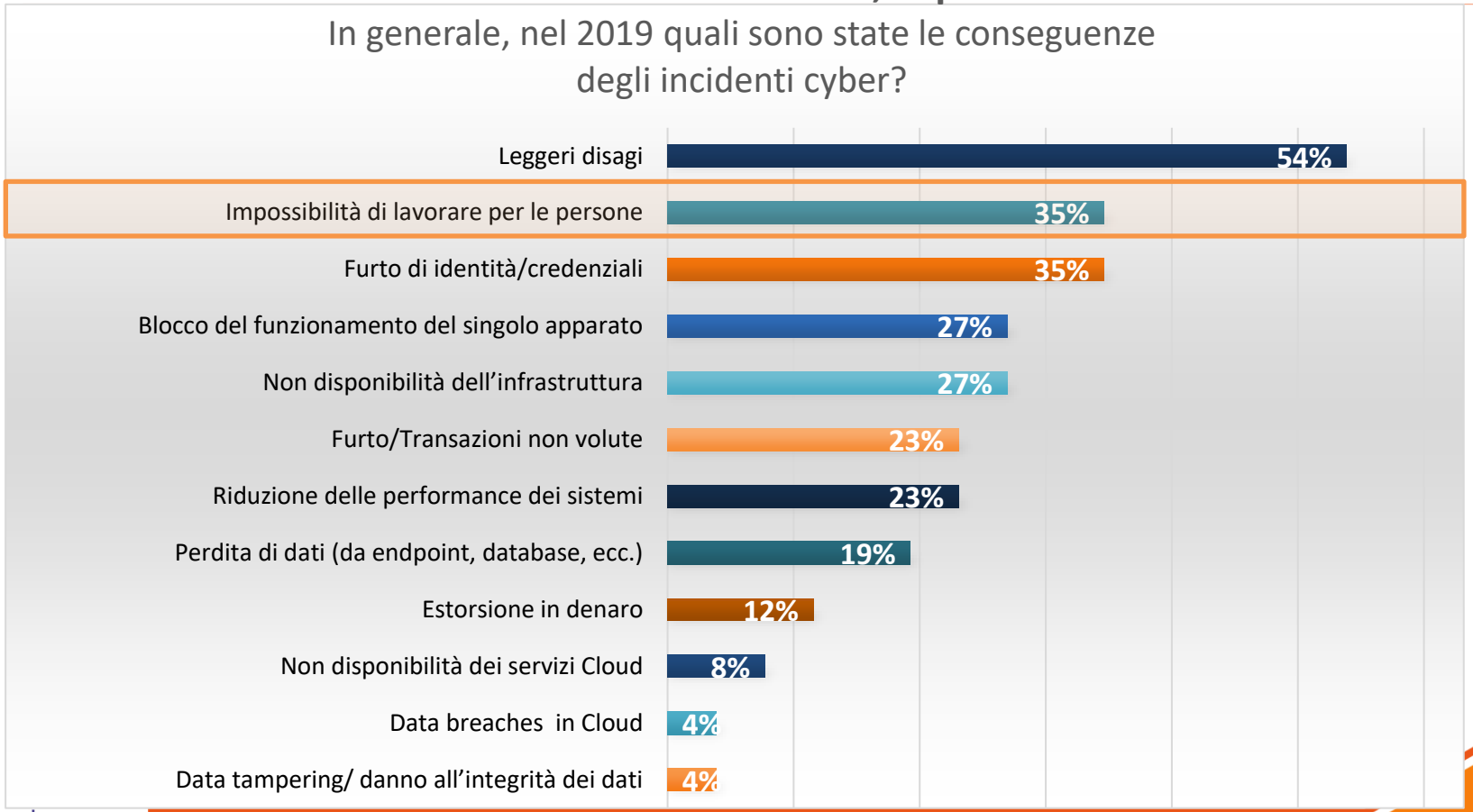
Se gli attacchi sono un problema generale, gli incidenti significativi sono in numero limitato. In 1 azienda su 2 non si osservano conseguenze negative

Quanti incidenti informatici subiti hanno avuto conseguenze in termini di data breach o indisponibilità/danni a sistemi e servizi ICT?



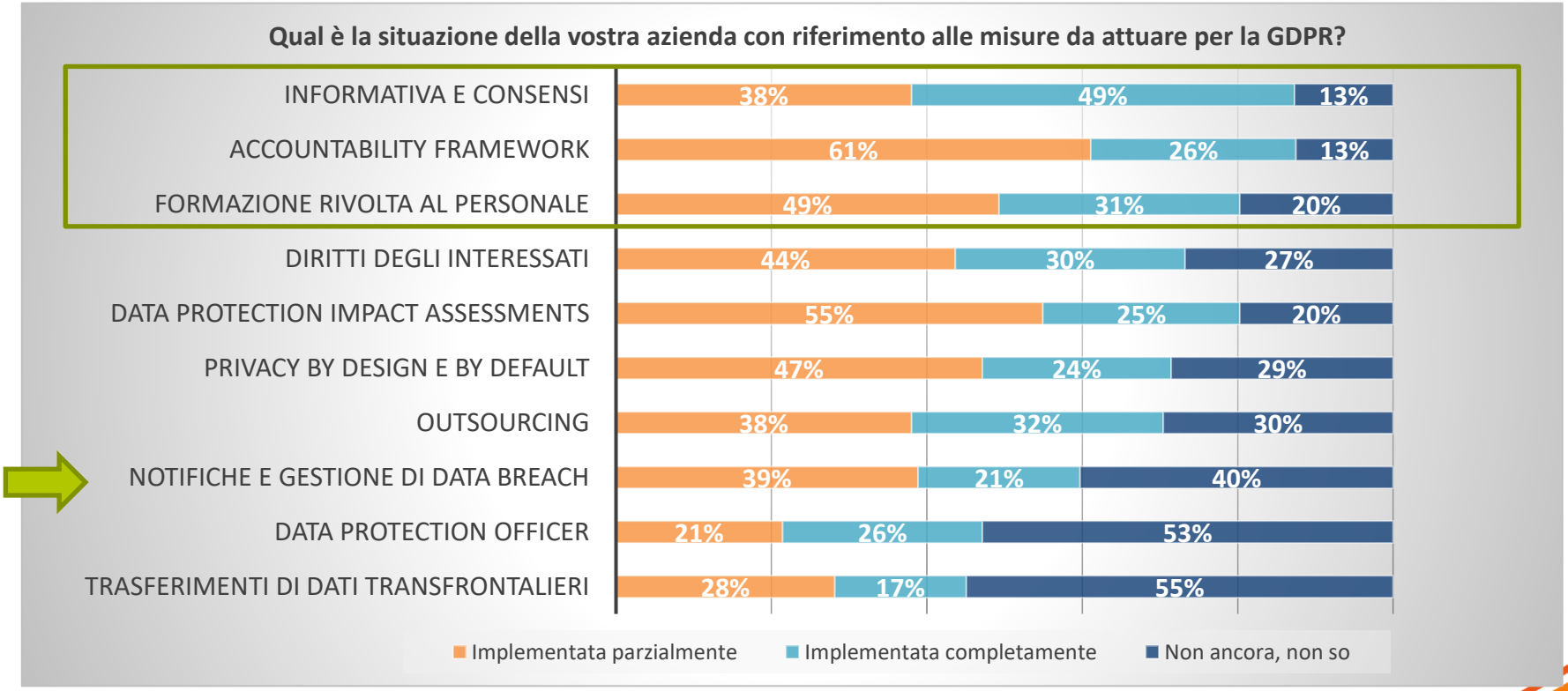
Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 63 aziende italiane

Parlando solo con chi ha avuto conseguenze da incidenti cyber, l'impatto è di nuovo molto variabile: nel 35% dei casi, le persone sono ferme



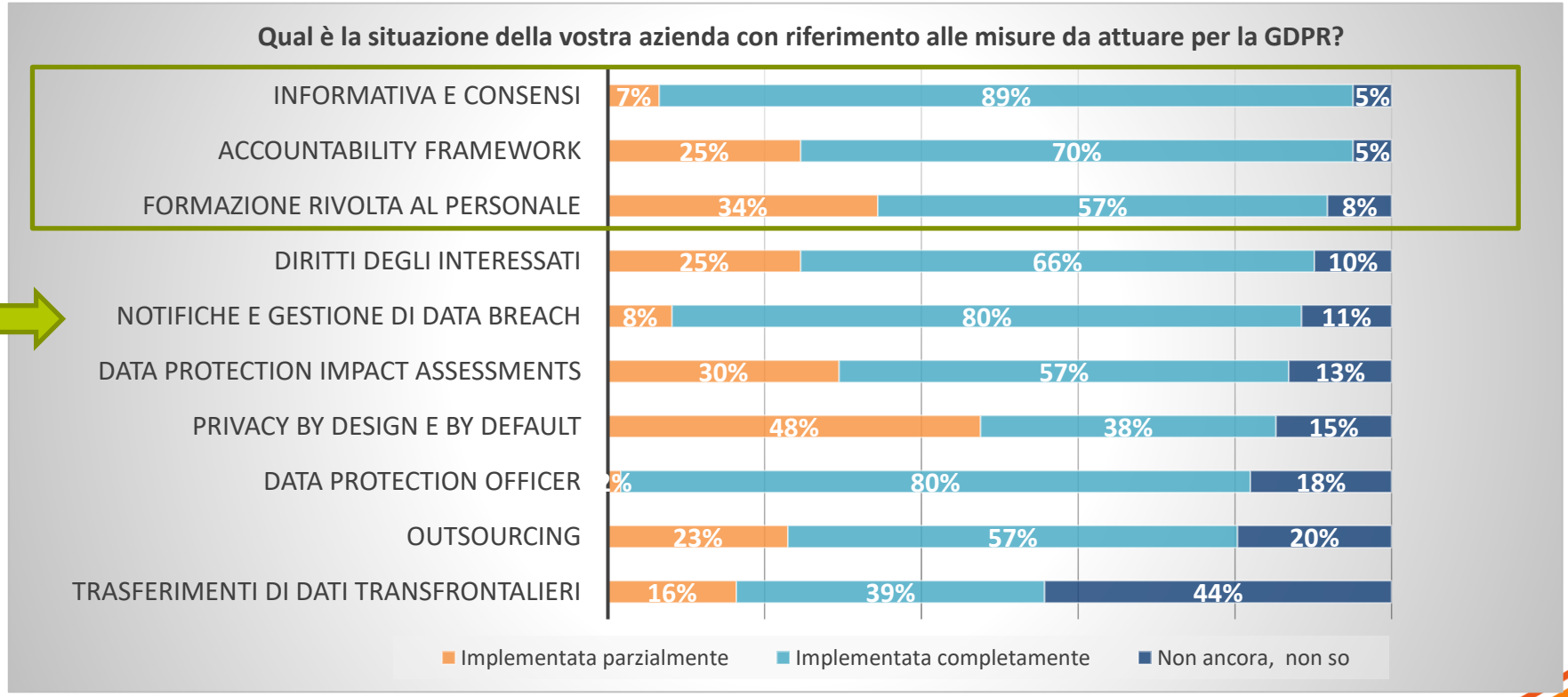
Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020.
Risponde solo chi ha subito incidenti con conseguenze. N = 26 aziende italiane

A gennaio 2018: molti lavori in corso



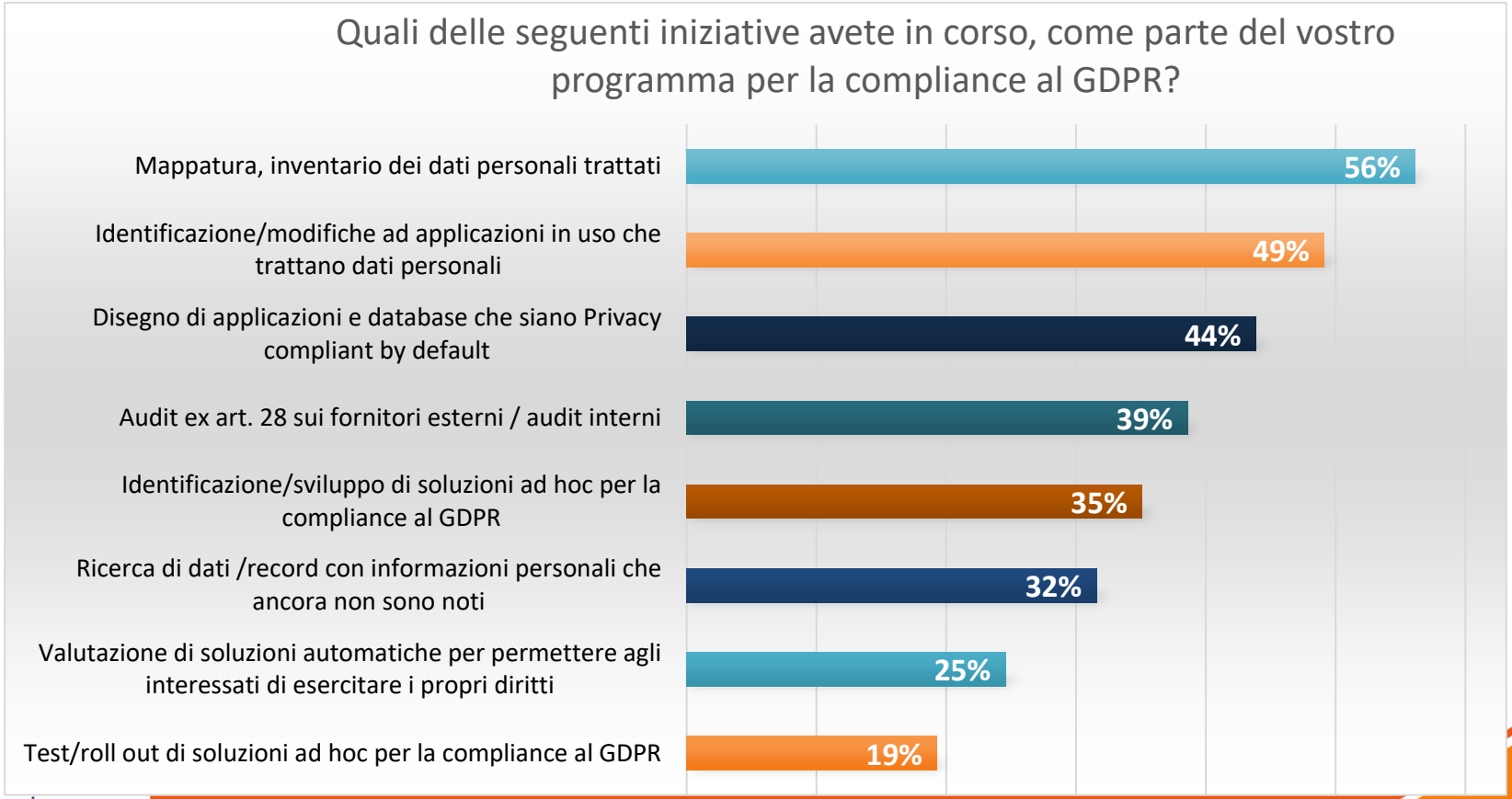
Fonte: The Innovation Group, Cyber Risk Management 2018 Survey, gennaio 2018. N = 88 aziende italiane

Dicembre 2019: netto miglioramento, ancora qualche attività



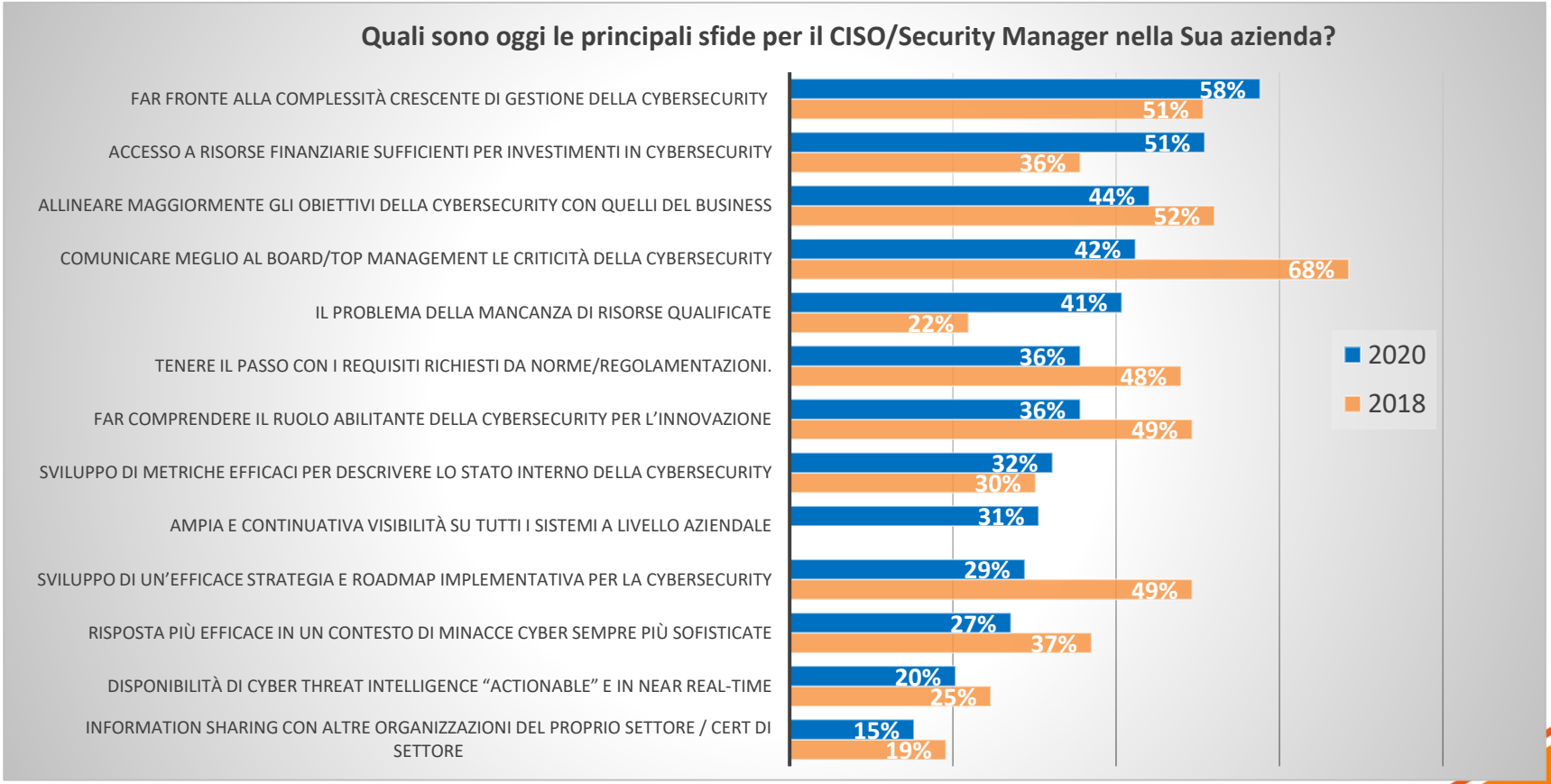
Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 61 aziende italiane

Il programma per la compliance vede tuttora numerose attività in corso



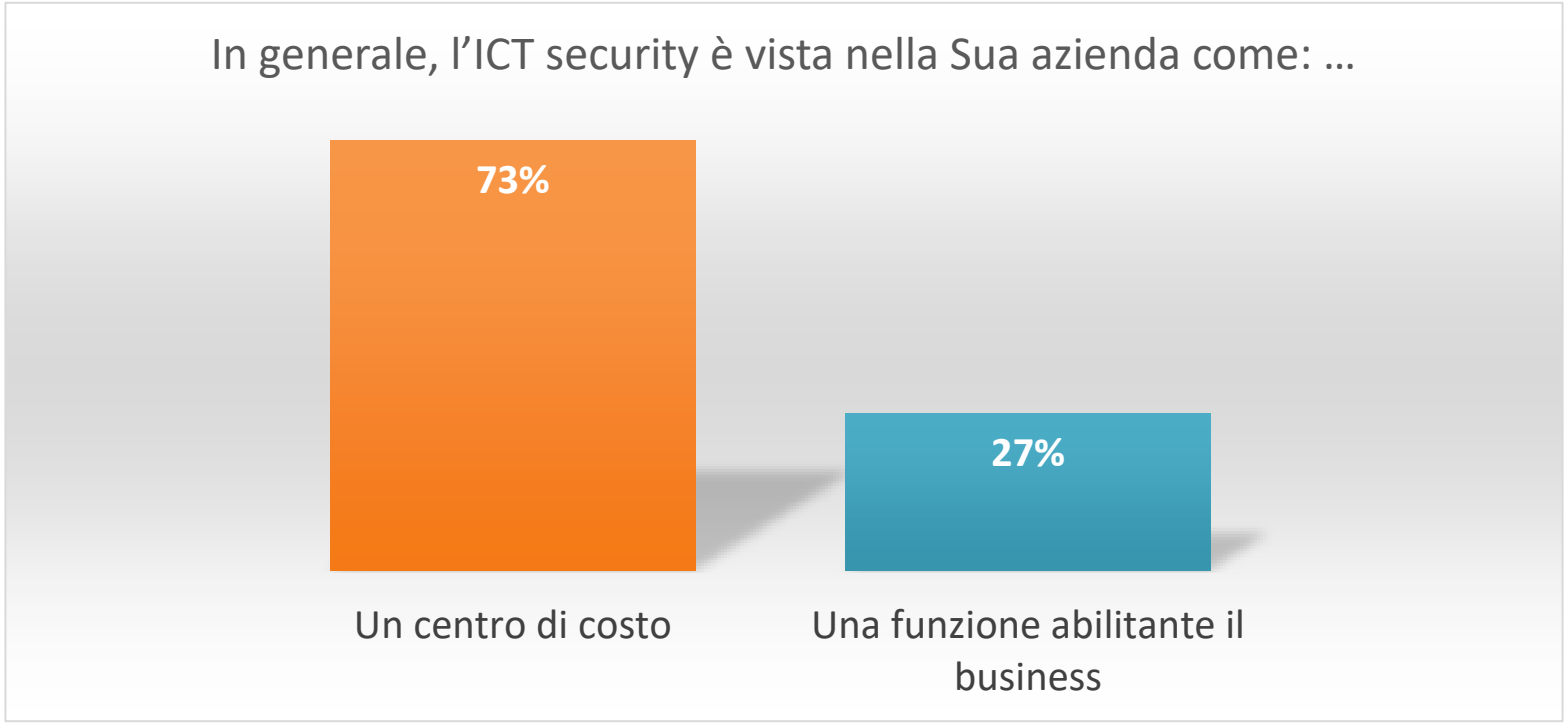
Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 57 aziende italiane

Tra i problemi maggiormente sentiti, la gestione della complessità e l'accesso a risorse finanziarie sufficienti



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 59 aziende italiane VS. CRM Survey 2018

Su un aspetto però c'è ancora molto lavoro da fare …



Fonte: The Innovation Group, Cyber Risk Management 2020 Survey, gennaio 2020. N = 56 aziende italiane