United Nations
Interregional Crime and Justice
Research Institute

“La Criminalità Informatica e i Rischi per l'Economia e le Imprese a Livello Italiano ed Europeo”

Flavia Zappa

Con il supporto di

Fondazione
Cassa di Risparmio
di Lucca

Metodologia della ricerca

Analisi dei risultati

Individuazione vulnerabilità delle PMI e necessità per il contrasto al cybercrime

Identificazione aree strategiche e modalità di intervento

Analisi delle fonti a disposizione

Identificazione caratteristiche del fenomeno e rischi per l'economia

Indagine qualitativa sul territorio, ricerca di tipo intensivo, interviste semistrutturate

PMI nell'Unione Europea

- + di 20 milioni di PMI, 99,8% della totalità delle imprese europee
- 86,8 milioni di persone impiegate
- 66,5% della forza lavoro
- Più della metà del fatturato totale europeo
- 92,1 % delle PMI sono micro imprese
- PMI italiane, il più grande settore d'Europa:
  - 3,7 milioni di imprese
  - + 18% del totale europeo

(dati Commissione Europa)

PMI in Italia

- 99,9% della totalità delle aziende
- Oltre 200 distretti industriali, che spesso rappresentano l'eccellenza a livello mondiale
- Produzione del 68% della ricchezza italiana
- 12 milioni di persone impiegate
- 94,4% del totale sono micro imprese
  - Peso in termini di occupazione 46,1%
  - 21% della Germania
  - 22% della Francia
  - 27% della Gran Bretagna

Dimensione globale del cyber crime

- 43% dei costi totali per furto di dati
- 36% dei costi totali per danni al business e perdita di competitività (dati Ponemon Institute)
- 2013, 550 milioni di identità violate (+493% rispetto al 2012) (dati Symantec)
- Fino a 3 mila miliardi di dollari di perdite stimate nei prossimi 6 anni (dati WEF)
- Costo globale del cyber crime tra i 375 e i 575 miliardi di dollari l'anno (dati McAfee)
- + 130% aumento del tempo necessario per la risoluzione di un problema

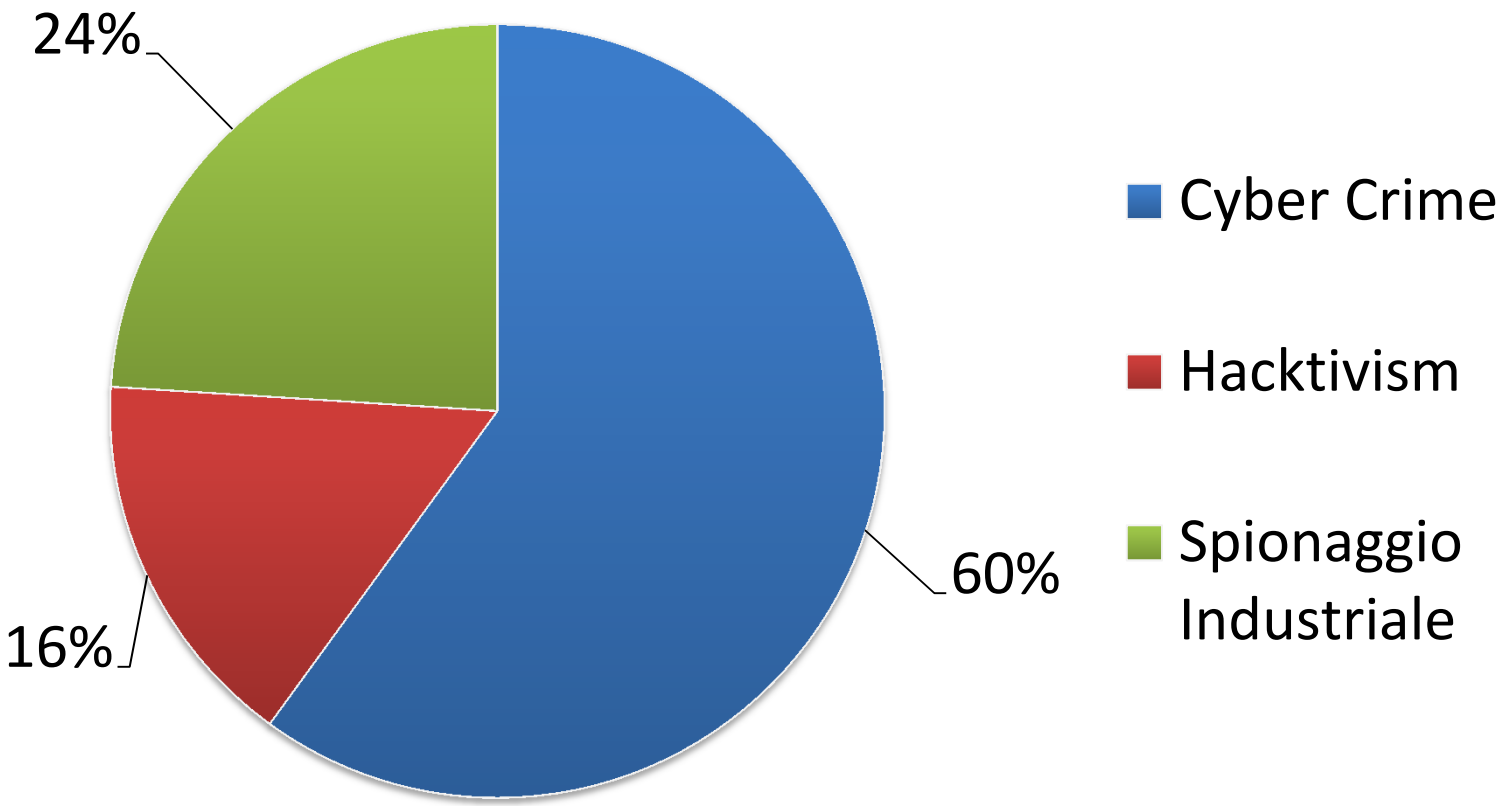
Dimensione europea del cyber crime

- Costo del cyber crime 750 miliardi di euro l'anno (dati Interpol)
- 150 mila posti di lavoro persi in Europa
- 89% degli europei è preoccupato della sicurezza delle proprie informazioni personali on-line
- 74% considera aumentato il rischio di essere vittima del cyber crime
- 10% degli europei è certo di aver subito frodi on-line
- 6% di essere stato vittima di furto di identità (dati Eurobarometro)
- Esempi:
  - UK, 2013, 93% delle grandi aziende e 76% delle PMI denuncia un attacco informatico
    - Costi tra 110 mila a 250 mila sterline per le grandi aziende e tra 15 mila e 30 mila sterline per le PMI (dati FBS Federal)
  - Germania, 96% delle aziende ha subito incidenti informatici (dati BMBF Ministero dell'Educazione e Ricerca)

Dimensione italiana del cyber crime

- 875 milioni di dollari all'anno di perdite per danni diretti
- + danni di immagine e reputazionali, costi di *recovery* e perdita di business, 8,5 miliardi (0,6% del PIL) (dati McAfee)
- 9 miliardi di dollari spesi per la perdita di dati sensibili
- + perdite da interruzioni operative dei sistemi 14,1 miliardi di dollari (dati Emc)

Motivazione degli attaccanti - Fastweb



Tipi di minacce

- **Frodi**
- **Furto di dati sensibili e di proprietà intellettuale**
- **Estorsione**
- Attacchi dimostrativi
- Furto d’identità
- Spionaggio
- Sabotaggio

Tipi di attacco

- **Phishing**
- **Spear phishing**
- Spam
- Pharming
- Malware
- Botnet
- Defacement
- DoS
- Social engineering
- Hacking

Tipi di attaccanti

- **Gruppi criminali organizzati**
- **Insider**
- Spie industriali
- Hacktivist
- Wannabe lamer, script kiddie

Rischi

- Trend degli ultimi anni: aumento attacchi verso PMI
  - Perché meno difese
  - Tramite per attacchi ad aziende più grandi
- Perdita del know-how
- Rischio per il “Made in Italy”
- Perdite economiche
- Danni d’immagine e reputazionali
- Danni ai sistemi aziendali che impattano sulla produzione

Vulnerabilità

- Vulnerabilità tecniche
  - Bug di programmi e sistemi
  - Mancato aggiornamento o errate configurazioni di sistemi di protezione (antivirus, firewall) e sistemi operativi
  - Protezione connessioni (wireless e reti)

- Vulnerabilità umane
  - Uso del mobile
  - Uso dei social network
  - Social engineering

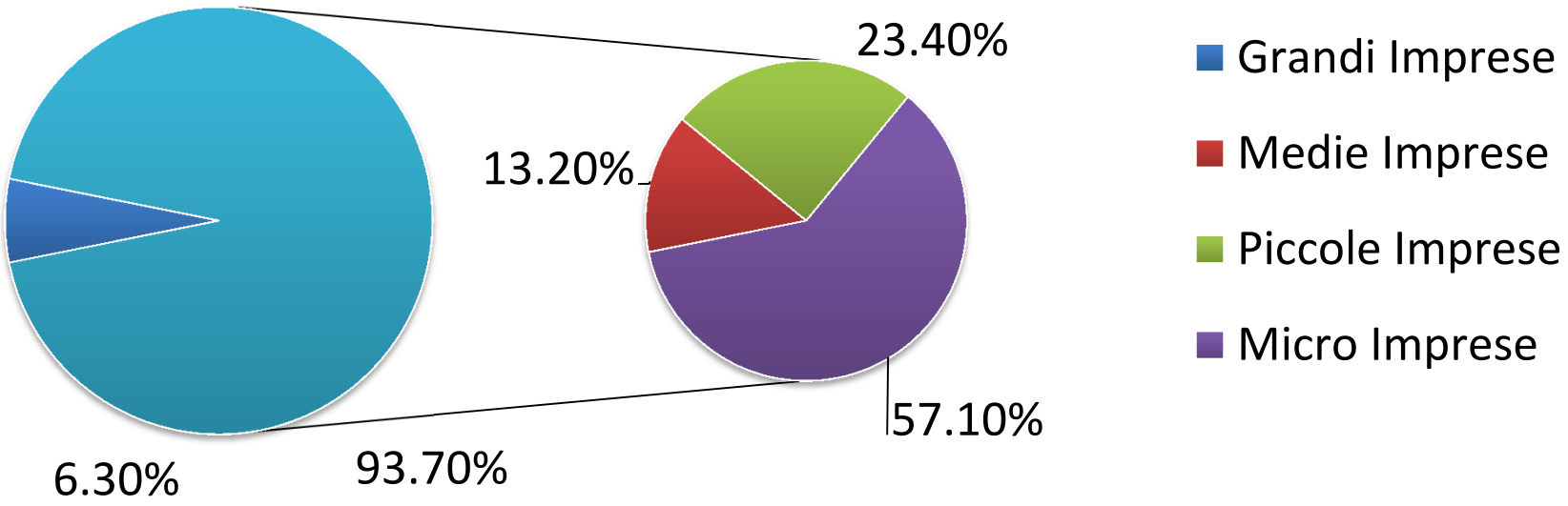
Interviste presso le Procure

- Gestione distrettuale casi cyber crime
- Maggioranza dei casi phishing / spear phishing
- Criminalità a forte carattere transnazionale
- Difficoltà nella collaborazione internazionale
- Tasso esercizio azione penale molto basso
- In media l’80% dei casi vengono archiviati

Caso studio

- Reato di frode informatica a danno di una PMI del Piemonte
- Subisce violazione dei database
- Inviate mail a clienti con fatture originali e segnalazione di cambio IBAN
- Tre aziende clienti pagano erroneamente fatture per un totale di 200 mila dollari
- Rogatoria internazionale alla Georgia
- Documenti degli intestatari dei conti falsi

Focus Provincia di Lucca



- 38.584 imprese attive sul territorio
- Esportazioni il doppio delle importazioni, maggiore settore quello cartario
- Settore cartario, + di 100 aziende con un fatturato di 3,5 miliardi di euro
- 6.500 dipendenti, + indotto 14.000
- 80% della produzione nazionale di carta tissue

Interviste a rappresentanti delle forze dell'ordine

- Escalation di phishing e spear phishing
- Aumentano le denunce
- Compartimento della Polizia Postale di Firenze, 2014:
  - 711 denunce ricevute per truffa
  - 231 per accesso abusivo
  - 92 per frode informatica
- Reati per frode, la metà di natura informatica
- + 2.600 procedimenti contro ignoti per reati di frode informatica
- Cifra sottratta dai cyber criminali commisurata alla parte offesa
- Differenziazione della tipologia di attaccante per reati
- Consapevolezza e preparazione delle PMI ancora molto basse

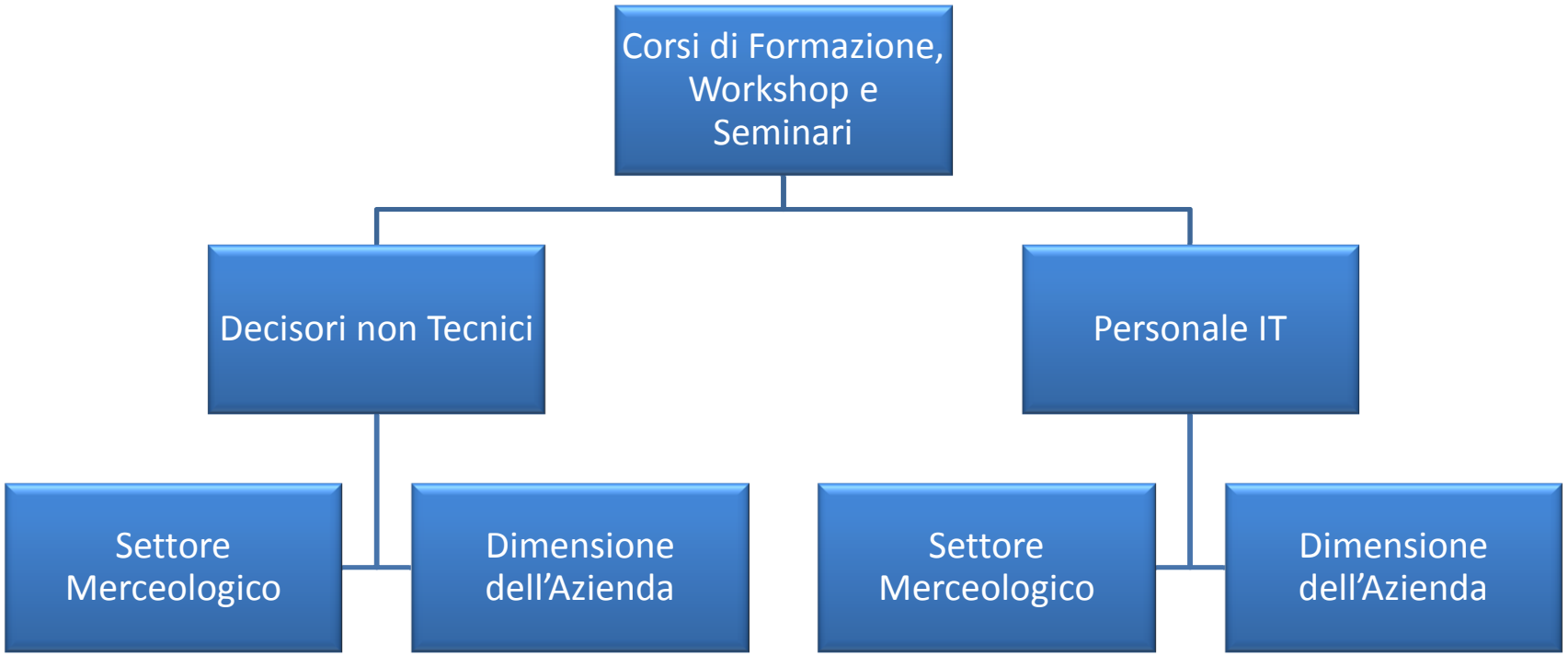
Interviste presso le aziende

- Aziende settore marmo, cartario e IT
- Concetti chiave:
  - Esigenza di investire in formazione
  - Vulnerabilità umane più pericolose di quelle tecniche
  - Necessità di un aumento di consapevolezza per i Decisori non Tecnici
  - Totale mancanza di condivisione e collaborazione tra le aziende
  - Sicurezza vista molto spesso come un costo e non come un valore
  - PMI italiane spesso vittime del furto della loro eccellenza da insider più che da hacker esterni

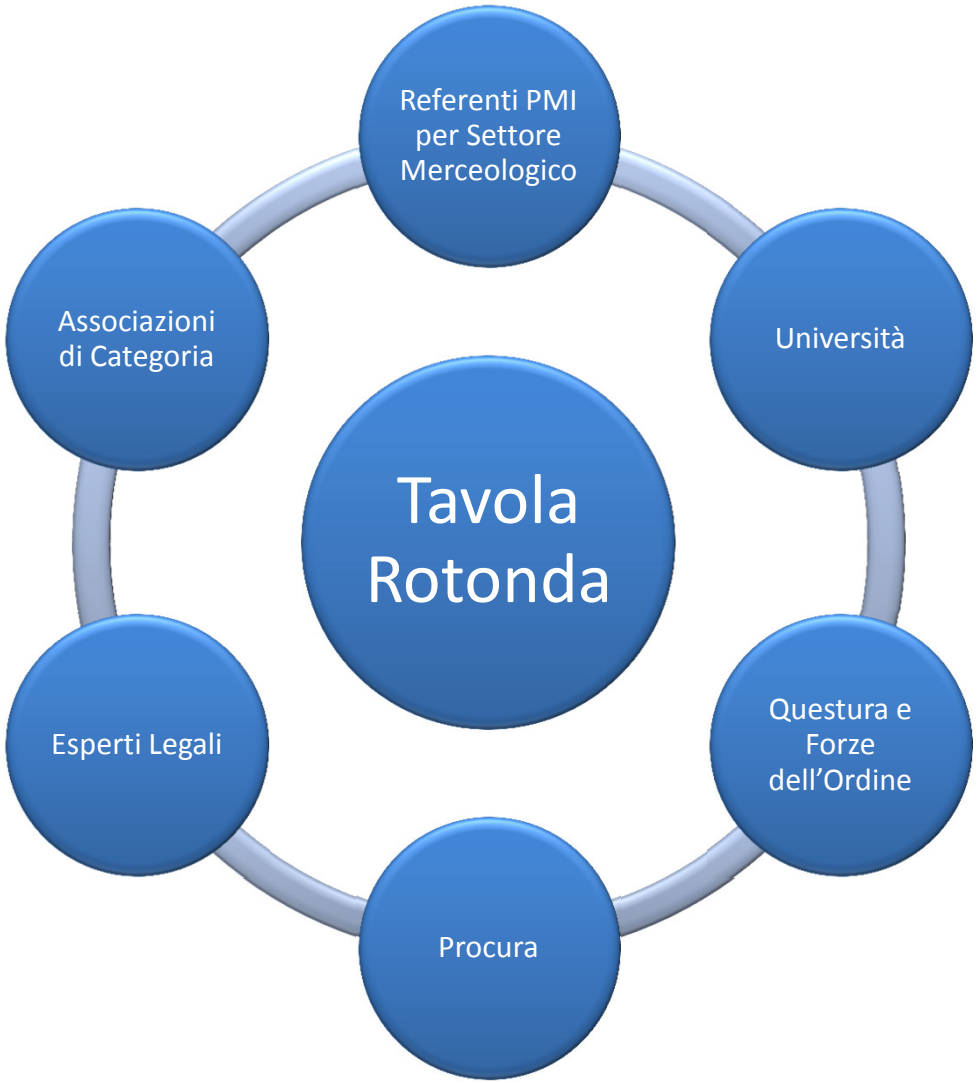
Conclusioni

- Diminuisce il confine tra i vari tipi di cyber attaccanti
- Aumentano i rapporti tra la criminalità informatica e gruppi criminali organizzati
- Percezione del rischio tra sicurezza fisica e informatica viziata dall'esperienza
- Fattore umano come elemento determinate
- Sicurezza informatica come opportunità per le PMI

Proposta di Corsi di Formazione Differenziati



Proposta di Istituzione di Tavole Rotonde Periodiche



Si ringrazia per la preziosa collaborazione

- Procura della Repubblica di Torino
- Procura della Repubblica di Firenze
- Polizia Postale e delle Telecomunicazioni di Firenze
- Polizia di Stato presso la Procura della Repubblica
- Giorgini Maggi s.r.l.
- Industria cartaria Pieretti S.p.A
- Lucart grop S.p.A
- Lucense S.C.p.A
- Tagetik s.r.l.
- Assindustria Lucca
- ABI Lab
- Consorzio Bancomat
- IBM
- Osservatorio per le Piccole e Medie Imprese
- Intesa Sanpaolo

Grazie per l'attenzione

Flavia Zappa – flavia.zappa@libero.it