Ania

Associazione Nazionale
fra le Imprese Assicuratrici

Cyber risk, assicurazioni e PMI

Carlo Savino

Senior Economist - ANIA

Milano, 7 marzo 2017

Agenda

- La dimensione del fenomeno
- Rischio informatico e assicurazione
- Analisi dei costi per danno informatico risarciti dalle assicurazioni
- La percezione delle imprese del rischio informatico in Italia e in Europa
- Le modalità di gestione del rischio informatico da parte delle imprese

Il cyber risk è la più temuta tra le minacce dai risk-manager

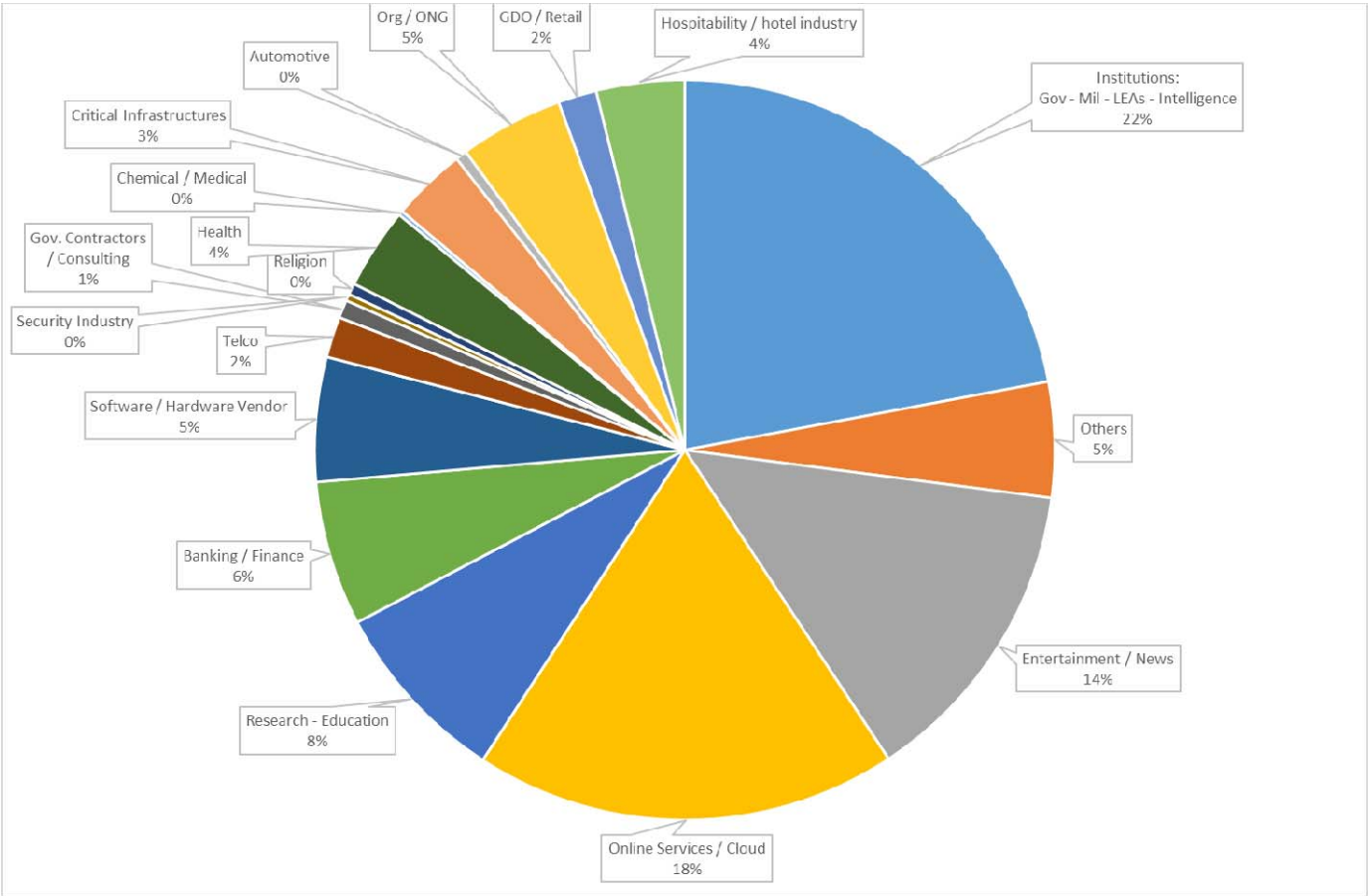
- L'Allianz Risk Barometer 2016 valuta che per i Risk Manager intervistati (circa 800) la **Business Interruption** è il rischio più temuto, che dipende in modo crescente dall'impiego di tecnologie digitali
- L'**incidente Cyber** propriamente detto è al terzo posto nella classifica delle minacce
- Sempre influenzati dalle nuove tecnologie sono la **perdita di reputazione** al settimo posto, fino al decimo posto con i **furti e le frodi**
- Questi quattro rischi sono considerati prioritari da circa il 45% del campione

La dimensione del fenomeno: andamento globale degli attacchi informatici

	2011	2012	2013	2014	2015	2015 su 2011
Cybercrime	170	633	609	526	684	+302%
Hacktivism	114	368	451	236	209	+83%
Espionage	23	29	67	69	96	+317%
Information Warfare	14	43	25	42	23	+64%

Attacchi informatici globali
Fonte: Clusit

La dimensione del fenomeno: chi viene attaccato



Distribuzione attacchi per tipologia di vittima
Fonte: Clusit

La dimensione del fenomeno: i costi globali

Globali ($ mld)	
Symantec (2013)	113
McAfee (2014)	445 (375-575)
Kshetri (2010)	100-1000

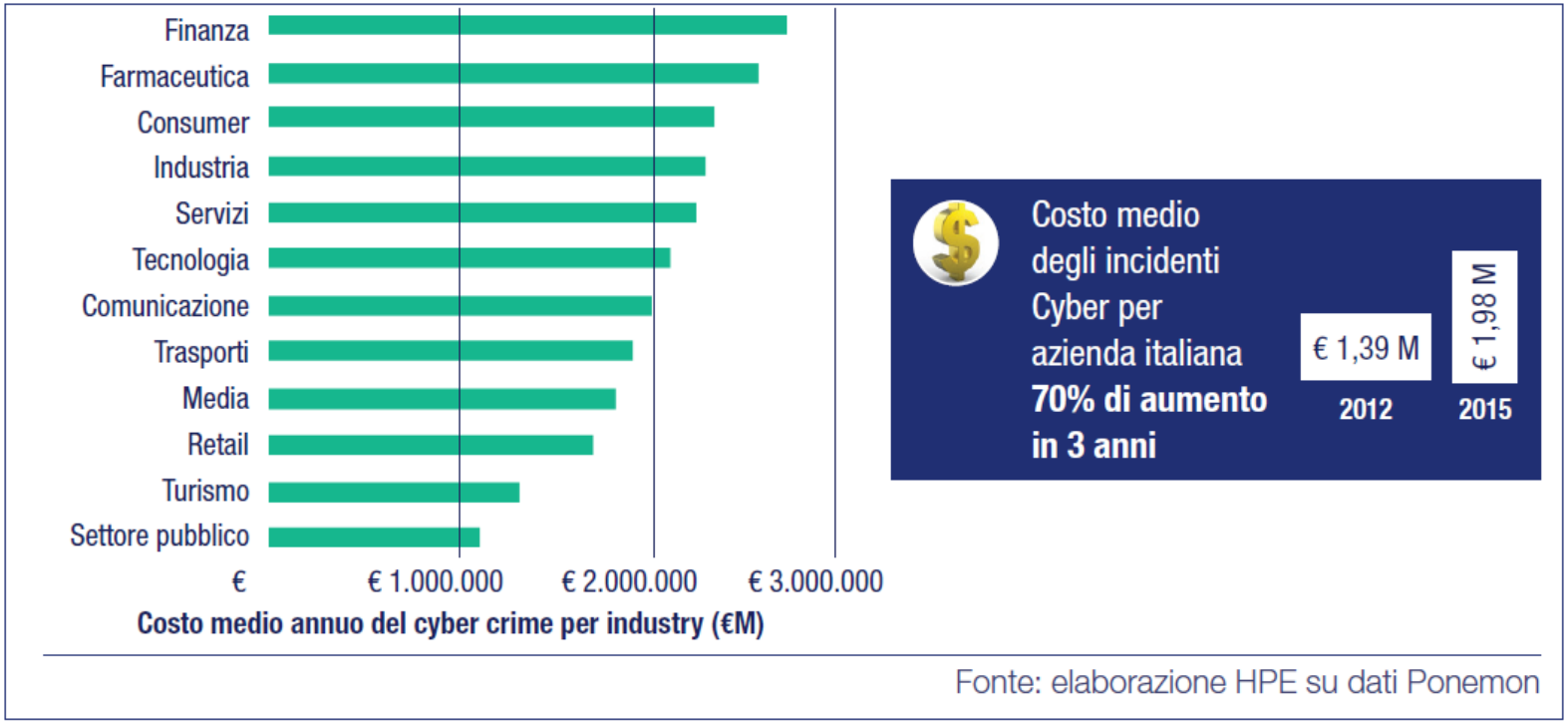
Per evento($ mln)	
Ponemon Institute (2015)	38
Geschonneket *al*. (2013)	21
Kaspersky Lab (2013)	24

per record ($)	
Symantec (2013)	298
Ponemon Institute (2015)	217
NetDiligence (2014)	956

Per paese (in % PIL)	
U.S.	0.64
China	0.63
Japan	0.02
Germany	1.60

Fonte: Geneva Association

La dimensione del fenomeno: i costi degli attacchi informatici in Italia



Iniziative governative/internazionali sul fenomeno cyber

- Priorità nella Global Agenda on Risk & Resilience del **World Economic Forum**
- In Europa: ENISA, l'Agenzia Europea per la sicurezza delle reti e delle informazioni
  - Produce Raccomandazioni
  - Offre sostegno per l'implementazione di politiche nazionali
  - Collabora con altre istituzioni UE sul tema della sicurezza digitale
- In Italia: «**Quadro Strategico Nazionale per la Sicurezza nello Spazio Cibernetico**», elaborato dal Tavolo Tecnico Cyber nel 2013, con lo scopo di potenziare la capacità di reazione del sistema paese alla minaccia cibernetica
  - Definendo e quantificando il fenomeno nel nostro paese
  - Identificando attori, strumenti e iniziative, pubbliche e private, per combatterlo

La natura del rischio cibernetico

- Il rischio informatico, o cyber risk, è un rischio di tipo operativo associato alle perdite economiche inflitte a una organizzazione dalla mancata confidenzialità, disponibilità di integrità di informazioni e/o sistemi informativi, propri o di terzi
- La sua origine può essere:
  - Accidentale. Sono eventi che si verificano indipendentemente dalla volontà di tutti i soggetti coinvolti (es. spegnimento server)
  - Deliberata (es. cyber crime). Sono eventi che derivano da azioni volontarie di soggetti allo scopo di raggiungere obiettivi personali di varia natura (es. furto dati sensibili)
- Il danno economico a un'organizzazione può derivare da malfunzionamenti del proprio sistema IT o essere conseguenza di malfunzionamenti di altri sistemi su cui non si ha il controllo
- Il rischio cyber può avere caratteristiche sistemiche, al pari del rischio finanziario. Casi isolati possono ripercuotersi su scala ben maggiore

Conseguenze potenziali di un evento cibernetico (accidentale o deliberato)

- Interruzione dell'attività
- Danno reputazionale/di immagine
- Diffusione di informazioni sensibili (clienti, pazienti, impiegati, fornitori)
- Violazione informazioni finanziarie; violazione conti bancari
- Violazione proprietà intellettuale
- Perdita quote di mercato
- Appropriazione identità
- Azioni legali da terzi
- Ecc.

Rischio informatico e assicurazioni

- Fine anni ‘70: prime polizze specializzate contro i crimini informatici
- Anni ’90: le compagnie di software commercializzano coperture attraverso accordi commerciali con le assicurazioni
- 1998: prima polizza anti-hacker
- Con la crescita dell’uso a fini commerciali di Internet aumenta l’incidenza e la severità degli attacchi informatici.
  - Nel 2000 alcuni hacker on-line «spengono» i siti di Amazon, eBay, CNN e altri grandi corporazioni causando danni stimati per $1,2 miliardi.
  - L’interesse per le coperture specifiche cresce esponenzialmente
- Due tipologie di coperture (danni):
  - Assicurazione primaria diretta che risarcisce chi si assicura (danni ad asset informatici, interruzione attività, danno reputazionale, estorsione, furto, ecc.)
  - Assicurazione RC vs. terzi (violazione dati sensibili, costi forensi, azioni legali, indennizzi a terzi)

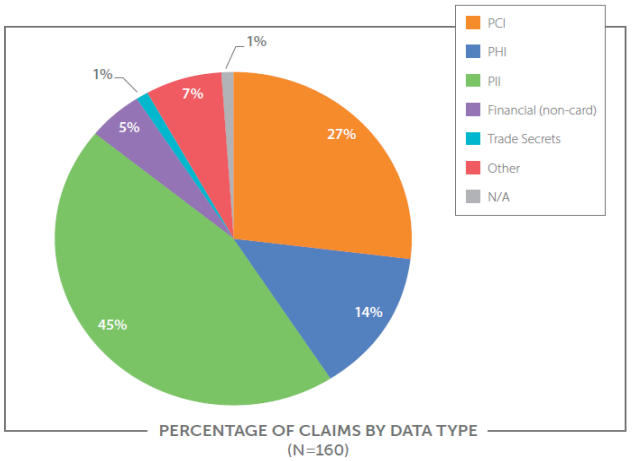
I rami assicurativi interessati dal rischio cyber

- Le **polizze tradizionali** con cui mettere in relazione la copertura Cyber o da analizzare in ottica Cyber prima di prendere delle decisioni sono:
  - Polizza Incendio
  - Polizza Danni Indiretti o Business Interruption
  - Polizza Elettronica
  - RC Generale – Responsabilità Civile Generale
  - RC Professionale – Responsabilità Civile Professionale
  - RC Prodotti – Responsabilità Civile per prodotto difettoso
  - D&O – Responsabilità degli Amministratori e dei Dirigenti
- Dalla lettura dei testi emerge che le polizze spesso non considerano o escludono in maniera specifica problematiche ICT correlate
- **Una copertura Cyber** è di solito strutturata in **macro-moduli attivabili o meno,** generalmente riguardanti:
  - Responsabilità Civile verso Terzi, tipicamente per violazione della privacy o utilizzo non autorizzato della
  - infrastruttura informatica;
  - Costi di reazione indennizzabili a fronte di sinistro;
  - Danni indiretti.

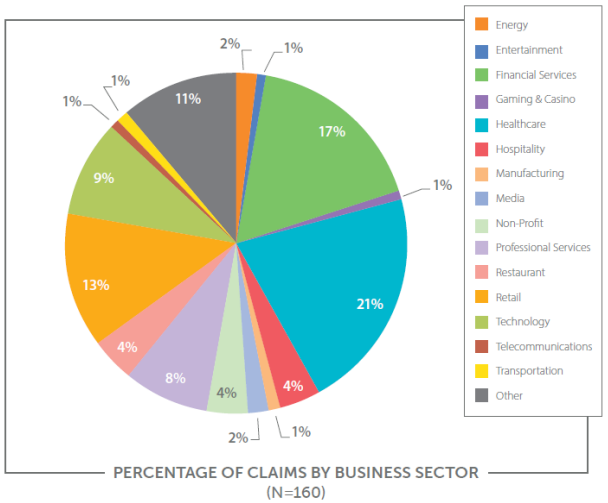
Assicurabilità rischio cyber?
In generale: sì, ma con molte criticità specifiche

Un’analisi dei costi per danno cyber risarciti dalle assicurazioni - 1

% di sinistri per tipologia di dato violato



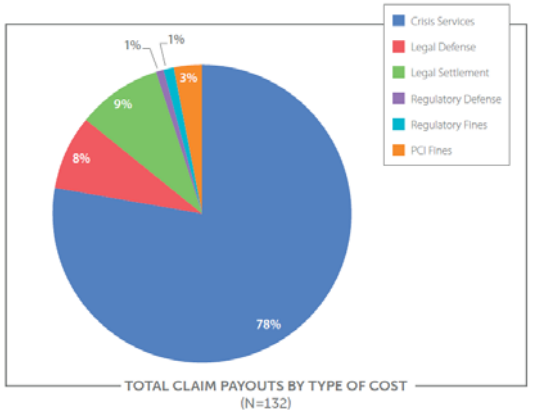
% di sinistri per settore di attività



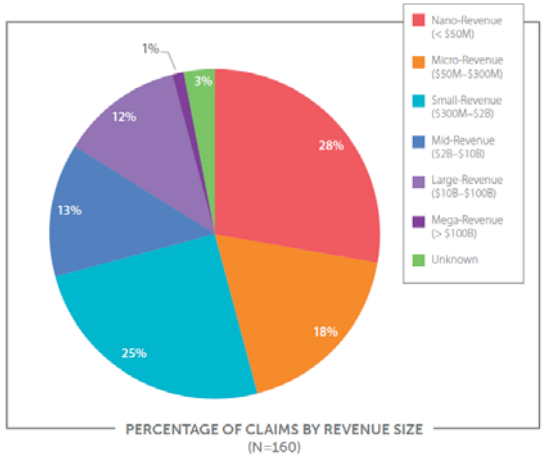
Campione: 160 imprese USA
Fonte: Netdiligence, 2015

Un’analisi dei costi per danno cyber risarciti dalle assicurazioni - 2

% di sinistri per tipo di costo incorso



% di sinistri per dimensione di impresa



Campione: 160 imprese USA
Fonte: Netdiligence, 2015

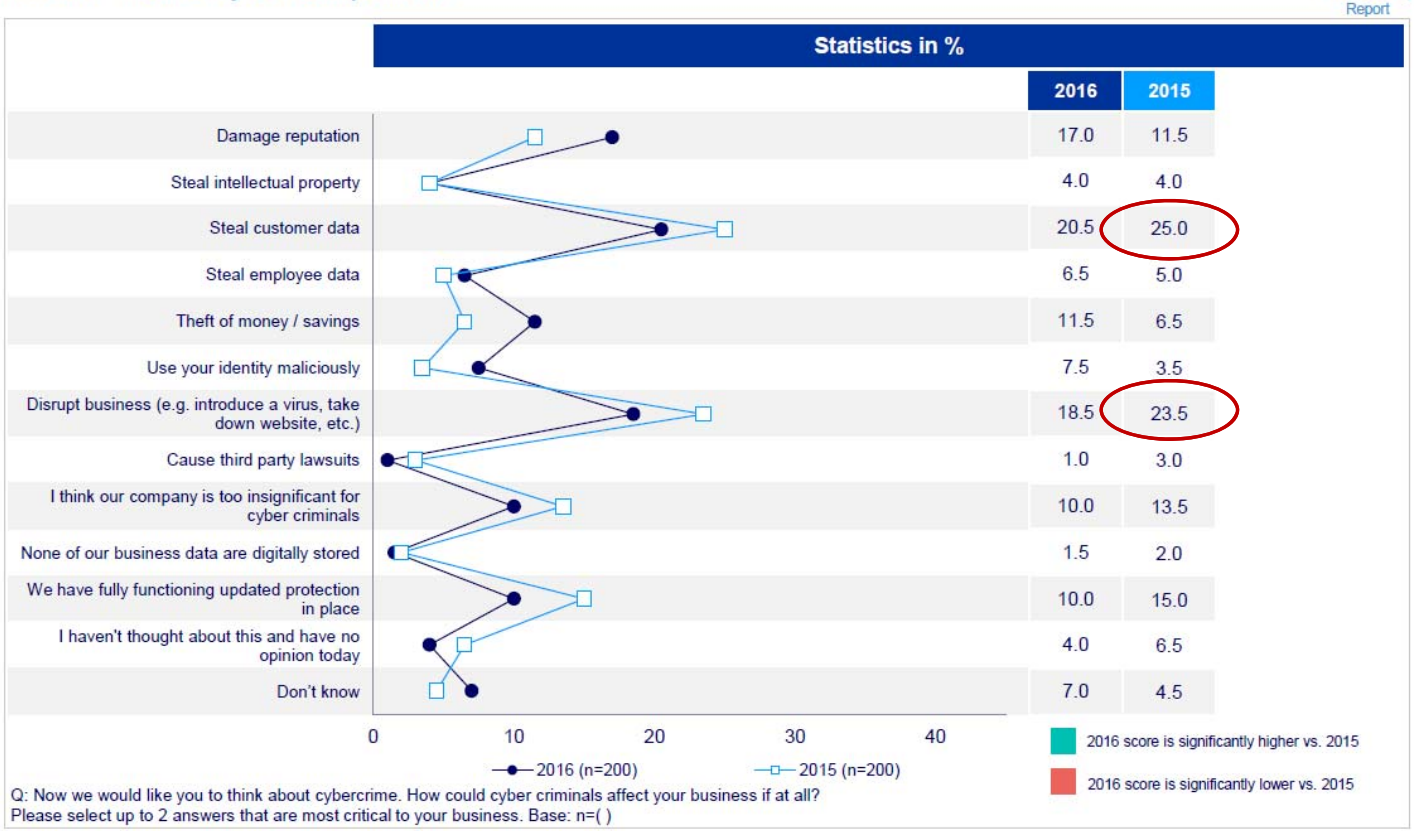
Percezione del rischio informatico delle PMI italiane

Potential business impact of cybercrime on small and medium enterprises in 2016
Results: Year-on-year comparison

Global Survey Report

Statistics in %

	2016	2015
Damage reputation	17.0	11.5
Steal intellectual property	4.0	4.0
Steal customer data	20.5	25.0
Steal employee data	6.5	5.0
Theft of money / savings	11.5	6.5
Use your identity maliciously	7.5	3.5
Disrupt business (e.g. introduce a virus, take down website, etc.)	18.5	23.5
Cause third party lawsuits	1.0	3.0
I think our company is too insignificant for cyber criminals	10.0	13.5
None of our business data are digitally stored	1.5	2.0
We have fully functioning updated protection in place	10.0	15.0
I haven't thought about this and have no opinion today	4.0	6.5
Don't know	7.0	4.5



Q: Now we would like you to think about cybercrime. How could cyber criminals affect your business if at all?
Please select up to 2 answers that are most critical to your business. Base: n=( )

Fonte: Zurich

Rischio informatico e PMI: un confronto europeo sulla percezione del rischio

Potential effect on business of small and medium enterprises due to cybercrime in 2016

Results: Comparison of countries in Europe

Global Survey Report

Note: A fair country comparison requires to consider both, the chart on the left (bubbles) and the chart on the right (ranks).

	Statistics in %								Ranks							
	Switzerland	Austria	Germany	Ireland	Italy	Portugal	Spain	Turkey	Switzerland	Austria	Germany	Ireland	Italy	Portugal	Spain	Turkey
Damage reputation	18	20	17	17	17	14	14	17	4	3	4	2	3	4	5	3
Steal intellectual property	6	5	9	12	4	7	6	16	8	9	7	6	10	9	8	5
Steal customer data	22	27	25	41	21	12	33	26	1	1	1	1	1	5	1	1
Steal employee data	7	8	6	8	7	5	11	6	7	6	8	7	9	10	6	8
Theft of money / savings	13	19	13	17	12	16	16	24	5	4	5	3	4	3	4	2
Use your identity maliciously	19	12	18	16	8	9	10	11	3	5	3	4	7	6	7	7
Disrupt business (e.g. introduce a virus, take down website, etc.)	21	27	21	15	19	5	17	16	2	2	2	5	2	11	3	4
Cause third party lawsuits	2	1	3	4	1	1	2	2	12	13	11	10	13	13	12	11
I think our company is too insignificant for cyber criminals	13	6	12	5	10	16	20	1	6	7	6	8	5	2	2	12
None of our business data are digitally stored	3	2	2	2	2	8	5	1	9	12	12	13	12	8	9	13
We have fully functioning and updated protection in place	3	6	3	5	10	9	3	3	10	8	10	9	6	7	11	10
I haven't thought about this and have no opinion today	2	3	4	3	4	19	4	13	13	11	9	11	11	1	10	6
Don't know	3	4	2	2	7	4	2	4	11	10	13	12	8	12	13	9

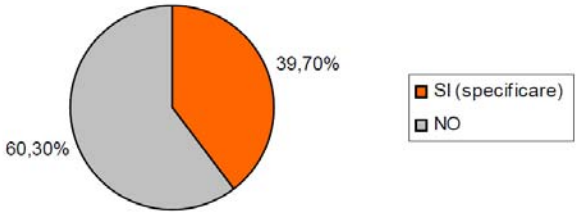
0–15% 16–30% 31%+

Q: Now we would like you to think about cybercrime. How could cyber criminals affect your business if at all? Please select up to 2 answers that are most critical to your business. Base: n=200 per country

Fonte: Zurich

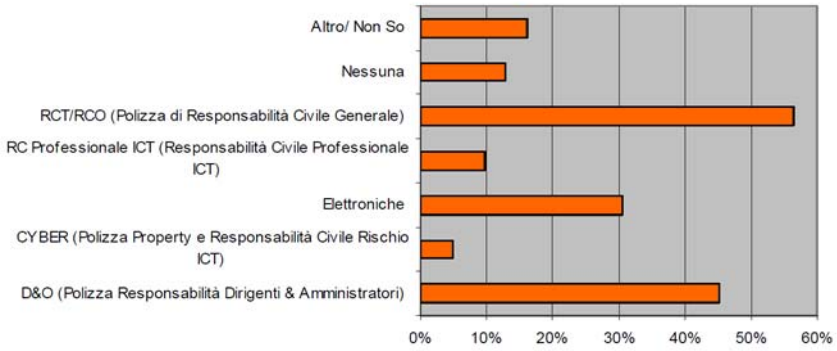
PMI e assicurazione cyber in un campione di imprese del Nord Italia - 1

Negli ultimi 5 anni l'impresa è stata vittima di attacchi informatici?



NOTE: La maggior parte dovuti a Ransomware.

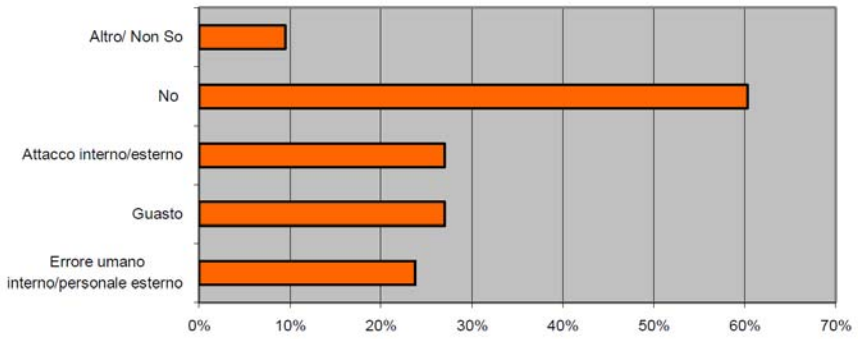
Coperture assicurative in possesso dell'impresa (sono ammesse più risposte)



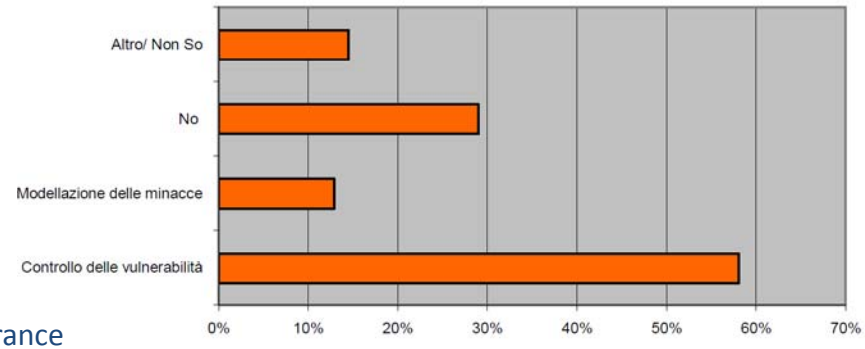
Fonte: WHITE PAPER. Cyber risk exposure & cyber insurance

PMI e assicurazione cyber in un campione di imprese del Nord Italia - 2

Il respondabile IT ha ricevuto esplicita richiesta di quantificare i danni di…
(più risposte sono ammesse)



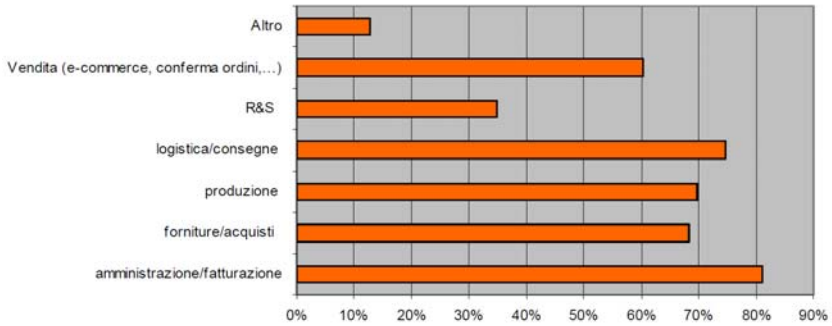
L'impresa ha implementato politiche/procedure di sicurezza IT
(sono ammesse più risposte)



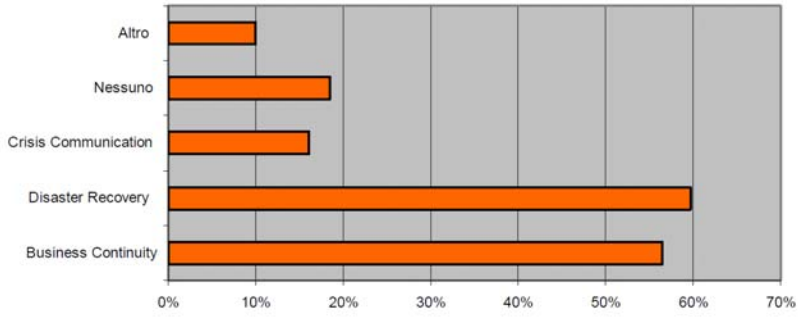
Fonte: WHITE PAPER. Cyber risk exposure & cyber insurance

PMI e assicurazione cyber in un campione di imprese del Nord Italia - 3

**Un malfunzionamento nel sistema IT avrebbe riprcussioni su…
(più risposte sono ammesse)**



**Relativamente al rischio cyber, esistono politiche di…
(sono ammesse più risposte)**



Fonte: WHITE PAPER. Cyber risk exposure & cyber insurance

Conclusioni

- La crescente digitalizzazione dell'economia sta rendendo il rischio informatico sempre più prevalente
- Il rischio informatico possiede caratteristiche peculiari rispetto alle altre tipologie di rischi
- In quasi tutti i paesi le assicurazioni offrono coperture per i rischi informatici (ma lo sviluppo del mercato è ancora limitato)
- Le PMI italiane sono già oggetto di attacchi informatici e stanno prendendo coscienza della minaccia informatica, ma acquistano poche coperture specifiche

Ania

Associazione Nazionale
fra le Imprese Assicuratrici

Grazie per l'attenzione

Cyber risk, assicurazioni e PMI

Carlo Savino

Roma, 3 marzo 2017