

# ***CYBER RISK MANAGEMENT SURVEY 2018***

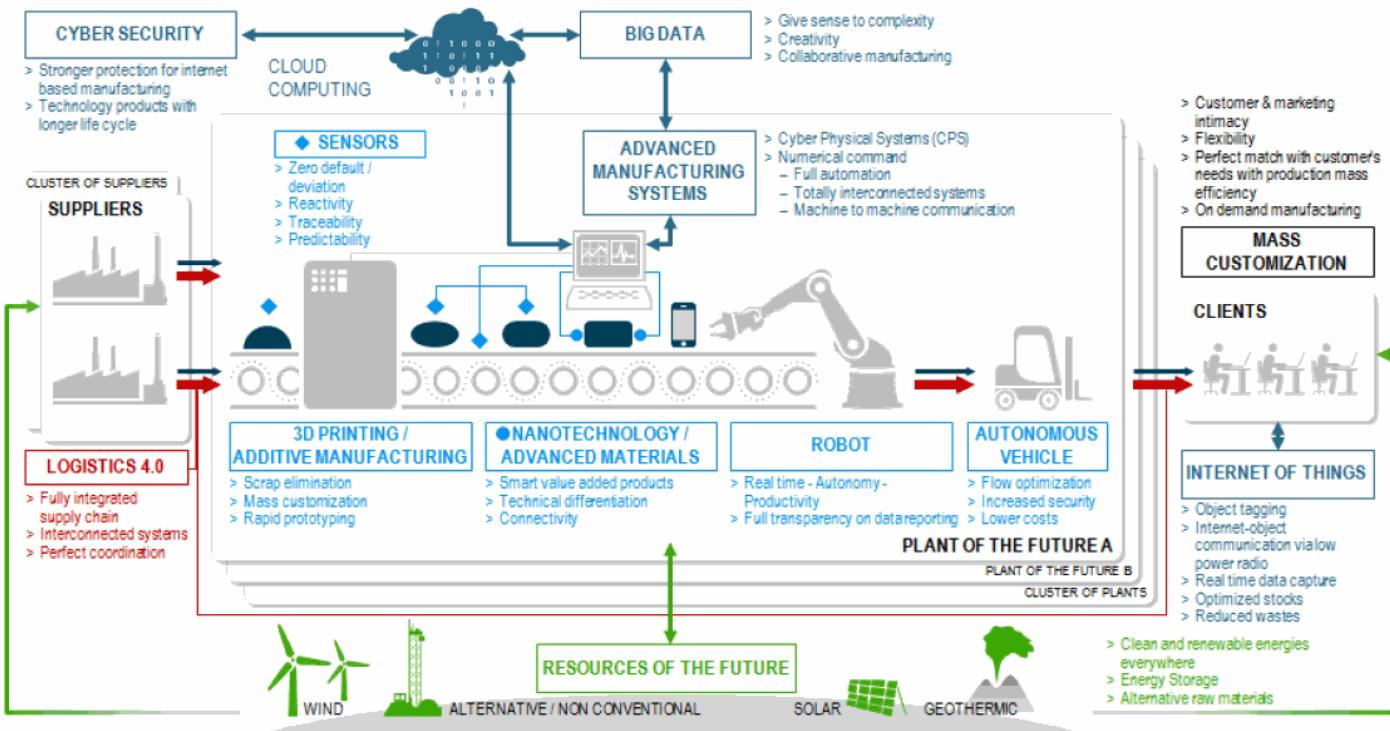
**CYBERSECURITY SUMMIT**  
Milano 30 -31 Maggio 2018



**The Innovation Group**  
Innovating business and organizations through ICT



# Quale scenario di rischi per l'Industria 4.0?



# Sezioni della Survey

1. *Attacchi Cyber: quale esperienza?*
2. *Programma sviluppato per la Cybersecurity e sua efficacia*
3. *Come cambia la funzione di ICT Security e il ruolo del CISO*
4. *Misurazione e Reporting al CEO/Board*
5. *Data Protection e adeguamento al GDPR*
6. *Misure e processi per la Supply Chain Security*
7. *Cyber Insurance: adozione e motivazioni*

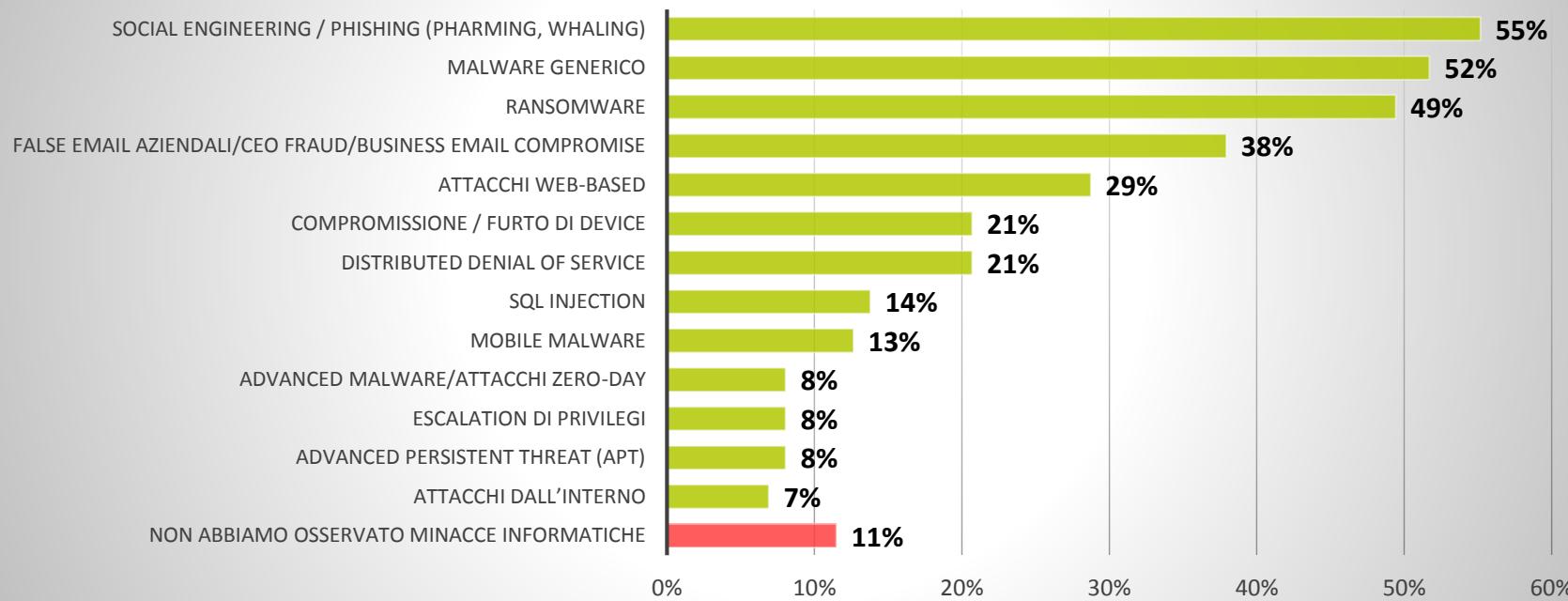
# Sintesi e Conclusioni

- ✓ **Le strategie di Cybersecurity non sono ancora** : vulnerabilità, sofisticazioni, crescita e dinamiche degli attacchi stanno ponendo sfide significative alle aziende italiane
- ✓ **I modelli organizzativi e i processi per la gestione e governance della Cybersecurity sono ancora «silos based»** : sono necessari più integrazione e coordinamento e una migliore comunicazione con il Top Management basata su performance indicator quali-quantitativi
- ✓ **Compliance è uno dei principali driver di investimento** : le aziende devono ripensare la cybersecurity come parte dell'approccio al Risk Management
- ✓ **Cyber threat intelligence, monitoring della supply chain dei vendor può facilitare la previsione** delle minacce e i rischi associati e valutare le priorità di investimento

*Come il Cyber Risk Management deve evolvere nelle organizzazioni Medio-Grandi ?*

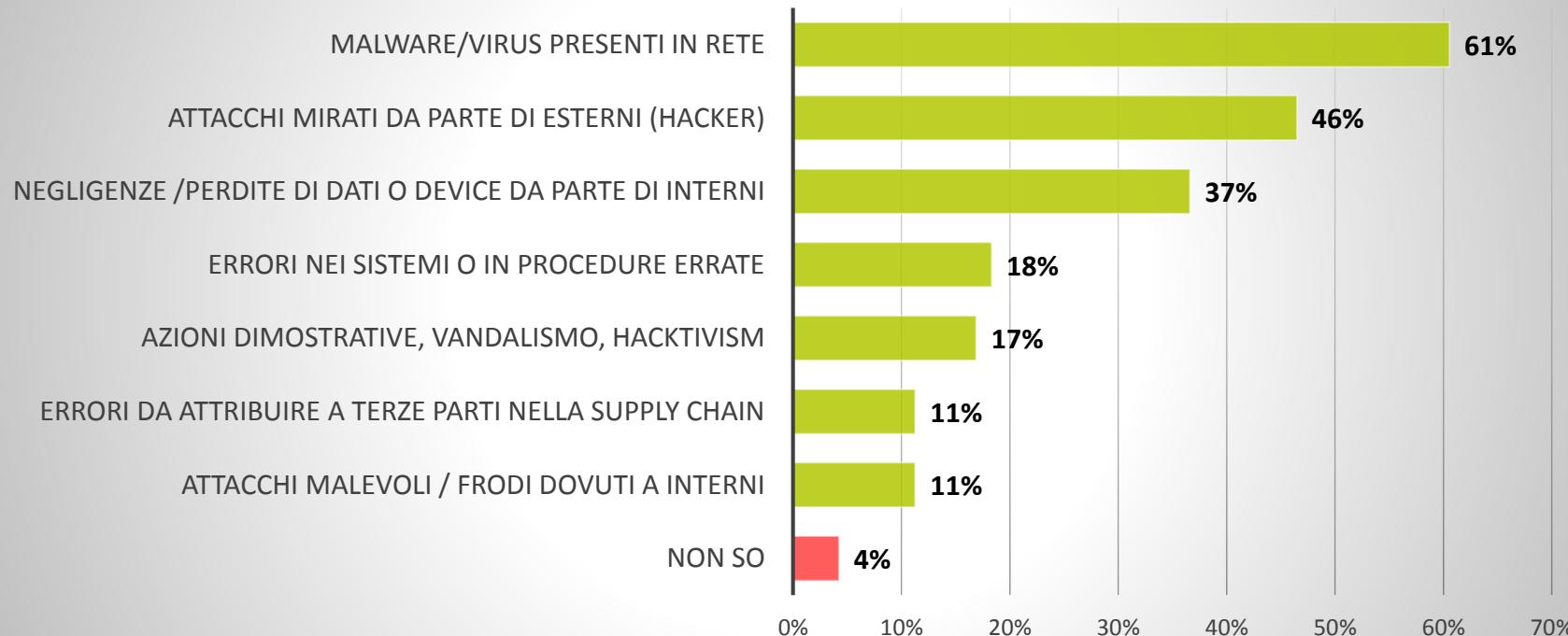
# Phishing al primo posto tra le minacce cyber 2017

Nel corso degli ultimi 12 mesi, quali delle seguenti minacce informatiche hanno riguardato la vostra azienda?



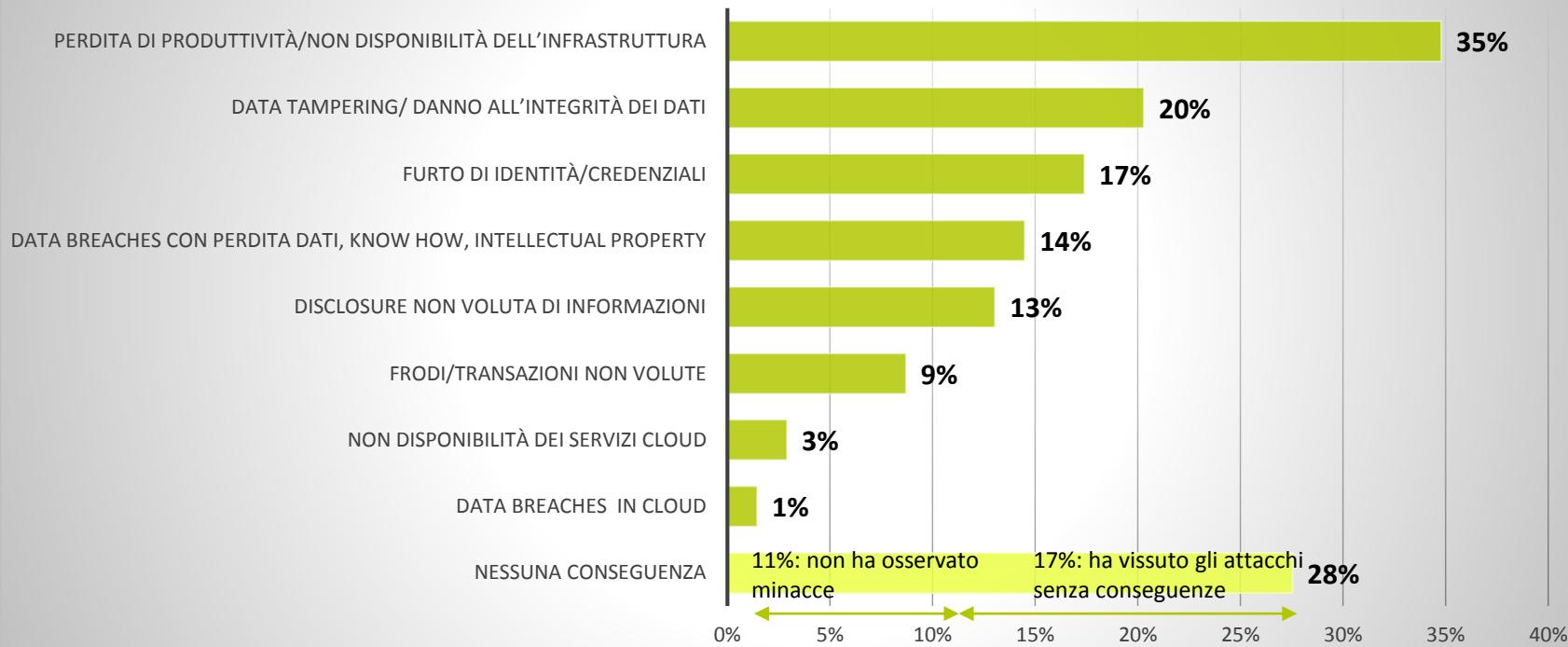
# Attribuzione dell'attacco: per il 46% dei casi, sono attacchi mirati

Quali sono state le cause all'origine degli incidenti osservati/subiti?



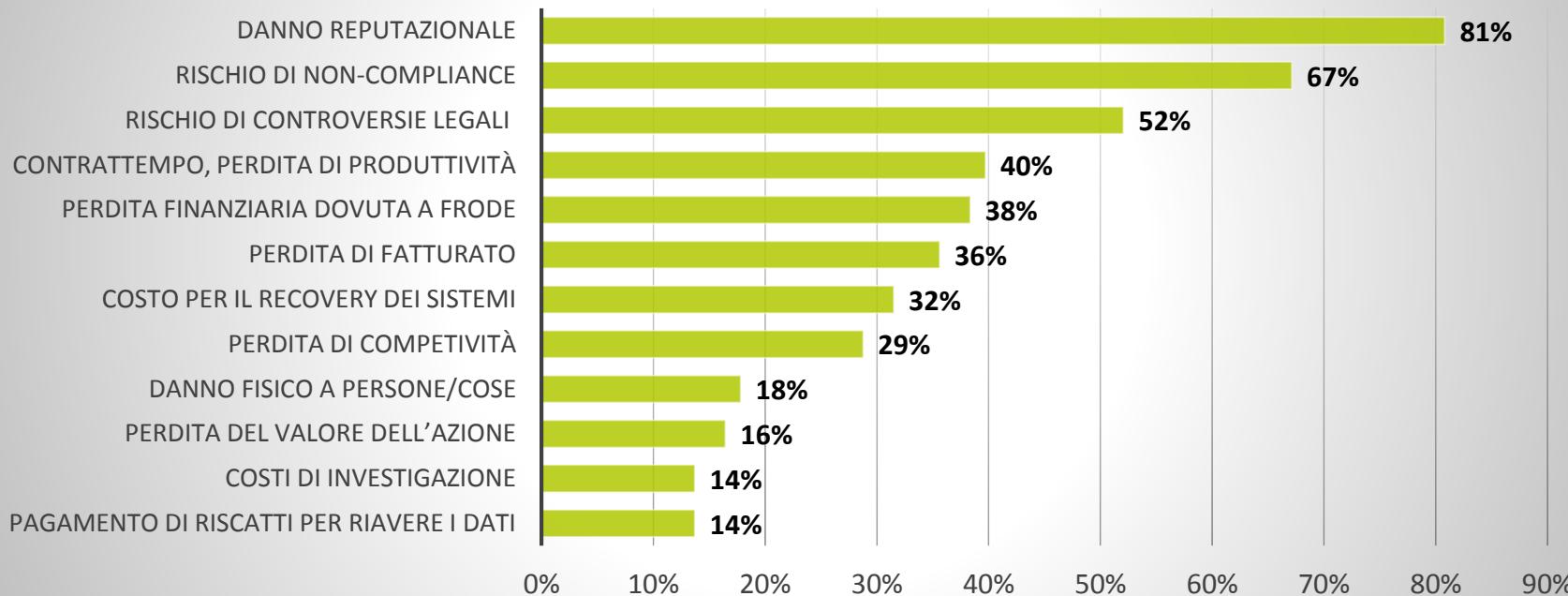
# Solo il 17% riesce a fermare gli attacchi senza subirne le conseguenze

## Quali sono state le conseguenze degli attacchi subiti?



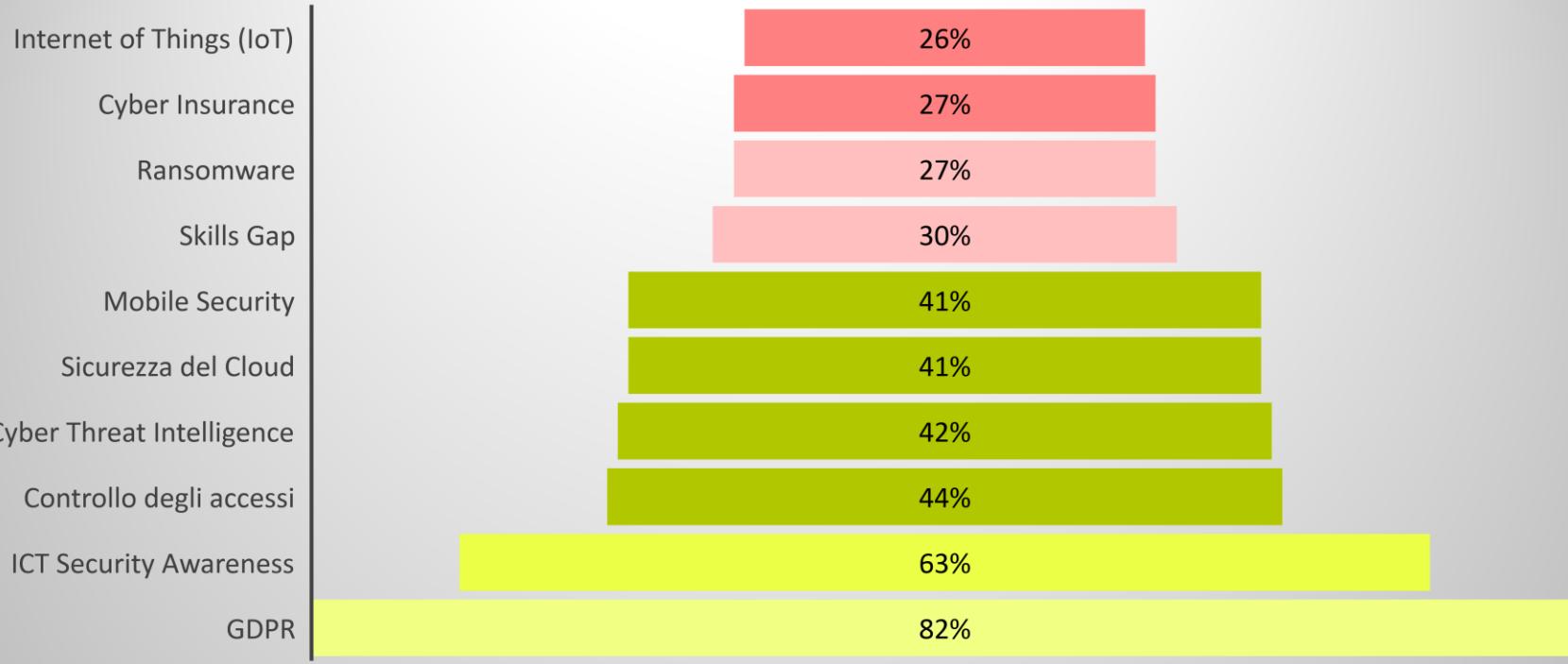
# Motivazioni per la Cybersecurity: danno reputazionale e compliance

Quali sono i principali impatti negativi che spingono l'azienda a prendere provvedimenti in ambito ICT Security?



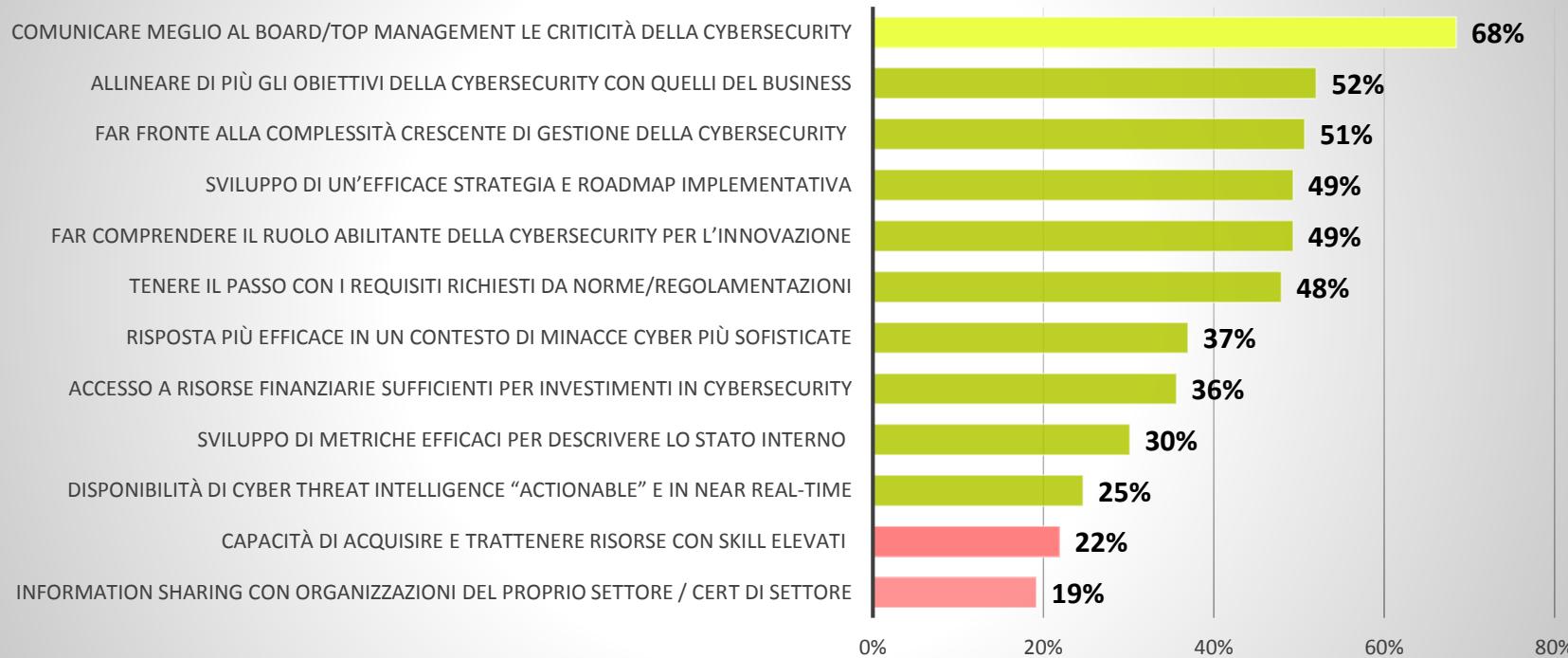
# Le priorità del CISO per il 2018: GDPR, Awareness, Controllo Accessi, Intelligence, Cloud e Mobile Security

Quali dei seguenti Hot Topic sono oggi più rilevanti secondo lei per un CISO/Security Manager?



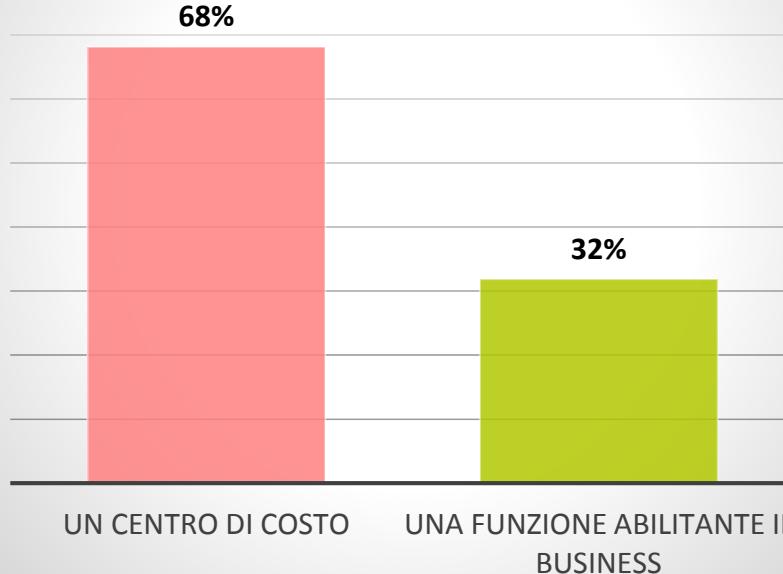
# Le prime criticità risiedono nella relazione della Security con il resto dell'azienda

Quali sono oggi le principali sfide per il CISO/Security Manager nella sua organizzazione?



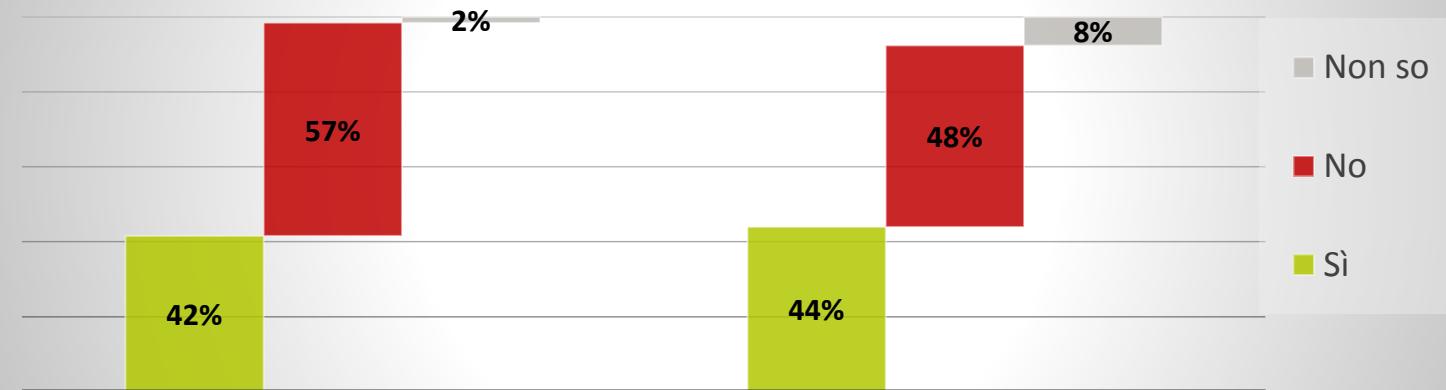
# La sicurezza è ancora percepita più come un costo che come un investimento per il business

In generale, l'ICT security è vista nella vostra azienda come



# WannaCry e NotPetya: presa di coscienza della necessità di introdurre nuovi controlli e comunicare meglio il rischio (per oltre un 40% di aziende)

Nell'ultimo anno, come conseguenza di cyber attacchi rilevanti (WannaCry, NotPetya), nella sua azienda ...

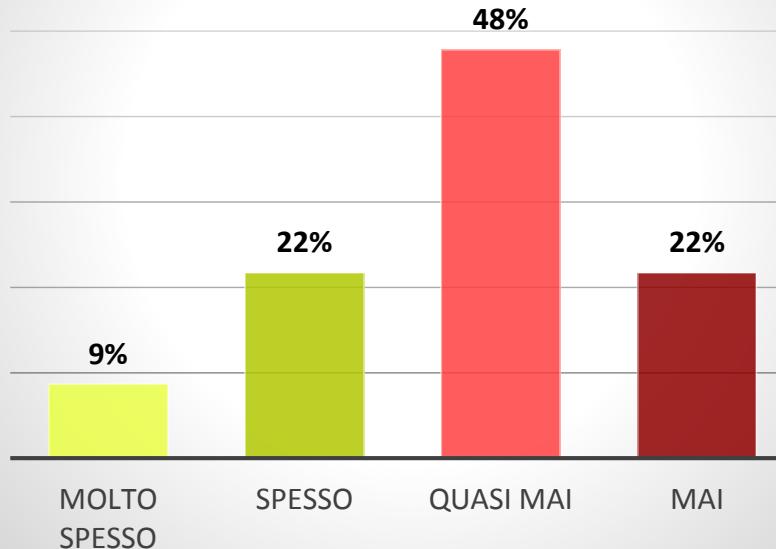


SONO CAMBIATI I CONTROLLI DI CYBERSECURITY

E' CAMBIATO IL MODO DI COMUNICARE I RISCHI/GLI  
INCIDENTI CYBER AL CONSIGLIO DI AMMINISTRAZIONE  
(CDA)/BOARD

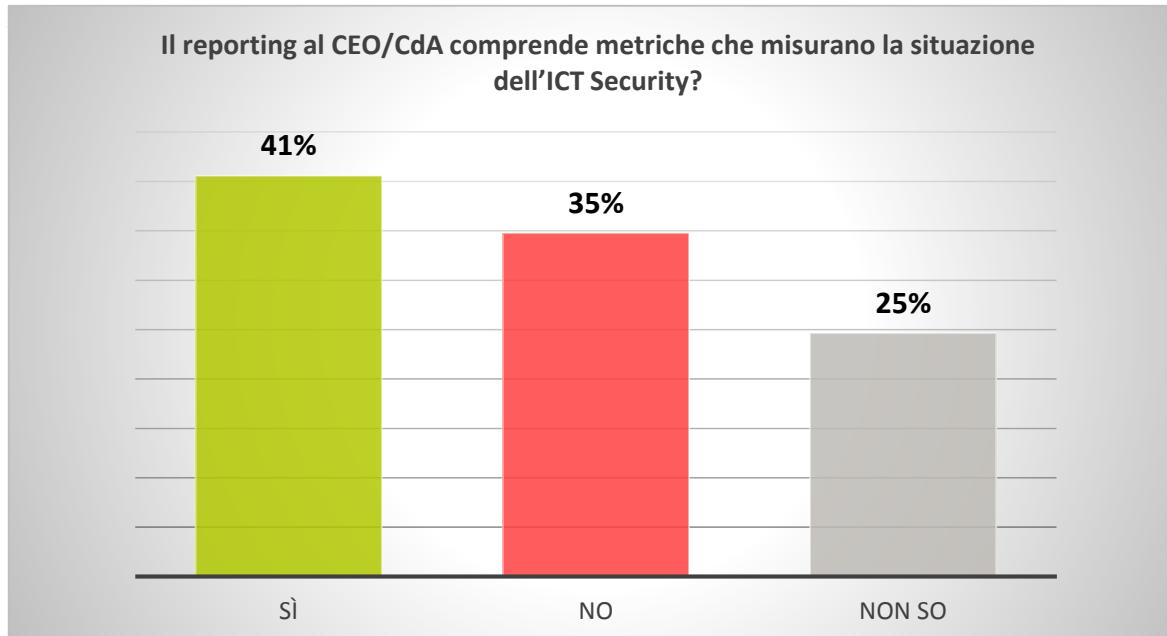
# Spesso il CEO/Board non è consapevole del rischio cyber

Quanto spesso il CISO/ruolo equivalente, partecipa ad incontri con il CEO/CdA durante l'anno?



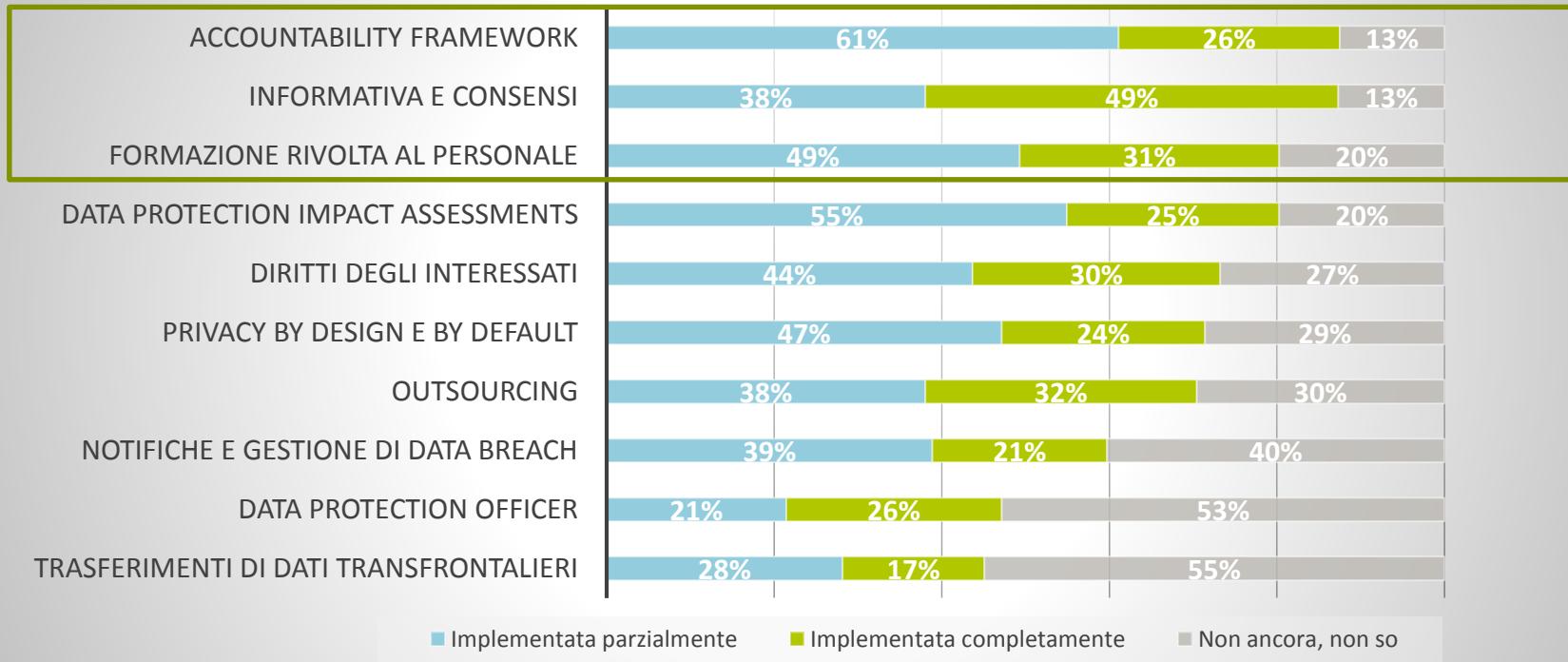
Fonte: The Innovation Group, Cyber Risk Management 2018 Survey, gennaio 2018. N = 88 aziende italiane

# Un sistema decisionale efficace andrebbe basato su una misurazione più quantitativa del fenomeno



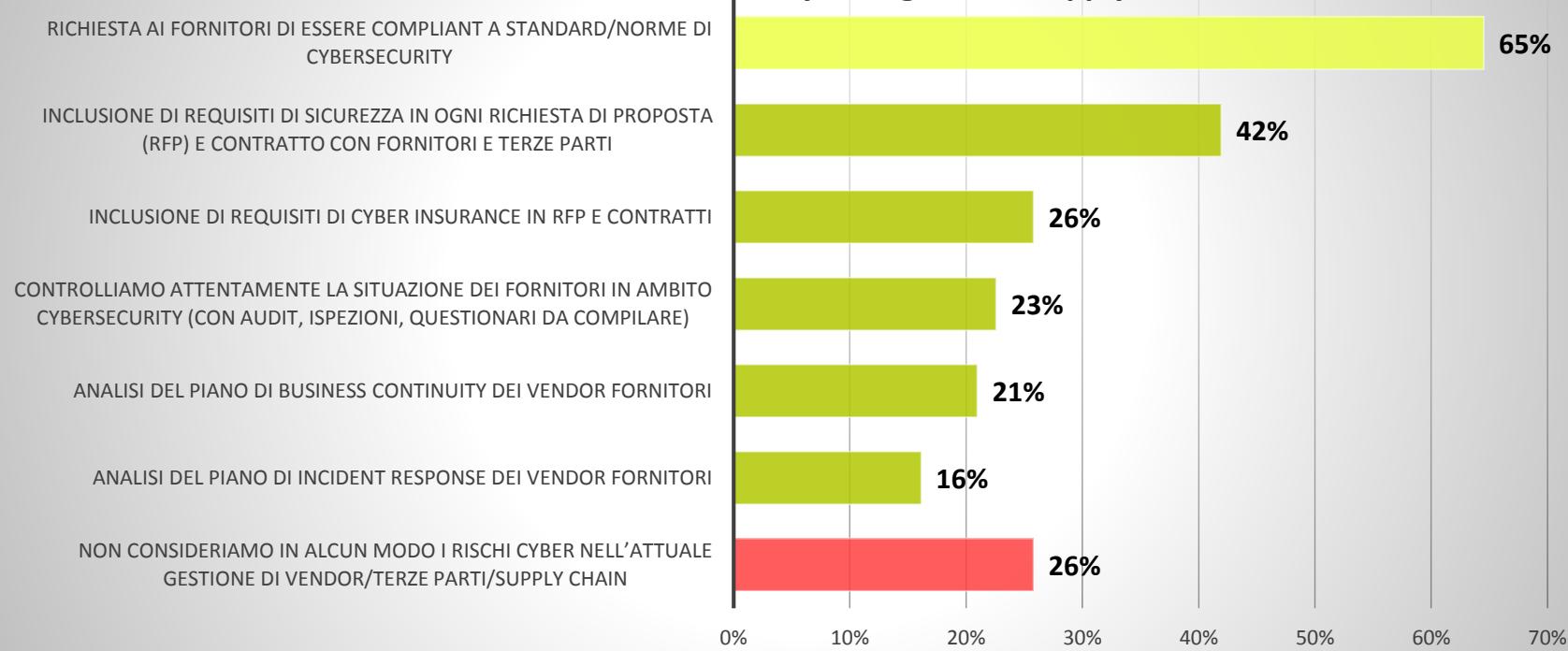
# A gennaio 2018: molti progressi ma ancora lavori in corso

Qual è la situazione della vostra azienda con riferimento alle misure da attuare per la GDPR?

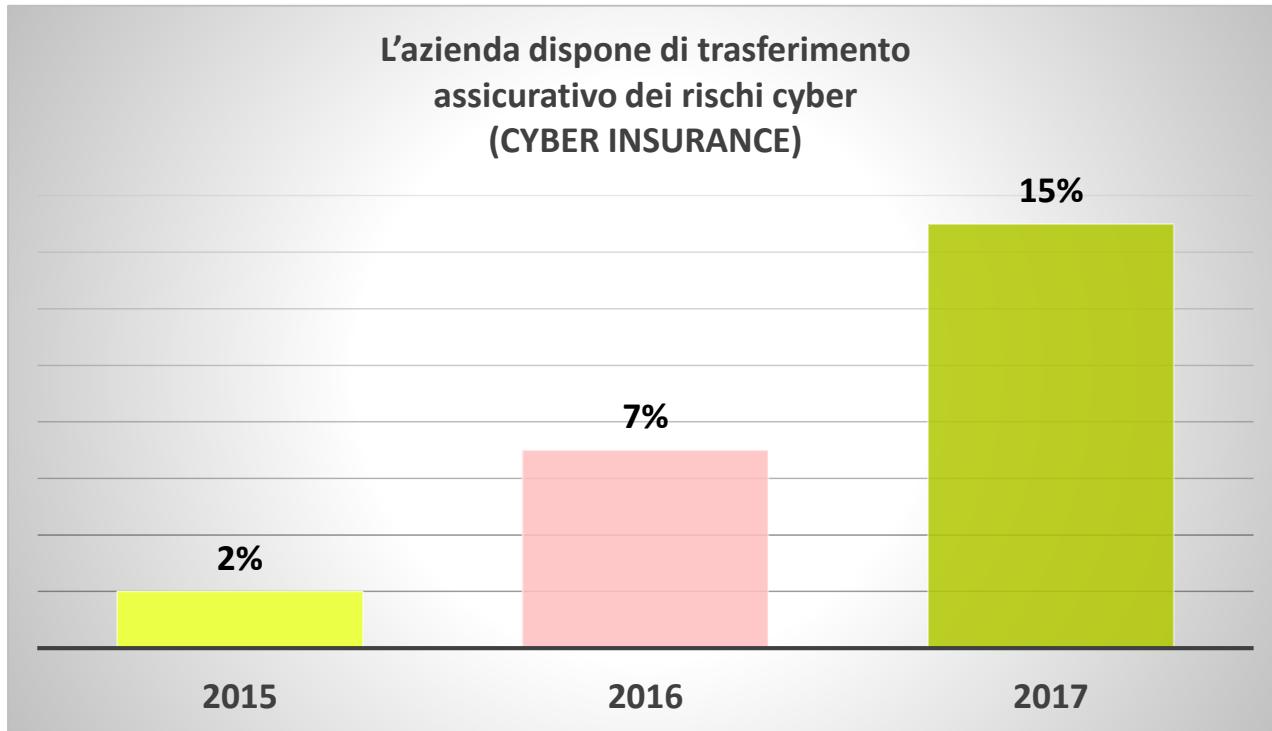


# I $\frac{3}{4}$ delle aziende ha già controlli per la sicurezza della Supply Chain

Quali dei seguenti controlli di Vendor Management ha implementato la sua azienda per ridurre il rischio cyber legato alla Supply Chain?



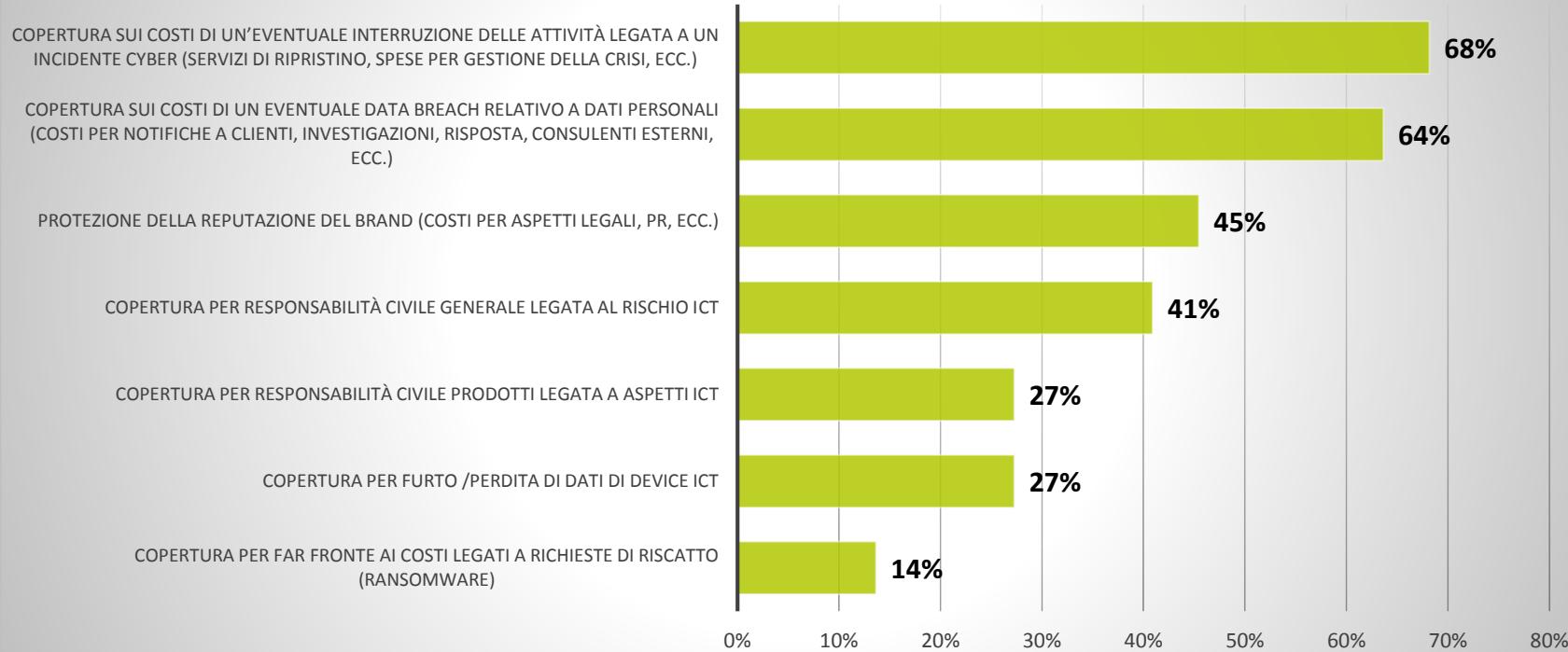
# Crescita molto elevata della Cyber Insurance negli ultimi 3 anni



Fonte: The Innovation Group, Cyber Risk Management 2018 Survey, gennaio 2018. N = 88 aziende italiane  
Confronto con Cyber Risk Management Survey di The Innovation Group e Deloitte, gennaio 2017 e febbraio 2016

# Business Continuity e Data Breaches sono i principali ambiti per la Cyber Insurance

Se si dispone/si prevede di avere a breve una copertura cyber, i motivi sono:

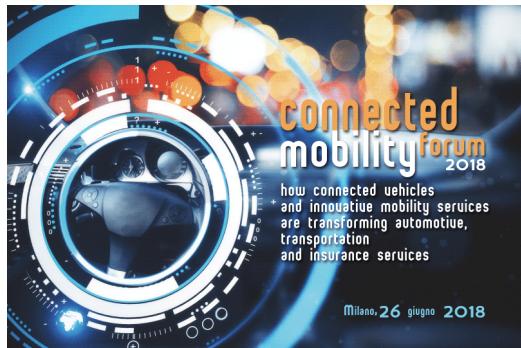


# Sintesi e Conclusioni

- ✓ **Le strategie di Cybersecurity non sono ancora** : vulnerabilità, sofisticazioni, crescita e dinamiche degli attacchi stanno ponendo sfide significative alle aziende italiane
- ✓ **I modelli organizzativi e i processi per la gestione e governance della Cybersecurity sono ancora «silos based»** : sono necessari più integrazione e coordinamento e una migliore comunicazione con il Top Management basata su performance indicator quali-quantitativi
- ✓ **Compliance è uno dei principali driver di investimento** : le aziende devono ripensare la cybersecurity come parte dell'approccio al Risk Management
- ✓ **Cyber threat intelligence, monitoring della supply chain dei vendor può facilitare la previsione** delle minacce e i rischi associati e valutare le priorità di investimento

*Come il Cyber Risk Management deve evolvere nelle organizzazioni Medio-Grandi ?*

# I PROSSIMI APPUNTAMENTI



Milano, 26 giugno



Milano, 20 settembre



Milano, 5 luglio



Stresa, 4 e 5 ottobre

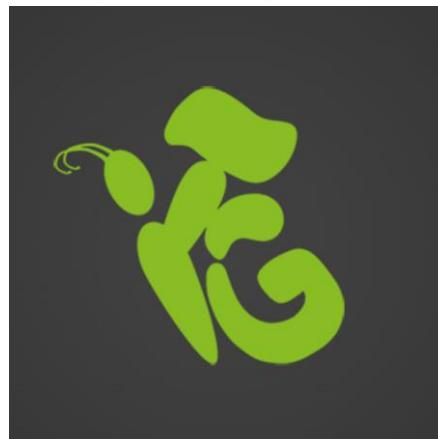
INTERAGISCI CON NOI...

Manda la tua domanda allo



+39 344 057 2201

# SCARICA L'APP MY TIG



**The Innovation Group**  
via Palermo, 5, 20121 Milano – Italia  
Tel. +39-02-87285500  
Fax +39-02-87285519

Website: [www.theinnovationgroup.it](http://www.theinnovationgroup.it)  
E-mail: [info@theinnovationgroup.it](mailto:info@theinnovationgroup.it)