CAMERA DI COMMERCIO CANTONE TICINO
industria | artigianato | servizi

100 ANNI

Risultati inchiesta sulla sicurezza cibernetica

22 novembre 2017

In collaborazione con:

SUPSI

inthecyber
intelligence & defense advisors

Sicurezza cibernetica
L'inchiesta

Luca Albertoni, direttore Cc-Ti

L’inchiesta

Partecipanti:

- Istituti bancari
- Fiduciarie e finanza
- Multinazionali
- Enti connessi a infrastrutture sensibili
- Istituzioni pubbliche o parapubbliche

SUPSI

Cyber Security

Cambio marcia e penso come un hacker!

Dr. Ing. Alessandro Trivilini

100 ANNI

Il mercato degli attacchi informatici

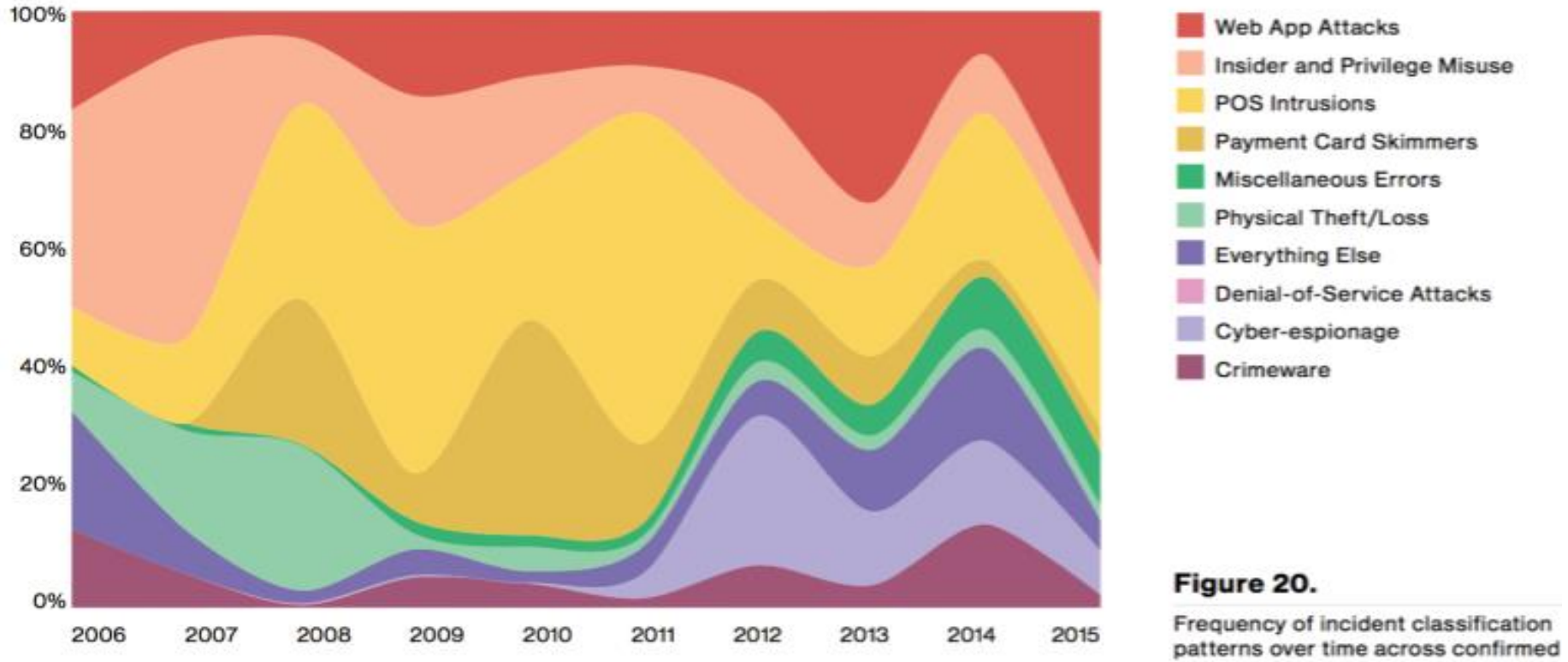


Figure 20.

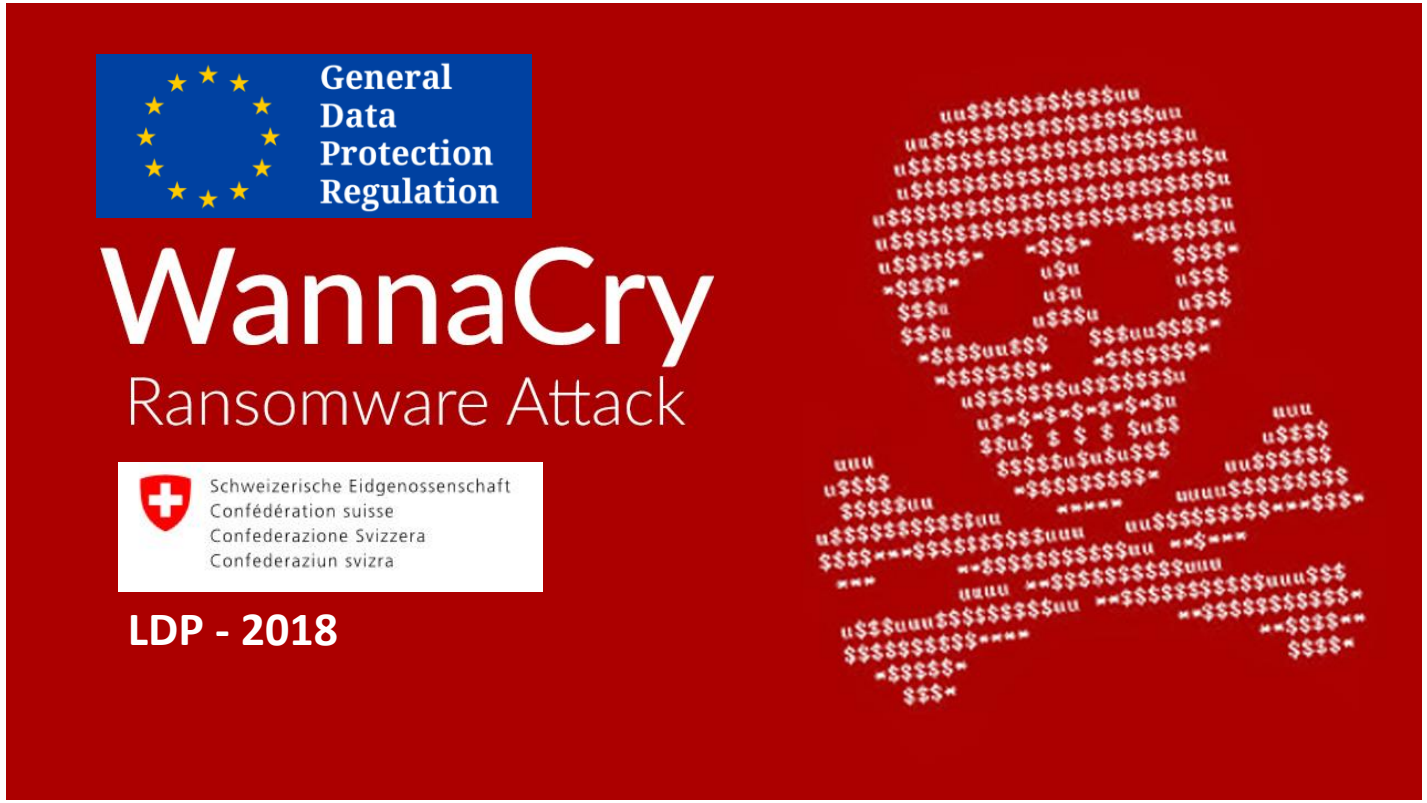
Frequency of incident classification patterns over time across confirmed data breaches.

Fonte: Jeremiah Grossman, BlackHat, Las Vegas, 2016

Il fattore umano è determinante

... ed è altamente prevedibile!

WannaCry – GDPR - LPD 2018



… e se dovessi dichiarare i dati ma questi fossero inaccessibili?

implementare misure tecniche e organizzative adeguate
per assicurare un livello di sicurezza appropriato al rischio

2018 in CH revisione totale della legge sulla protezione dei dati, verosimilmente simile al GDPR!

inthecyber
intelligence & defense advisors

CYBER SECURITY SURVEY

Paolo Lezzi, CEO e fondatore IntheCyber SA

100 ANNI

Classificazione degli elementi analizzati

GOVERNANCE

STRUTTURA

- Organizzazione e figure specifiche
- Standard e certificazioni
- Priorità aziendali

PROCESSI

- Tipologia di attività di Audit
- Cyber risk assessment
- Modalità gestione attacchi
- Capacità di reazione

TECNOLOGIE

DIFESA

- Grado protezione dalle minacce
- Security by design

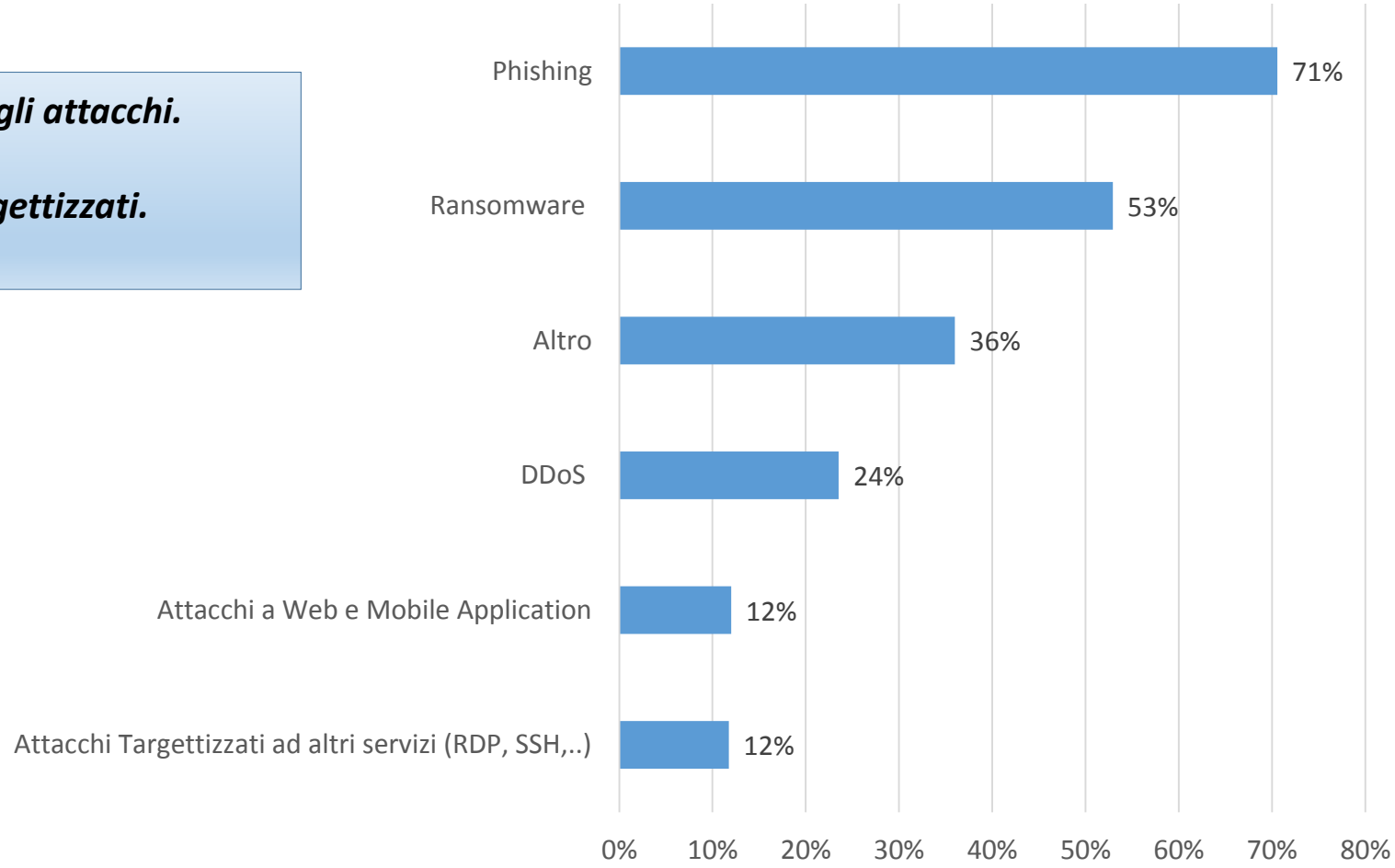
DETECTION

- Livello di identificazione minacce
- Capacità rilevazione attacchi
- Capacità di Threat Intelligence

Tentativi di attacco degli ultimi 24 mesi

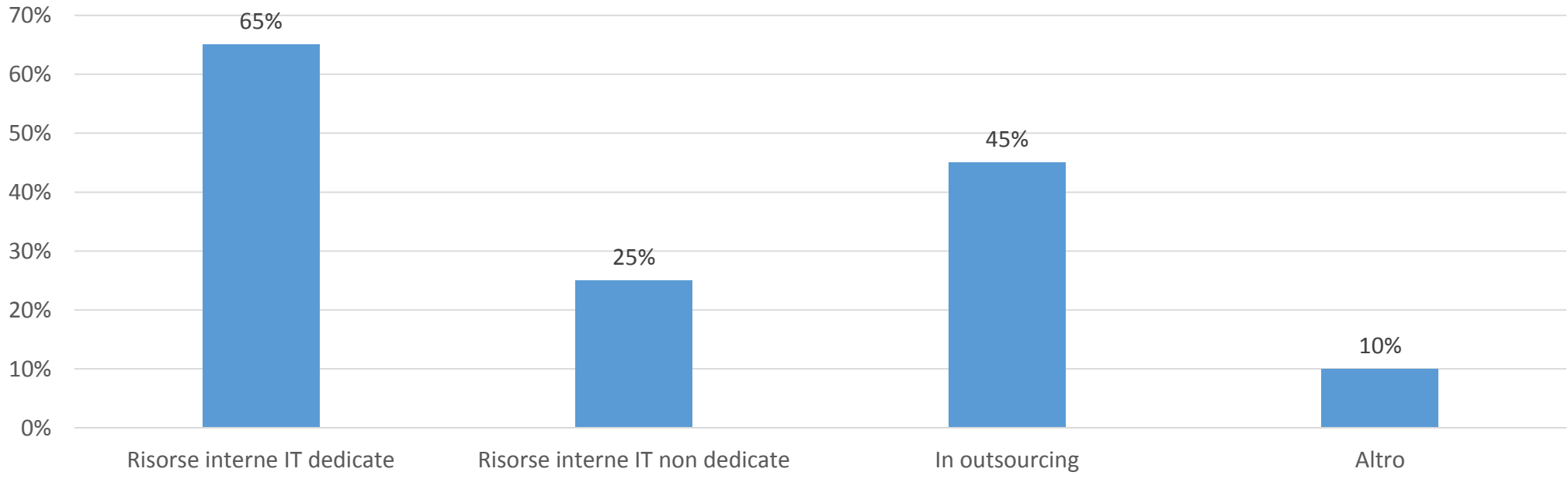
Ransomware & Spear Phishing in testa agli attacchi.

In particolare aumento gli attacchi targettizzati.



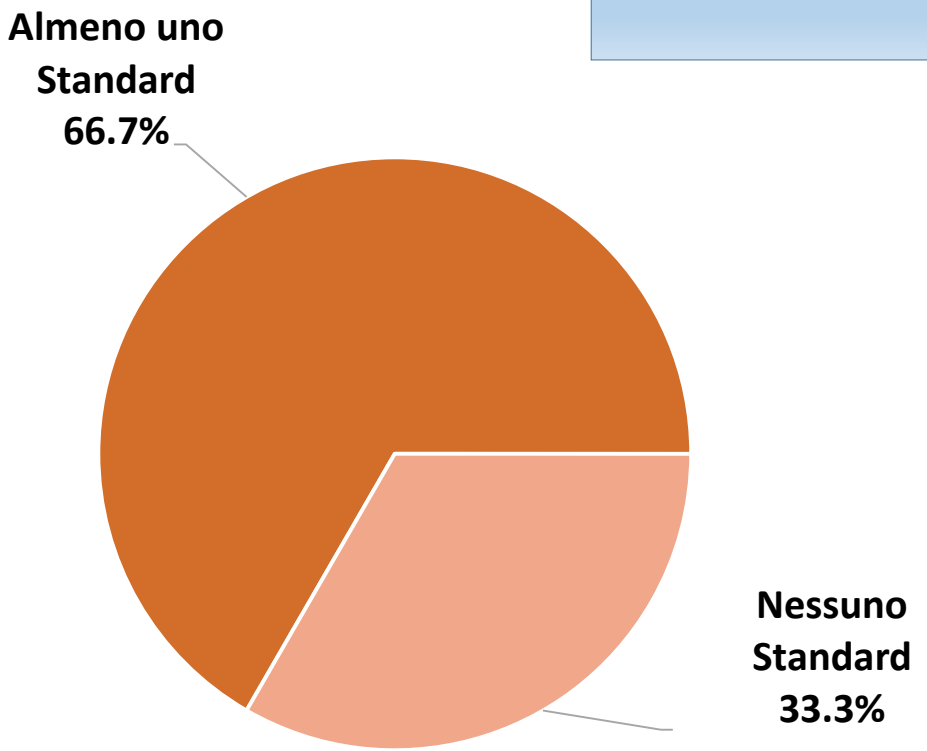
Organizzazione interna per la gestione della Cyber Security

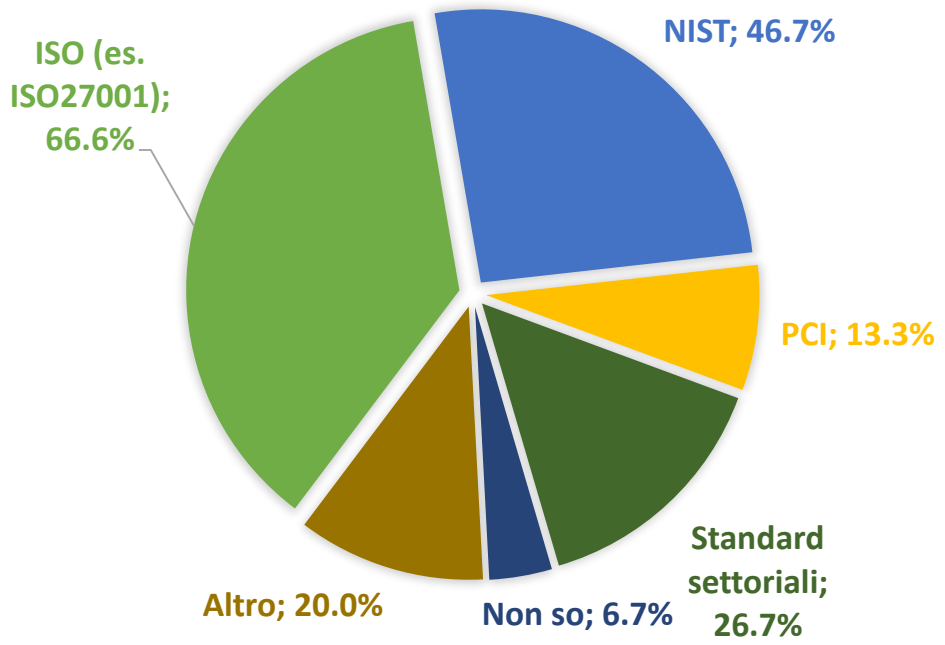
Un quarto delle Aziende intervistate non ha risorse dedicate



Standard e modelli di riferimento

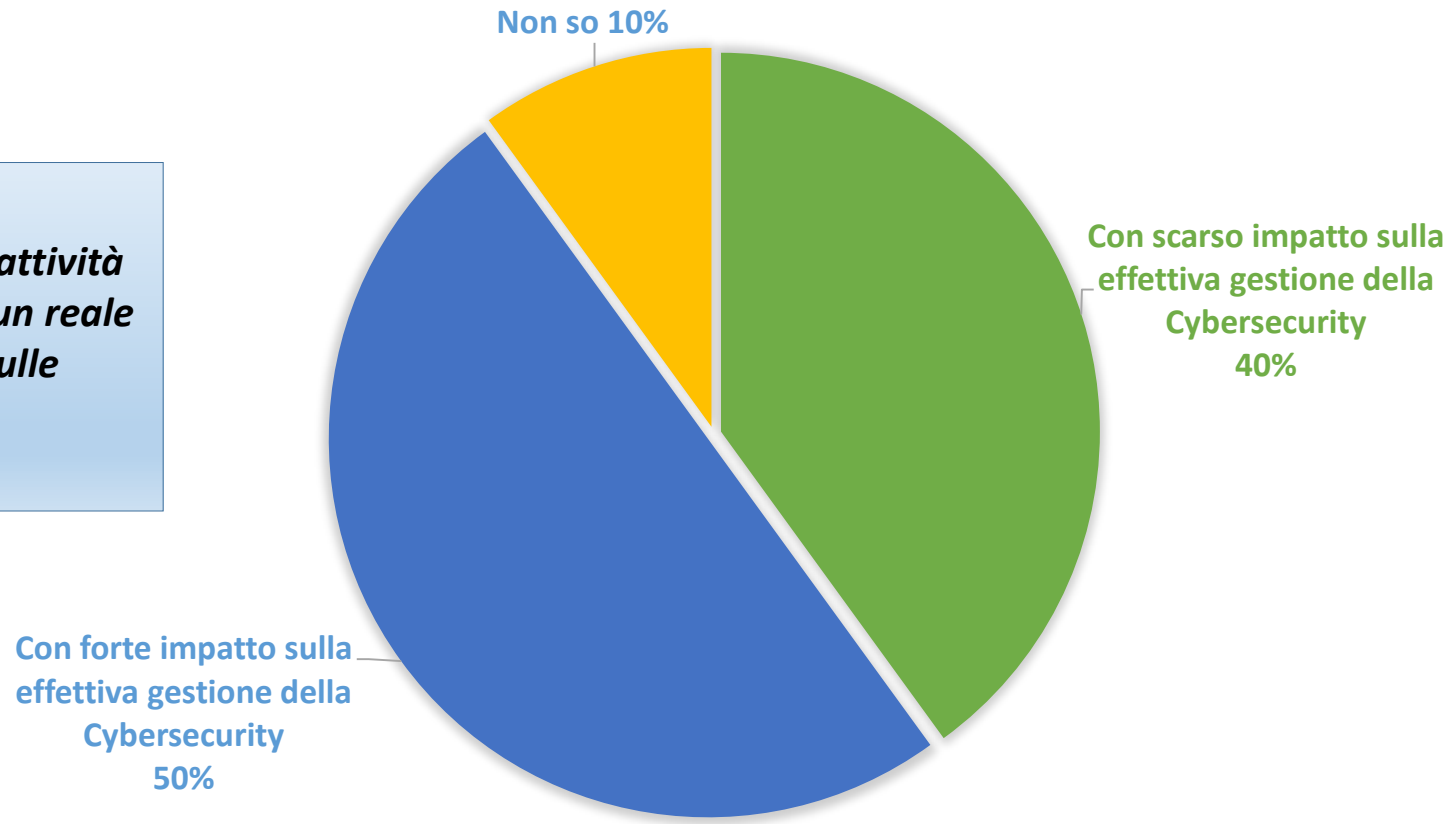
Un terzo degli intervistati non utilizza alcuno Standard di Cybersecurity Governance





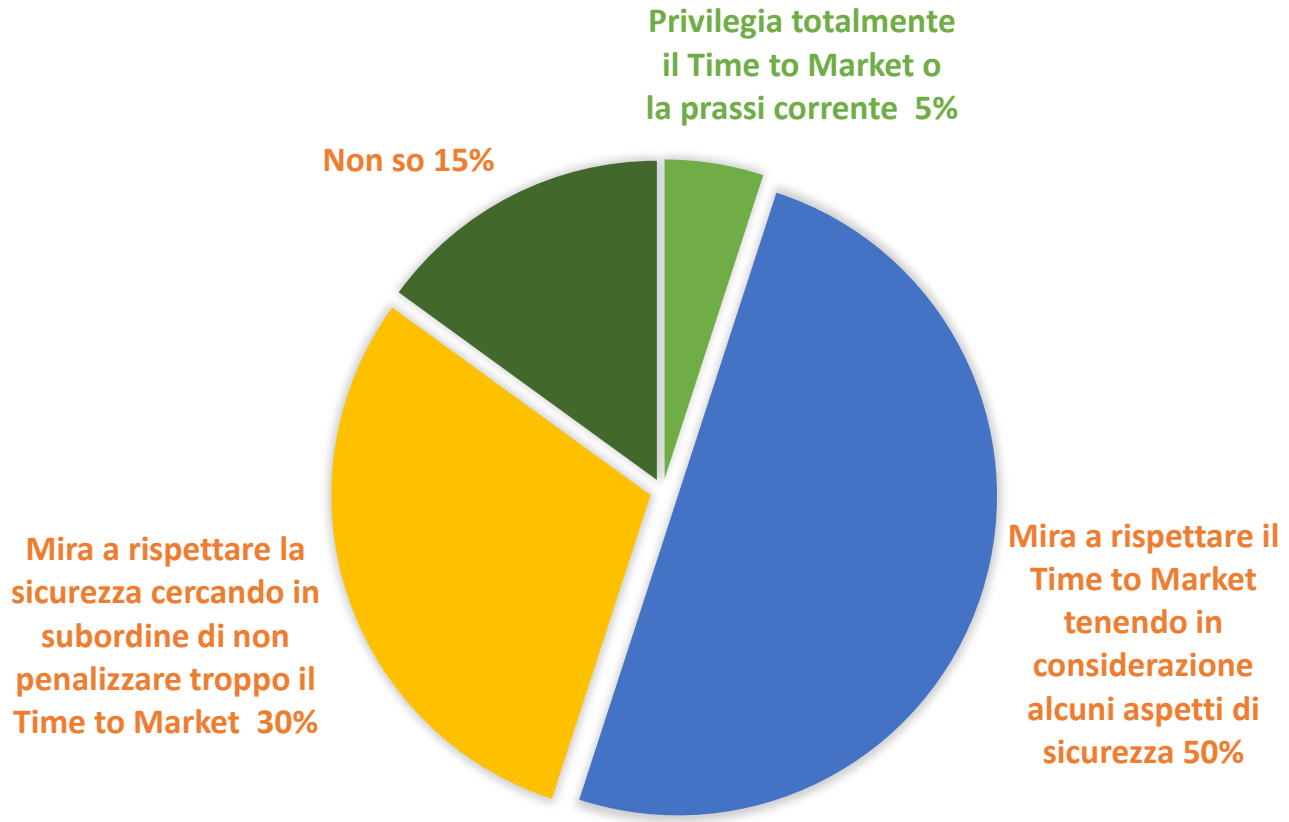
Caratteristiche delle attività di Audit, Risk e Compliance

Solo per la metà delle Aziende le attività di Audit,Risk&Compliance hanno un reale effetto sull'organizzazione e sulle tecnologie adottate



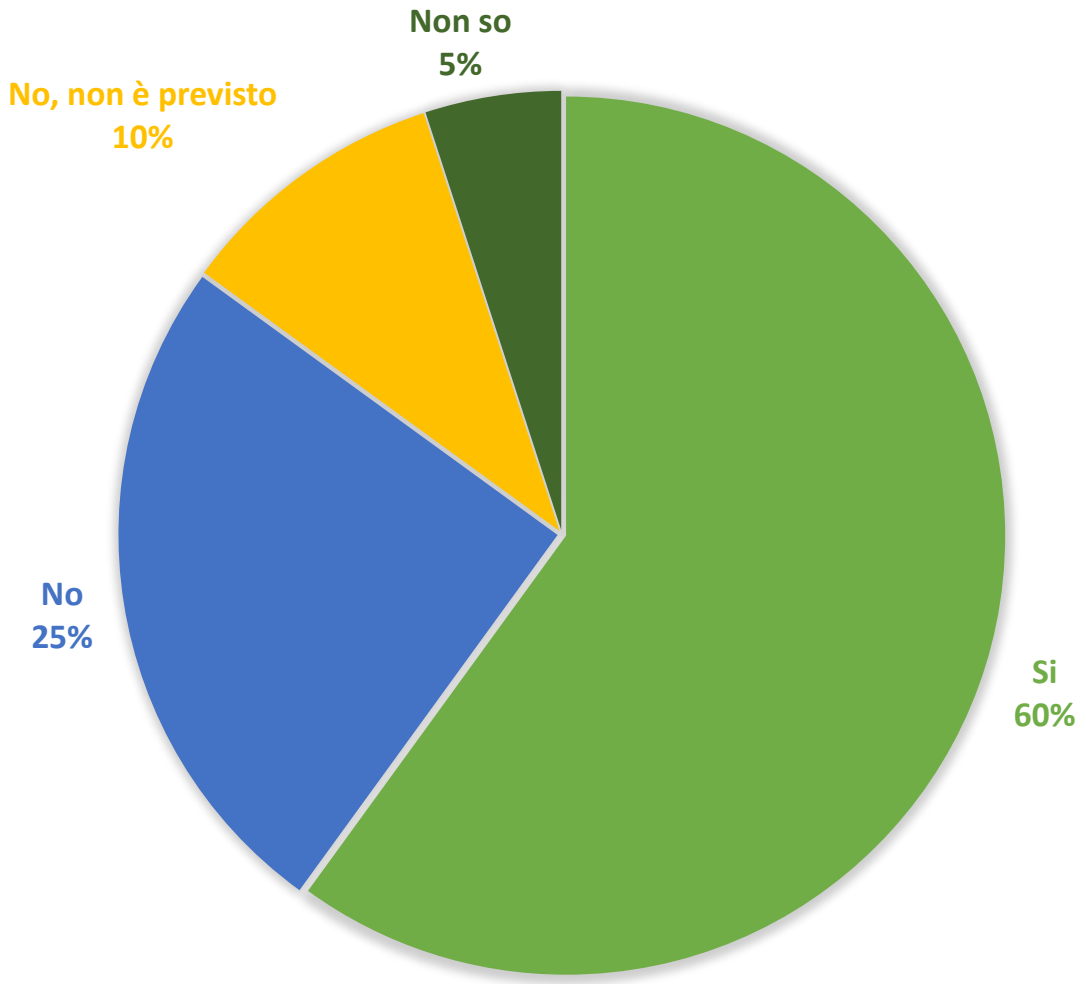
Time to Market VS Cybersecurity

Più della metà delle Aziende intervistate tiene in secondo piano il tema della Cybersecurity e privilegia il Time to Market



Cybersecurity Risk Assessment

Solo il 60% delle Aziende intervistate lo ha eseguito in modo strutturato

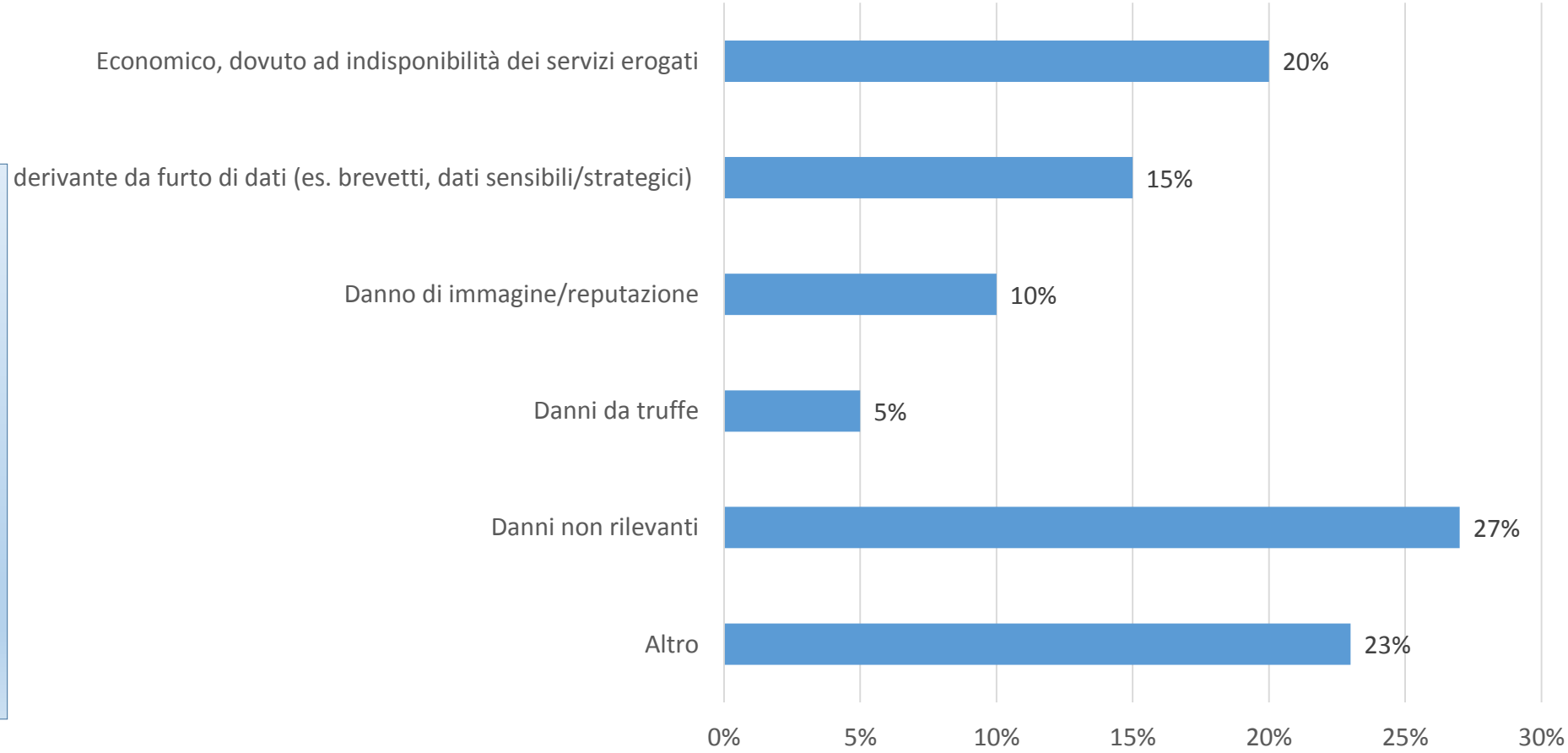


Tipologie di danno subito

Nel 20% dei casi le Aziende hanno subito un danno economico diretto.

L'aumento degli attacchi targettizzati coincide con danni relativi a dati sensibili e di proprietà intelletuale.

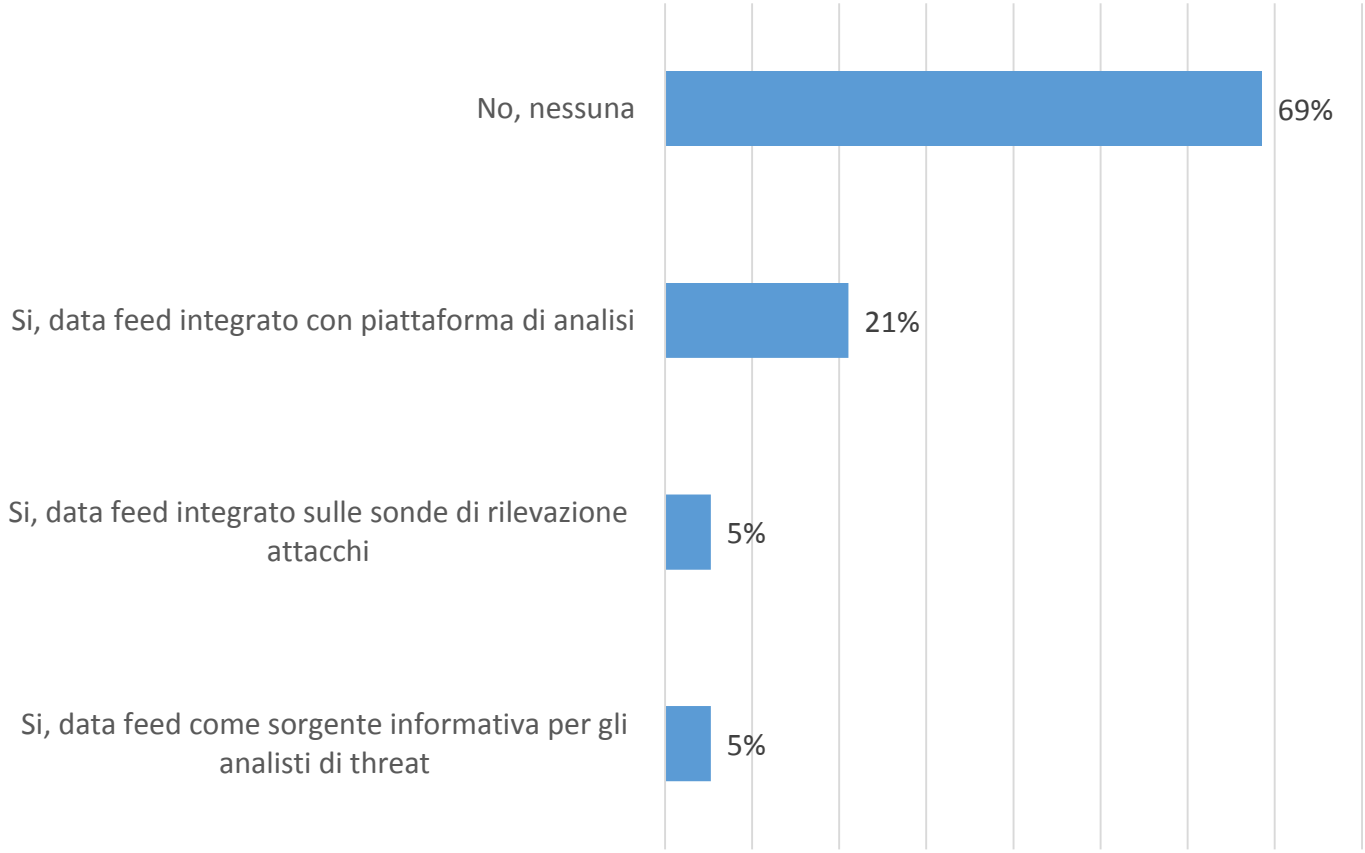
L'ulteriore danno è reputazionale.



Capacità di Threat Intelligence

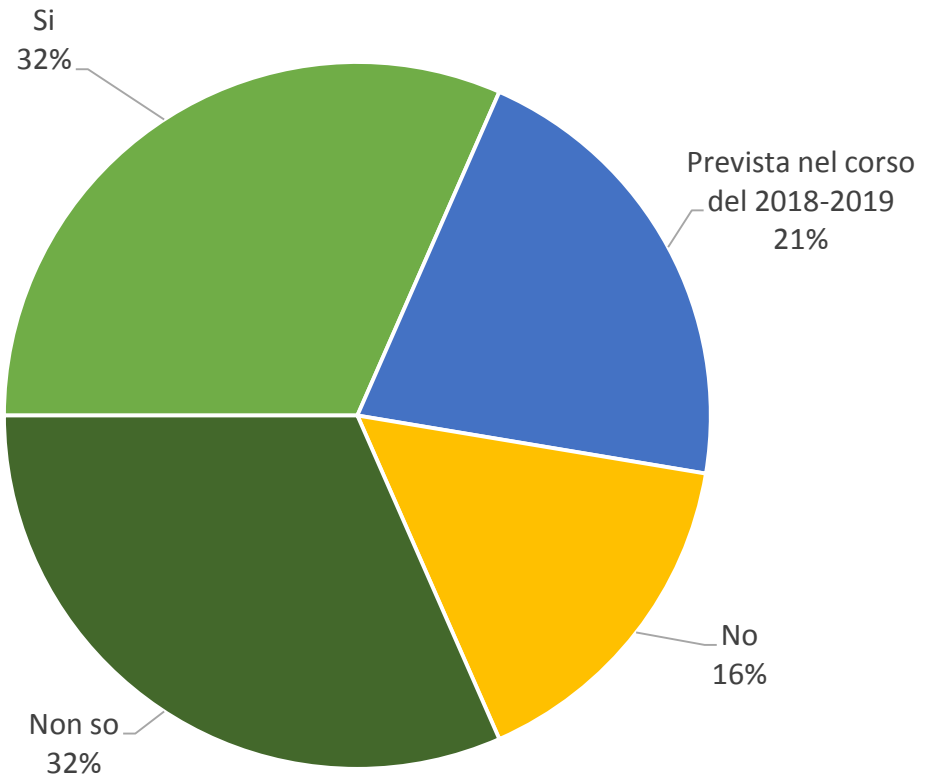
Il 69% delle Aziende intervistate non dispone di capacità di Threat Intelligence

Solo il 5% ha capacità che riteniamo essenziali



Security by Design

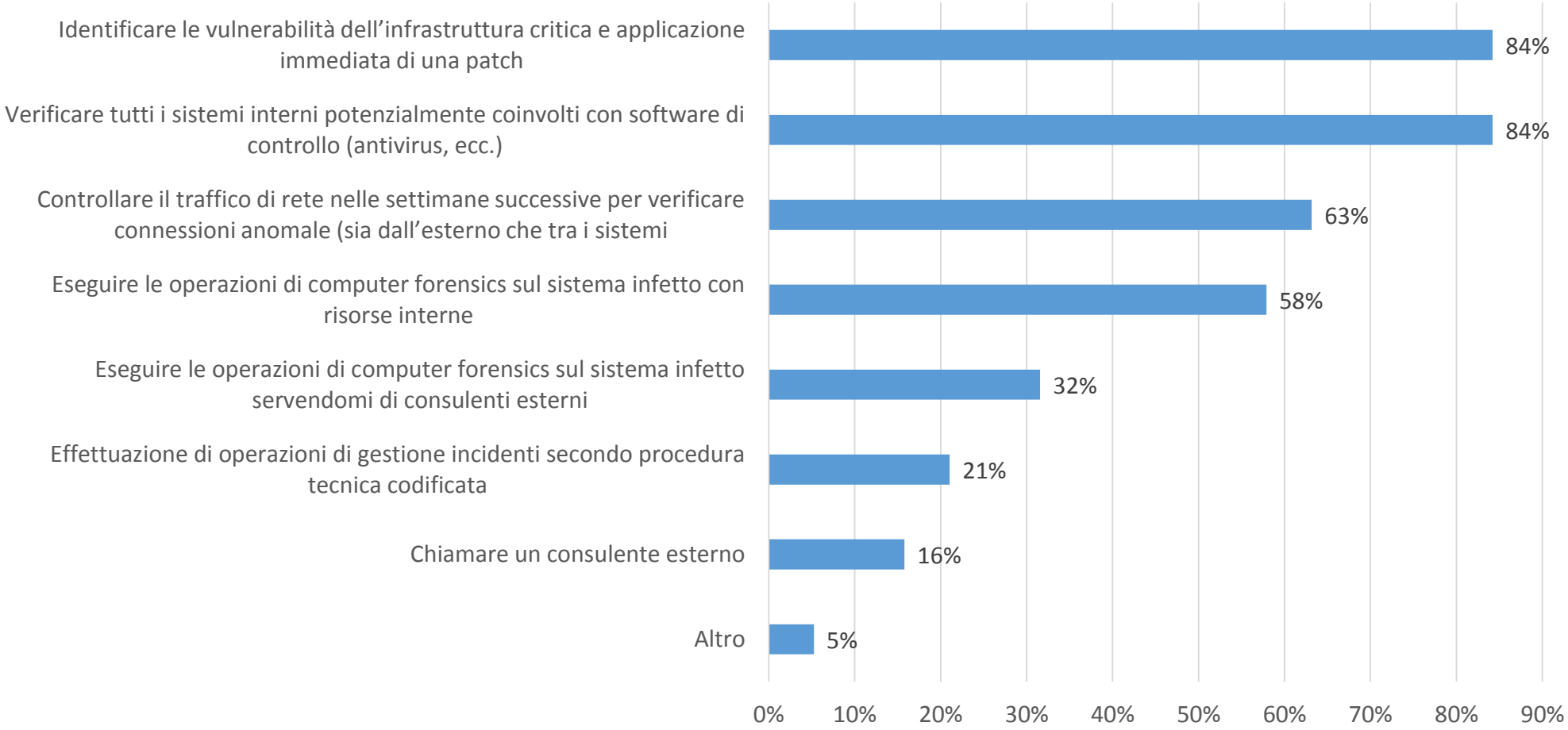
Solo il 53% delle Aziende intervistate pone attenzione al tema del Security by Design che sarà imposto dalle normative Svizzere ed Europee (nuova LPD e GDPR)



Gestione degli incidenti di Cybersecurity

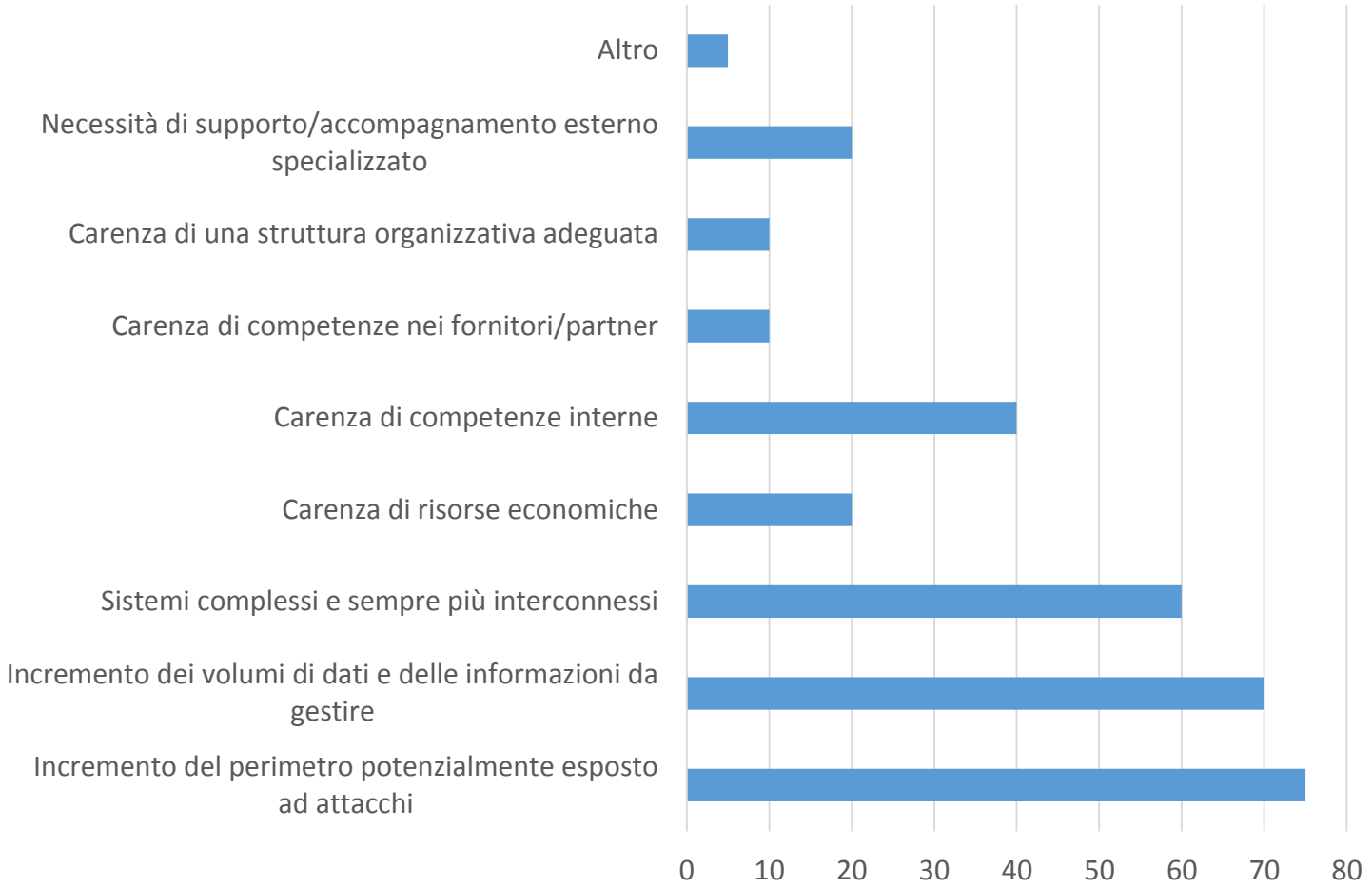
Solo il 21% delle Aziende intervistate segue uno standard codificato

Il 63% delle Aziende intervistate dichiara però di essere preparata a gestire adeguatamente un incidente di CyberSecurity con un Team dedicato



Le evoluzioni a maggior impatto sulla Cybersecurity

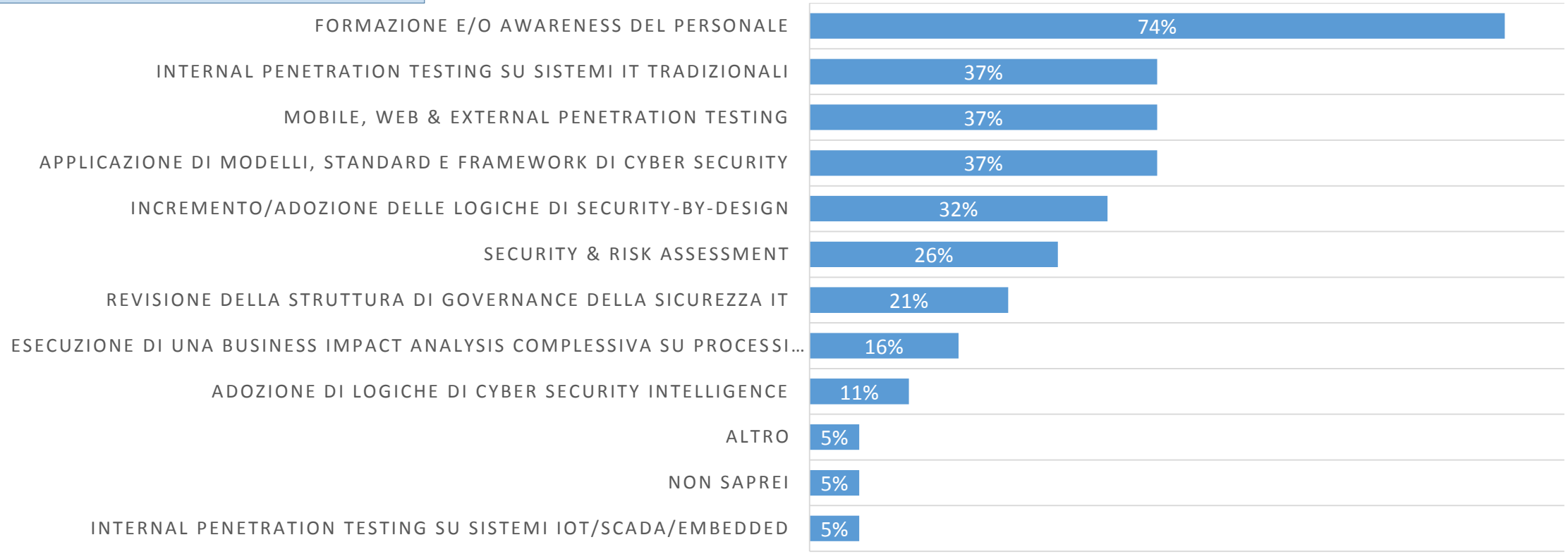
Incremento di perimetro, volume di dati e complessità dei sistemi in testa



Priorità degli investimenti di Cybersecurity

Campagne di Awareness, Penetration Testing e applicazione di Standard in testa.

Gestione del rischio e della Governace sottovalutate

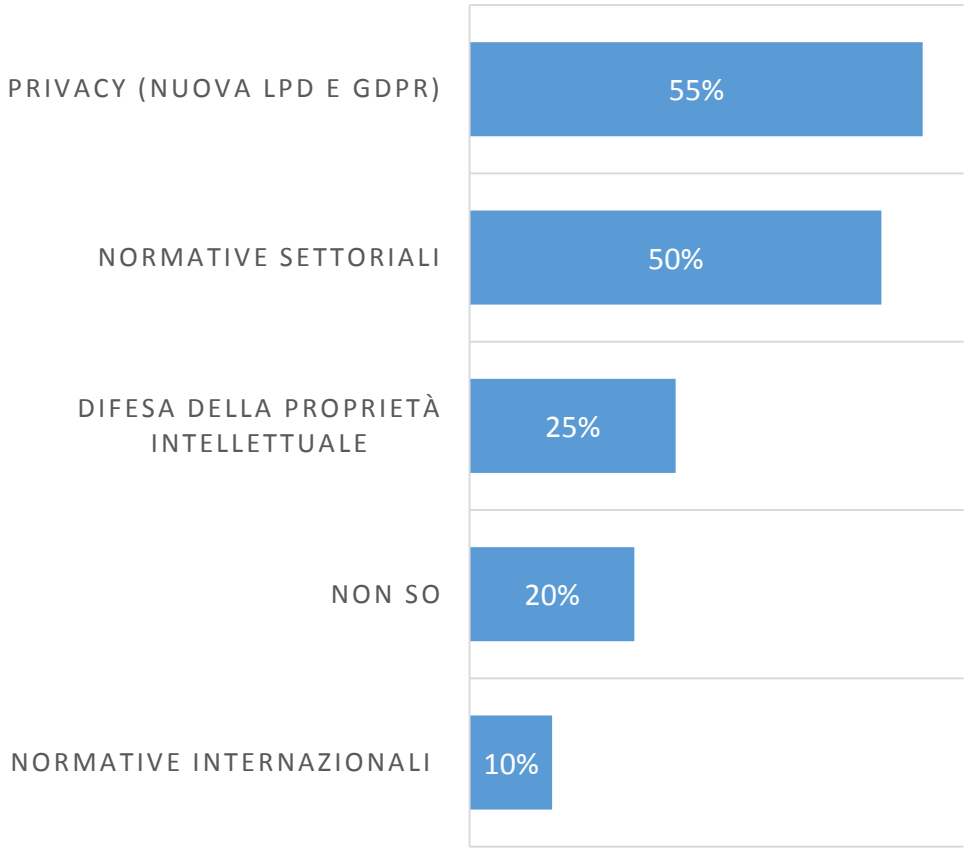


Normative e investimenti

TLP: GREEN

Privacy e normative settoriali guidano gli investimenti nell'ambito della Cyber Security.

Solo il 25% considera il tema della difesa della proprietà intellettuale.



Principali evidenze

TLP: GREEN

Il rischio cyber non viene rilevato e mappato nella sua interezza.
Le attività di protezione non sono tarate proporzionalmente al rischio, nonostante questo sia requisito di molti dei più recenti standard (ad es. ISO e NIST), normative e regolamenti (ad es. LPD e GDPR)

Gli investimenti si concentrano sulle tecnologie ma risulta necessario investire nel miglioramento di organizzazione e processi

Il fattore umano e la vulnerabilità al social engineering sono due aspetti non considerati con l'attenzione che meritano

La capacità di contrastare il cyber crime richiede necessariamente la presenza di analisti in grado di gestire adeguatamente allarmi ed eventi

Principali azioni suggerite

TLP: GREEN

Test del reale livello di protezione da minacce avanzate tramite Red Team Exercise

Gap Analysis rispetto alle best practices internazionali di cybersecurity e di risk management

Empowerment delle strutture di difesa con particolare attenzione alla organizzazione e alle configurazioni tecnologiche

Grazie per l'attenzione !

SUPSI

inthecyber
intelligence & defense advisors