Protezione Cyber

Cyber Risk nella professione del commercialista

Indagine 2016

Dott. Andrea Natta
Dott. Luca Furgiuele

Ricerca effettuata con la supervisione scientifica della **Prof.ssa Paola De Vincentiis**, Dipartimento di Management, Scuola di Management ed Economia - Università degli Studi di Torino

Chi siamo

- **Protezione Cyber** è la divisione rischi informatici di **Furgiuele Srl**, società di consulenza e intermediazione assicurativa, che dal 1975 affianca le aziende e i professionisti nella predisposizione e gestione dei programmi assicurativi.
- Siamo **specializzati nel trasferimento assicurativo dei rischi informatici** mediante l'offerta di innovative soluzioni rivolte ad aziende e professionisti: **le polizze cyber risk,** studiate per tutelare l'**operatività**, la **solvibilità** e la **reputazione** degli assicurati.
- **Quali intermediari abbiamo la facoltà di selezionare le migliori soluzioni disponibili sul mercato assicurativo adattandole alle specifiche esigenze dell'assicurando.**
- **Team di professionisti con formazione specifica** in:
  - Risk Management
  - Informatica
  - Assicurazione

L'indagine: perché il settore dei commercialisti?

- Professione sempre più legata all'uso degli strumenti informatici e alla **digitalizzazione del dato**

- I commercialisti e le PMI sono vittime appetibili in quanto:
  - la piccola dimensione spesso è sinonimo di **minori risorse disponibili da destinare alle politiche di prevenzione e protezione**;
  - sfruttati come **"ponte"** per aggirare più facilmente le solide difese delle grandi imprese

    → sicurezza della filiera produttiva
  - **la minore dimensione NON è sinonimo di risorse meno preziose** (ingente quantità di dati personali di persone fisiche, di aziende, di dipendenti, ecc.)
  - **processi meno formalizzati:**

    → reti di comunicazione con fornitori e/o clienti meno controllate e basate sulla fiducia

«Cyber Risk nella professione del commercialista»
Indagine 2016

- **Autori:**

Dott. Andrea Natta e **Dott. Luca Furgiuele** di **ProtezioneCyber**, sotto la supervisione scientifica della **Prof.ssa Paola De Vincentiis**, Dipartimento di Management della Scuola di Management ed Economia dell'**Università degli studi di Torino.**

- Popolazione di riferimento:

2.500 Commercialisti iscritti all'Albo di Torino, Ivrea e Pinerolo

- Campione rispondenti:

4,5% del totale

- **Questionario di 134 domande divise in 3 sezioni:**

1) Attività e organizzazione

2) Percezione e conoscenza dei rischi

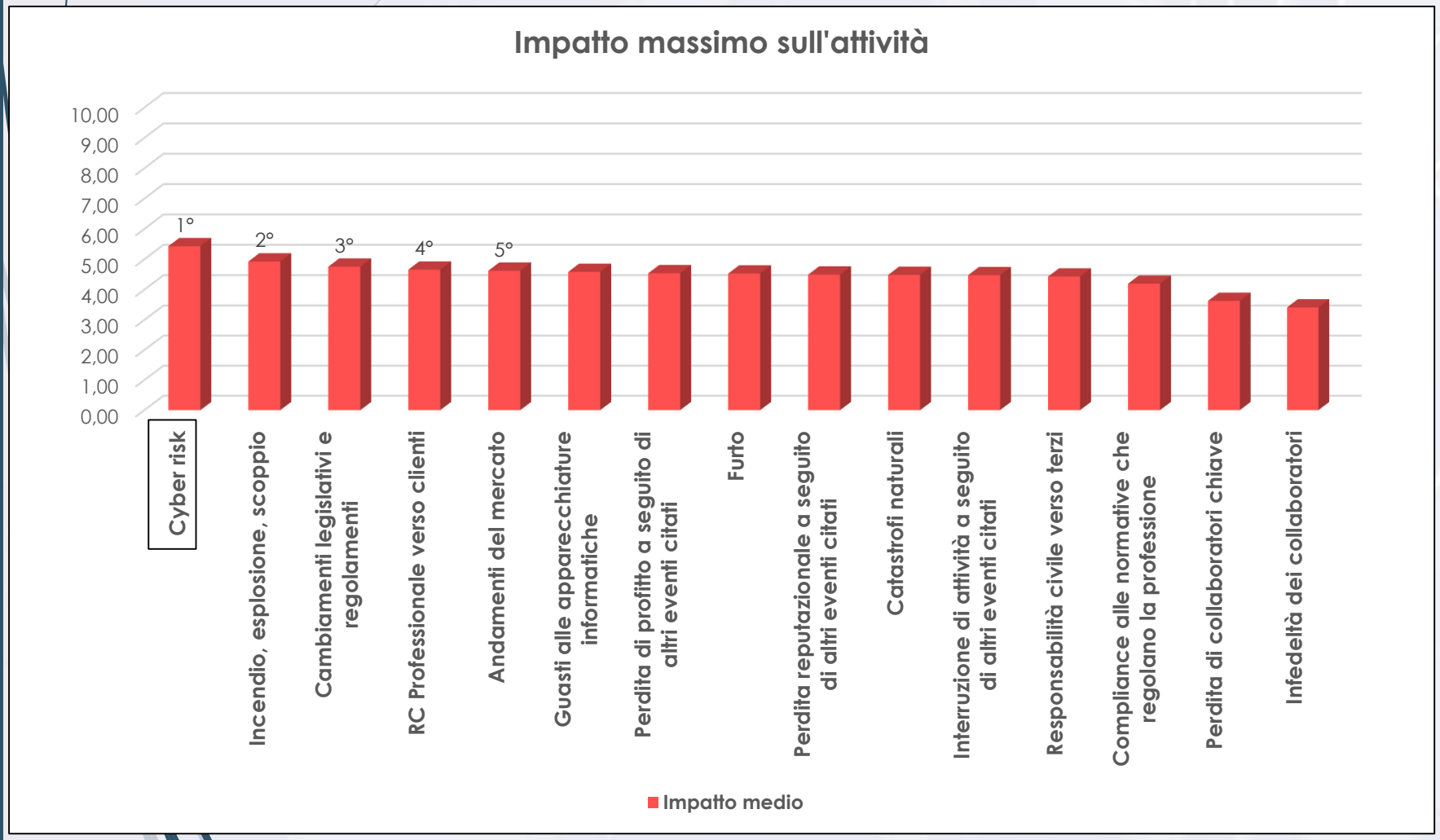
3) Trattamento e gestione del rischio

L'indagine – Gli Obiettivi

- Far emergere la **percezione e il grado di conoscenza dei commercialisti** in merito a:
  - cyber risk in generale;
  - impatto dei rischi informatici;
  - sicurezza del proprio sistema IT;
  - assicurazione del danno derivante dal rischio informatico.
- **Classificare** per importanza i **rischi ritenuti più preoccupanti** dai commercialisti, in base a probabilità e impatto. Con particolare focus sul Cyber Risk.
- Registrare lo **stato attuale del sistema di prevenzione e protezione** adottati e le misure di gestione e trattamento del rischio.
- **Valutare l'adeguatezza delle polizze cyber attualmente offerte dal mercato assicurativo** alle effettive necessità del professionista.

L'indagine: i principali risultati

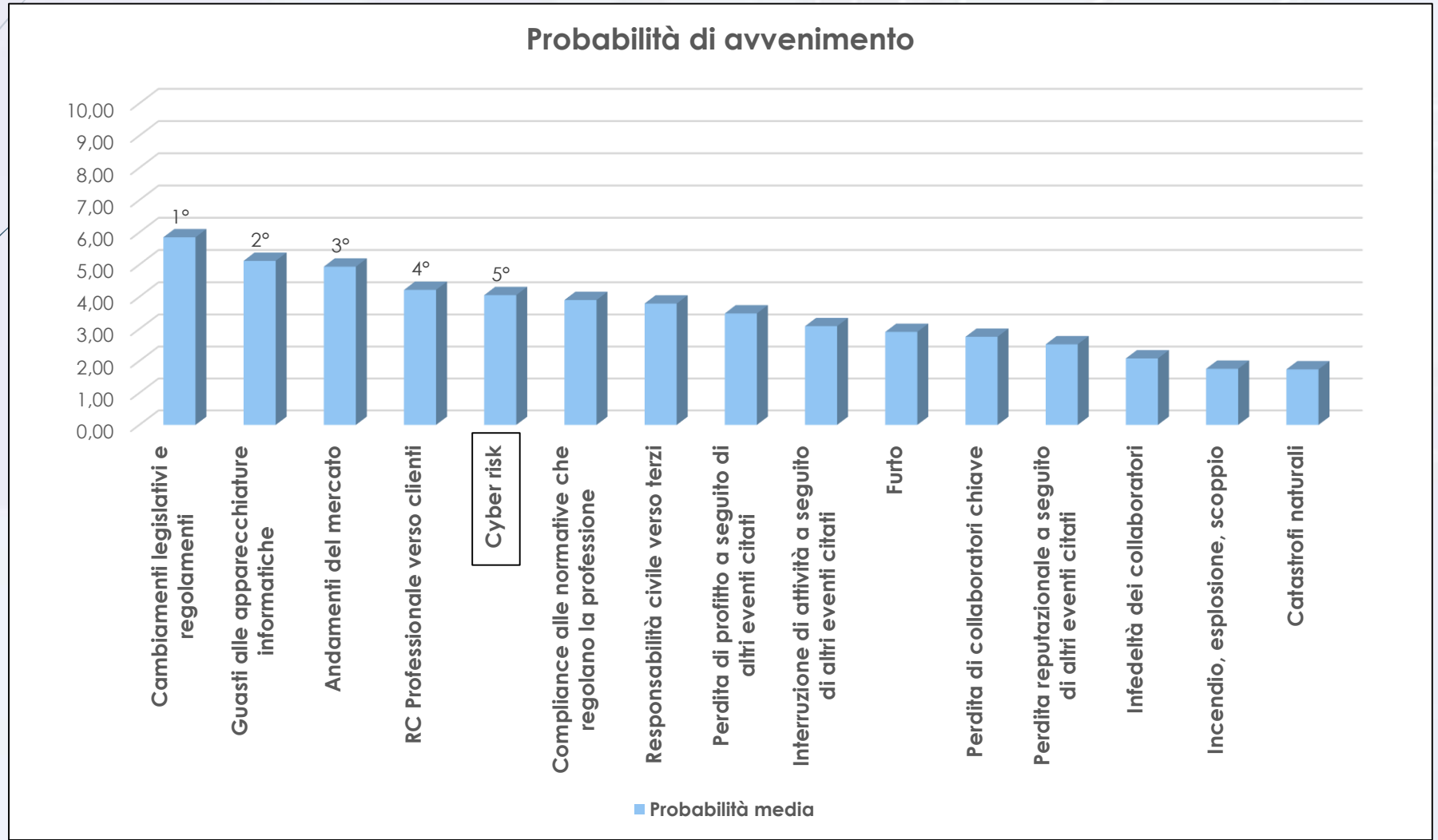
Il Cyber Risk è il rischio ritenuto più preoccupante in termini di impatto potenziale!



- *Questa consapevolezza è accompagnata da un approccio proattivo alla gestione del rischio Cyber?*
- *Quale sarebbe l'impatto sulla propria attività in seguito alla divulgazione, indisponibilità e/o perdita di dati elettronici?*

L'indagine: i principali risultati

Diffusa consapevolezza della portata del rischio Cyber in termini di probabilità



L'indagine: i principali risultati

Combinando i punteggi assegnati dai commercialisti alla probabilità/impatto di ogni rischio, quelli che in assoluto sono ritenuti più pericolosi sono:

→ Considerando che i Guasti alle apparecchiature informatiche sono una fattispecie inclusa nel Cyber Risk, la posizione dello stesso è sottostimata.

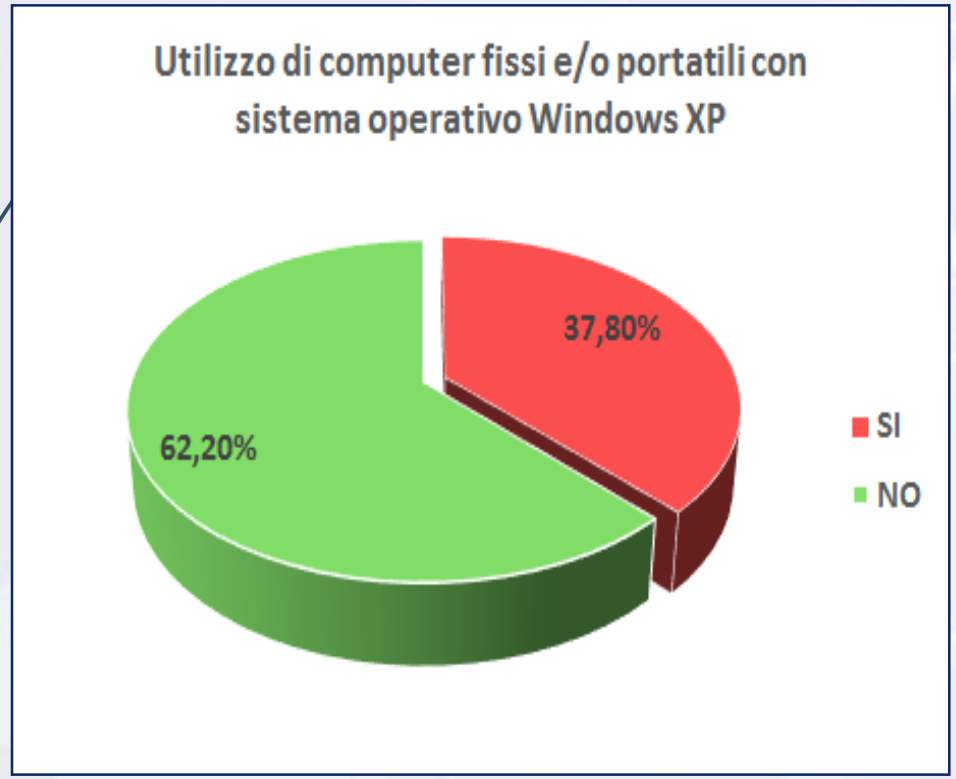
1. Cambiamenti legislativi e regolamenti
2. Guasti alle apparecchiature informatiche
3. Andamenti del mercato
4. **Cyber Risk**
5. RC Professionale verso clienti

L'indagine: i principali risultati

Mancanza di compliance alla Normativa Privacy

→ non completa adozione degli strumenti di prevenzione e protezione e delle misure minime.

Ad esempio:



Windows XP non è più aggiornato da Microsoft da Aprile 2014!

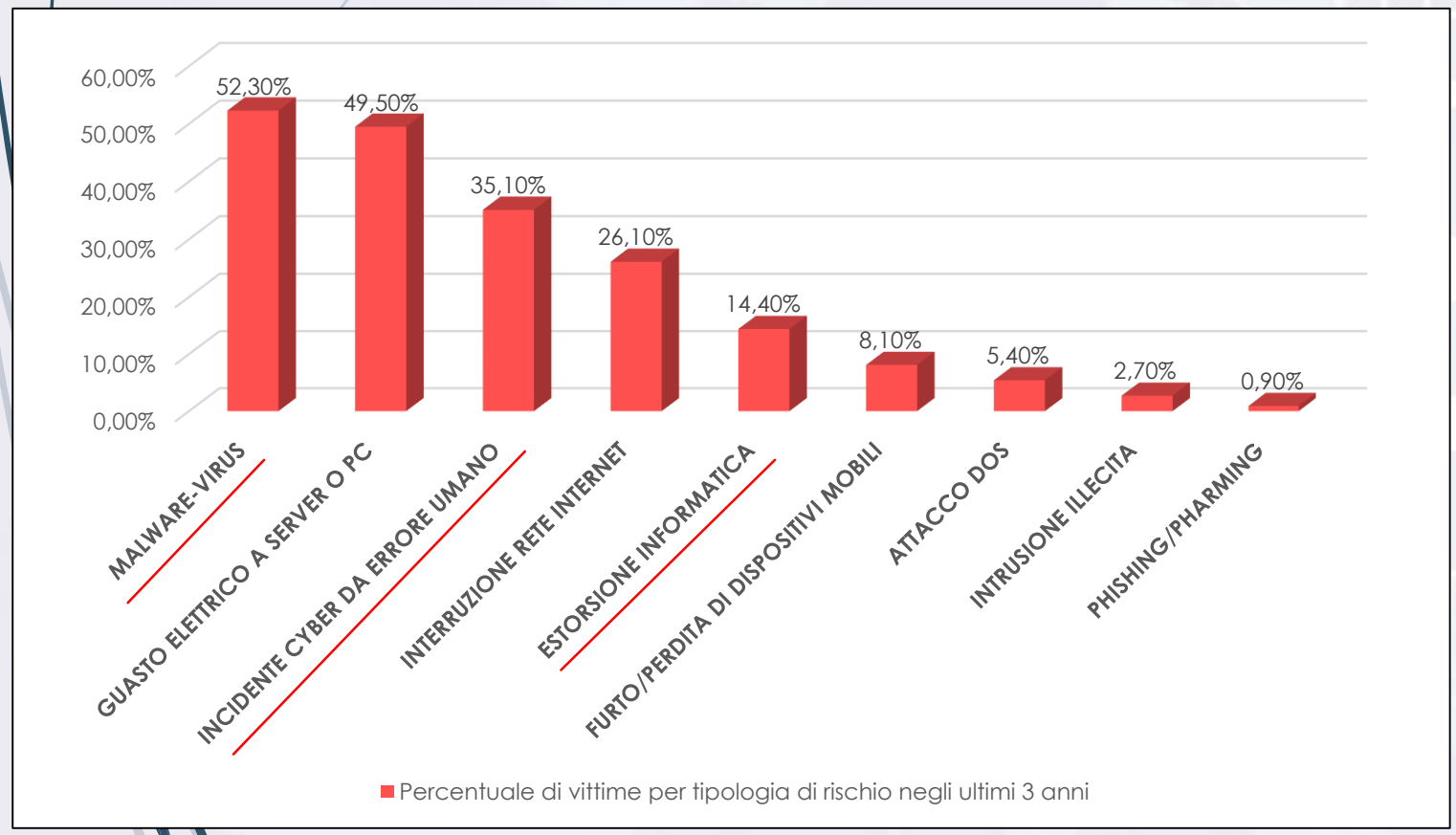
Pertanto il suo utilizzo comporta:

- maggiori rischi conseguenti a **vulnerabilità non più risolte** sul sistema;
- **non conformità alla Normativa Privacy** → sanzioni pecuniarie e sanzioni penali.

Il Codice della Privacy infatti prescrive l'**obbligo di aggiornamento semestrale** dei software contenenti dati sensibili.

L'indagine: i principali risultati

Percentuale di commercialisti vittime di eventi cyber negli ultimi 3 anni



1. Il **52,30% del campione è stato vittima di Malware** almeno una volta negli ultimi 3 anni (più della metà nell'ultimo anno) → **Incremento.**

2. **Estorsione informatica** (Ransomware): la quasi totalità è avvenuta nell'ultimo anno → **Incremento**

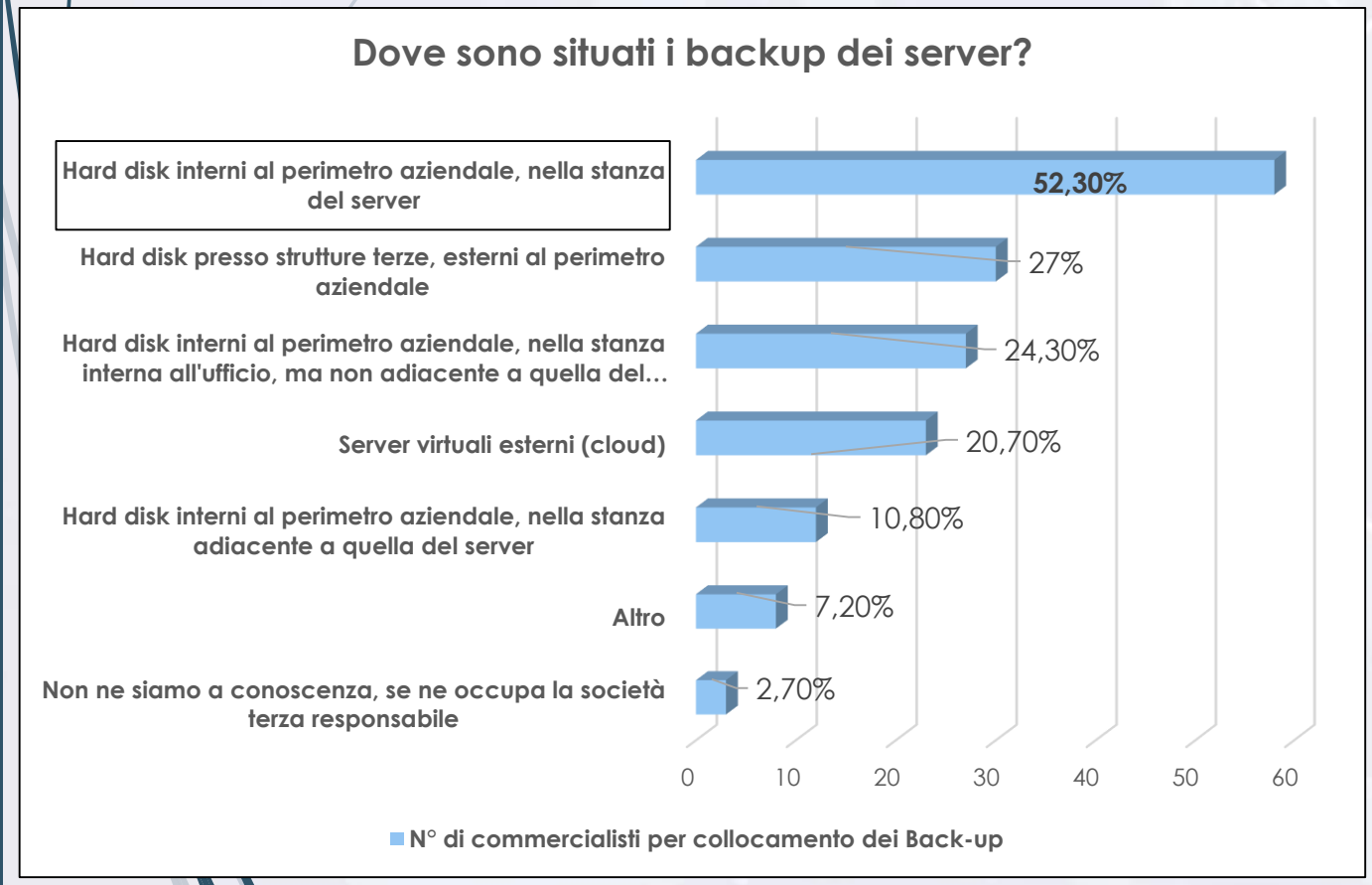
3. **Attenzione all'errore umano**: causa di incidenti informatici per il **35%** dei commercialisti del campione. *Avete in atto politiche di formazione del personale in ambito informatico?*

4. **Per molte di queste minacce il tempo di ripristino supera una giornata lavorativa; in alcuni casi il fermo può arrivare ad un'intera settimana.**

L'indagine: i principali risultati

Insufficiente percezione delle implicazioni economiche e di responsabilità di un evento cyber

Esempio 1



→ Risulta **molto pericoloso conservare i backup nella stessa stanza in cui si trovano i server** (Es: un incendio o altro guasto nella sala server intaccherà anche i backup)

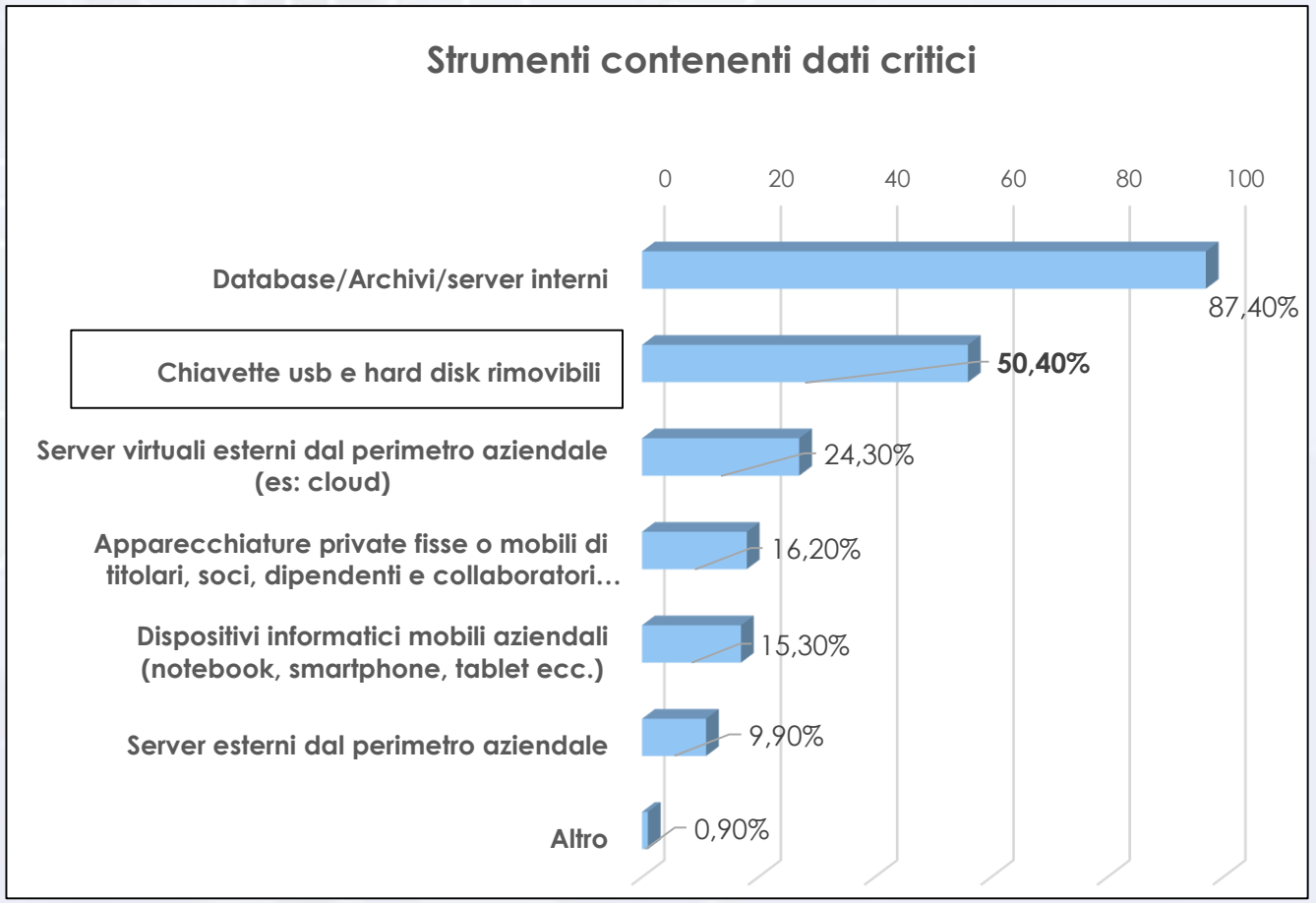
L'indagine: i principali risultati

Insufficiente percezione delle implicazioni economiche e di responsabilità di un evento cyber

Superficie di rischio più ampia se si detengono dati critici su:

- **chiavette Usb** (facilmente smarribili e/o veicoli di infezione)
- **device personali e/o mobili** che si portano al di fuori dell'ufficio (livello di sicurezza tendenzialmente inferiore rispetto agli hardware fissi aziendali)

Esempio 2



L'indagine: i principali risultati

- **Il 60,40% di commercialisti non fa formazione ai propri dipendenti in ambito di sicurezza informatica**
- L'errore umano è la prima causa di incidenti informatici → Sbagliato sottovalutarlo!

- Con la Nuova Normativa Europea sulla Protezione dei Dati (**GDPR**) la formazione in ambito di sicurezza informatica diventerà obbligatoria!