Kroll | A Division of DUFF & PHELPS

La cyber (in)sicurezza nella *digital economy*: un problema aziendale non un problema tecnico

Marianna Vintiadis

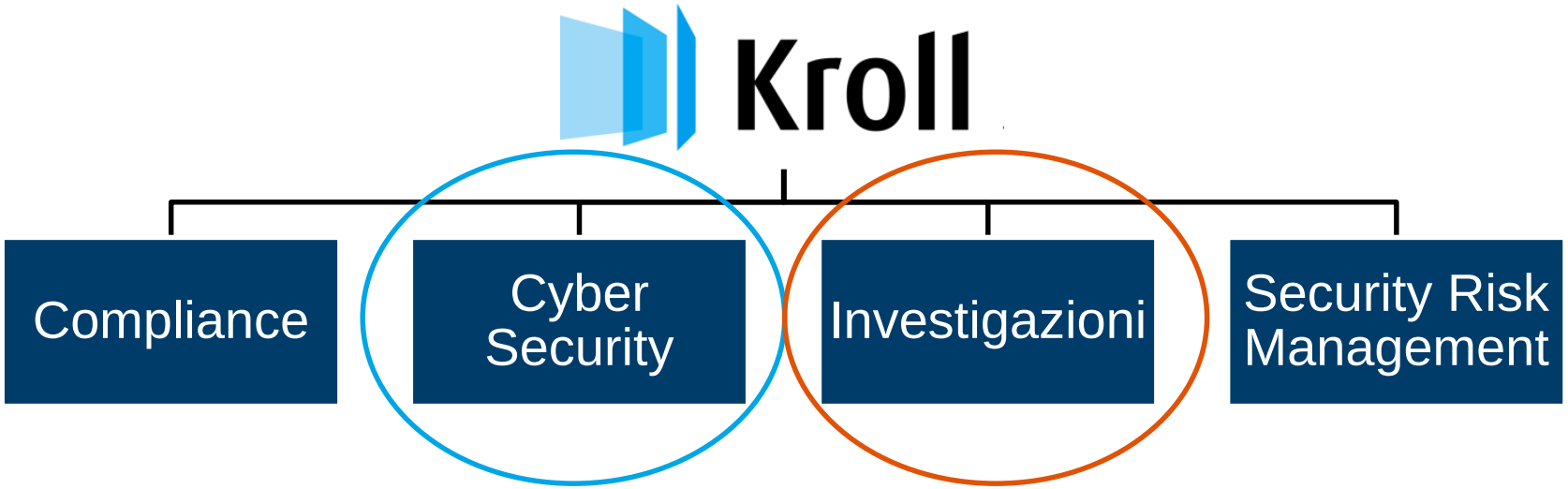
ACFE, Milano 12 dicembre 2018

Una considerazione…

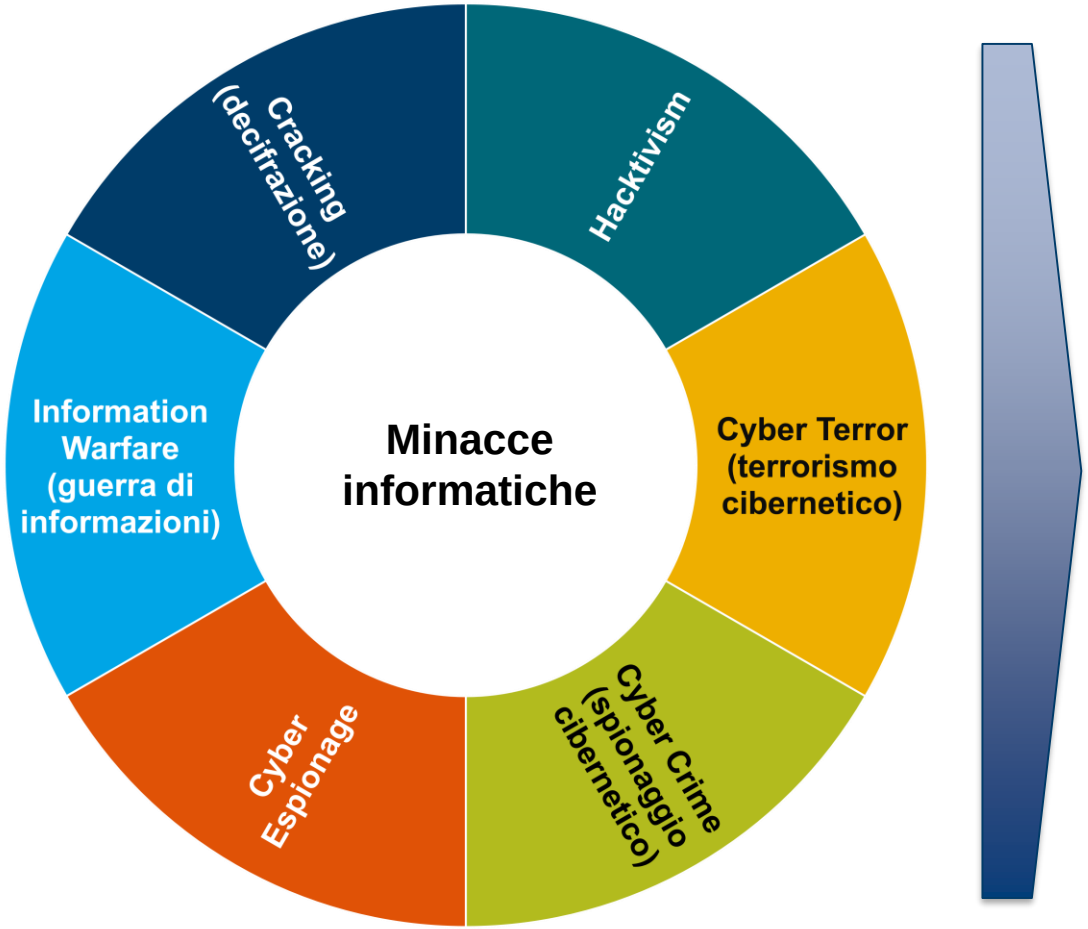
Image from Google

(Q incontra James Bond – Skyfall 2012)

Chi siamo



Tipologie di crimini e prime misure di sicurezza



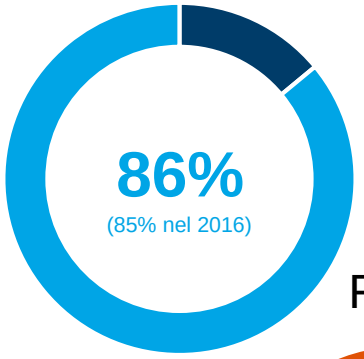
Tipologie di crimini informatici

- Phishing
- Ransomware
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Man in the middle
- Attacchi Malware
- Spyware
- Spam
- Truffe legate ai rinnovi dei domini
- Furti di identità
- Furti di proprietà intellettuale / informazioni copiate
- Wireless Local Area Networks (WLAN) senza sicurezza
- Frode dell'AD (CEO)/ Business Email Compromise (BEC)
- Furto di laptop o altro hardware … etc. etc. etc.

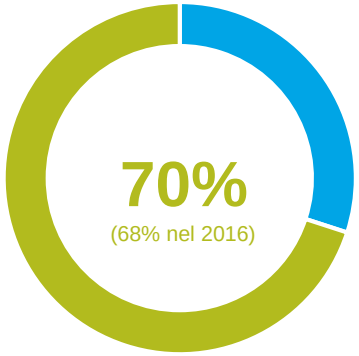
Qualche numero

Dati consolidati

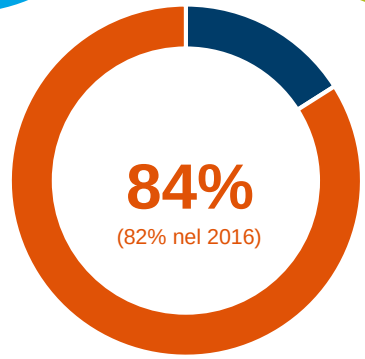
Incidenti informatici



Sicurezza



Frodi

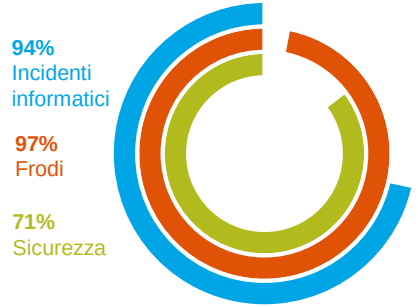


Global Fraud & Risk Report 2017/18

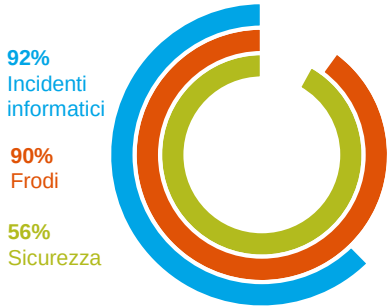
Dati per Paese

Stati Uniti

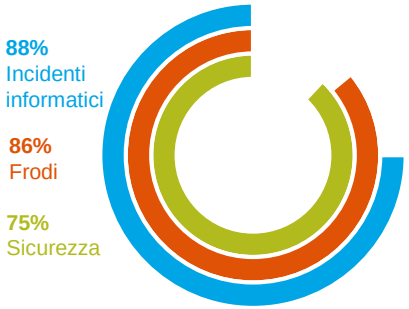
Gran Bretagna



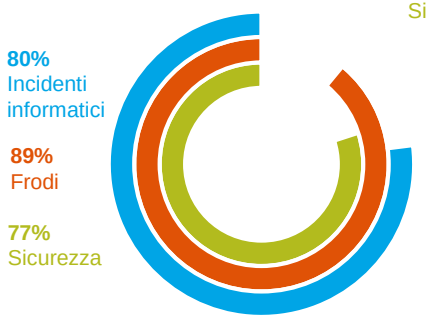
Italia



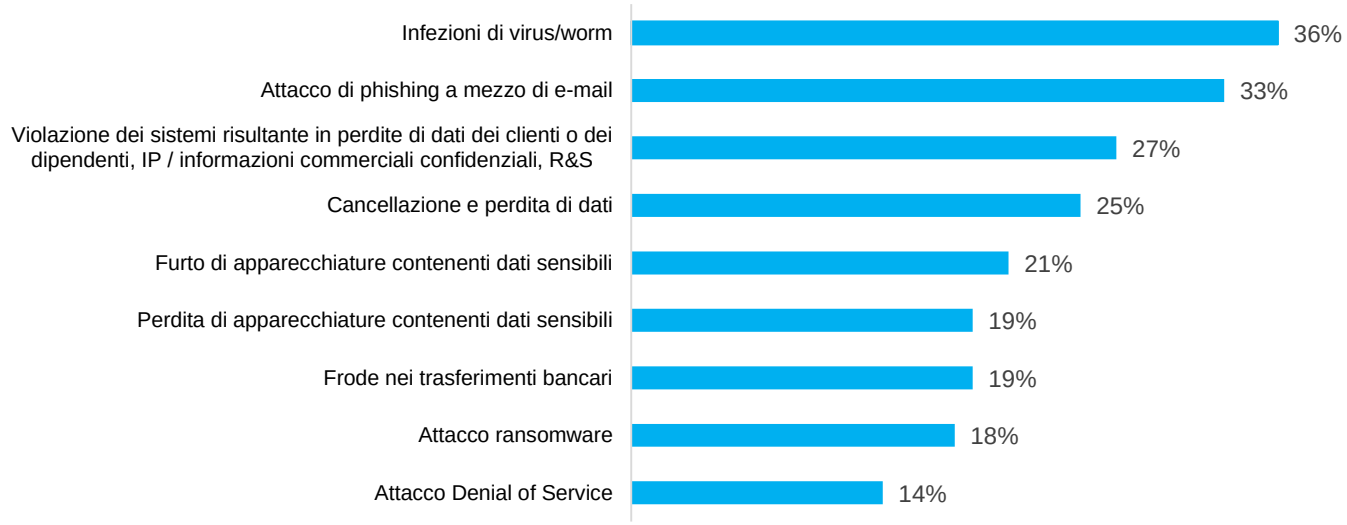
Cina



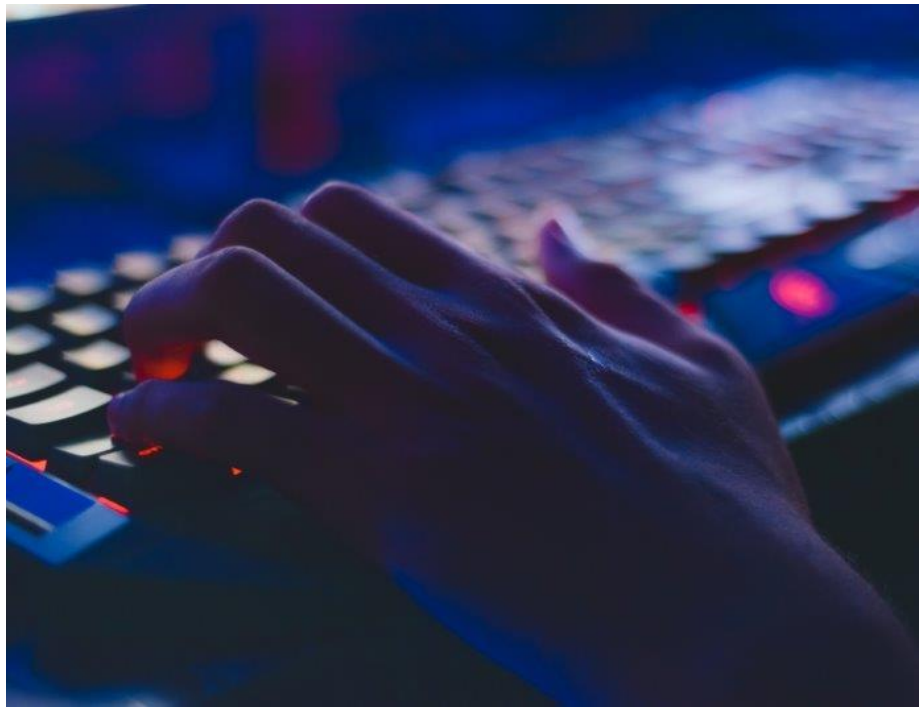
Russia



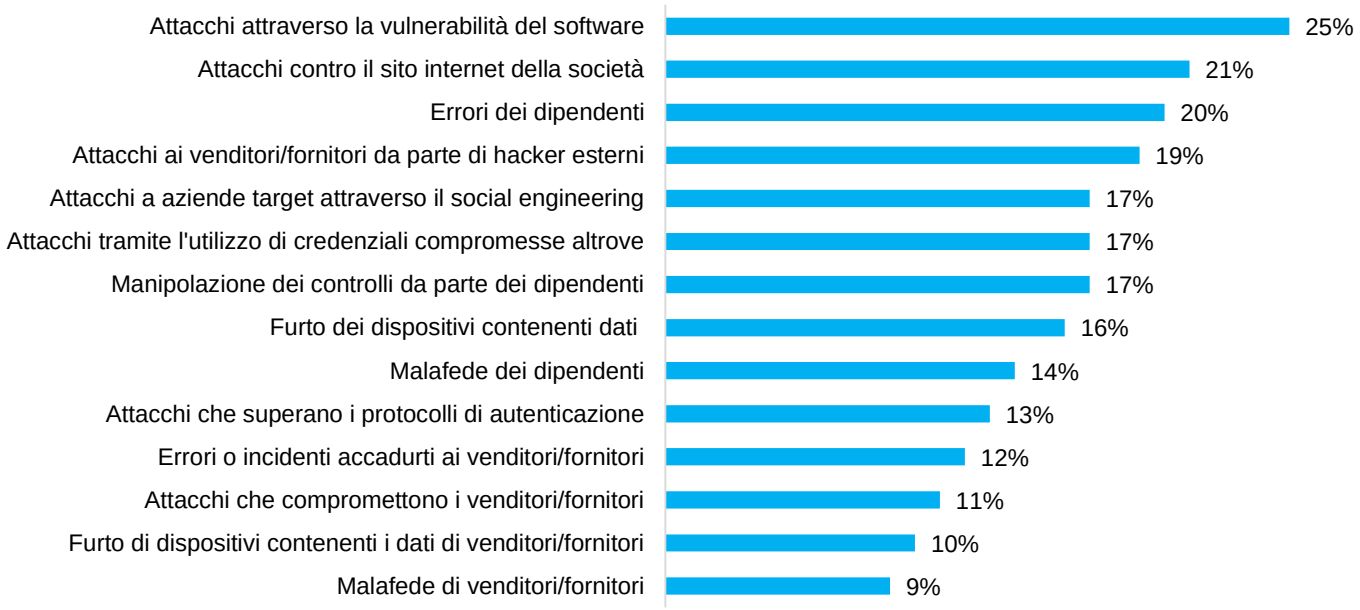
Tipologia di attacchi informatici



Global Fraud & Risk Report 2017/18

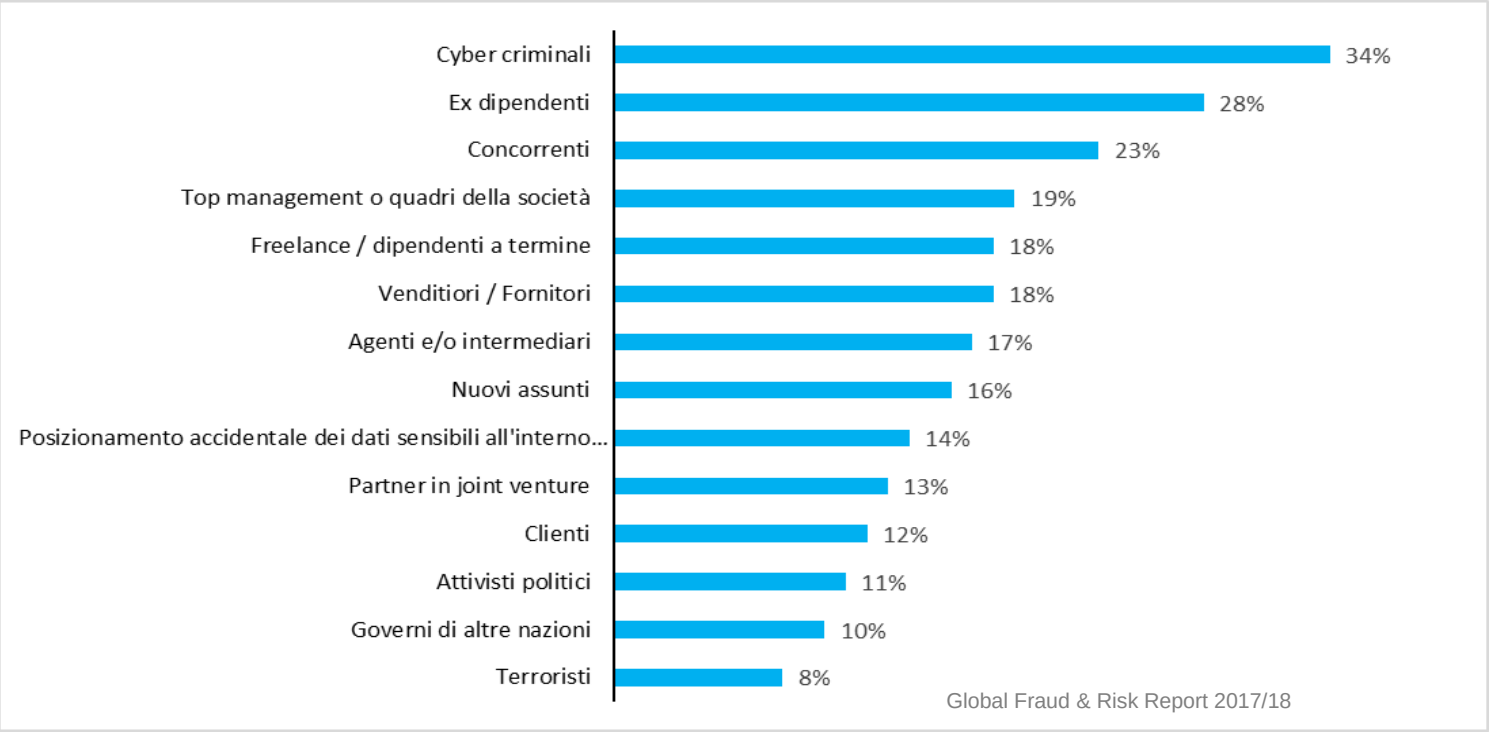


Come avvengono gli attacchi informatici



Global Fraud & Risk Report 2017/18

Gli autori degli attacchi



> 20%

- Cyber criminali
- Ex dipendenti
- Concorrenti

15% - 20%

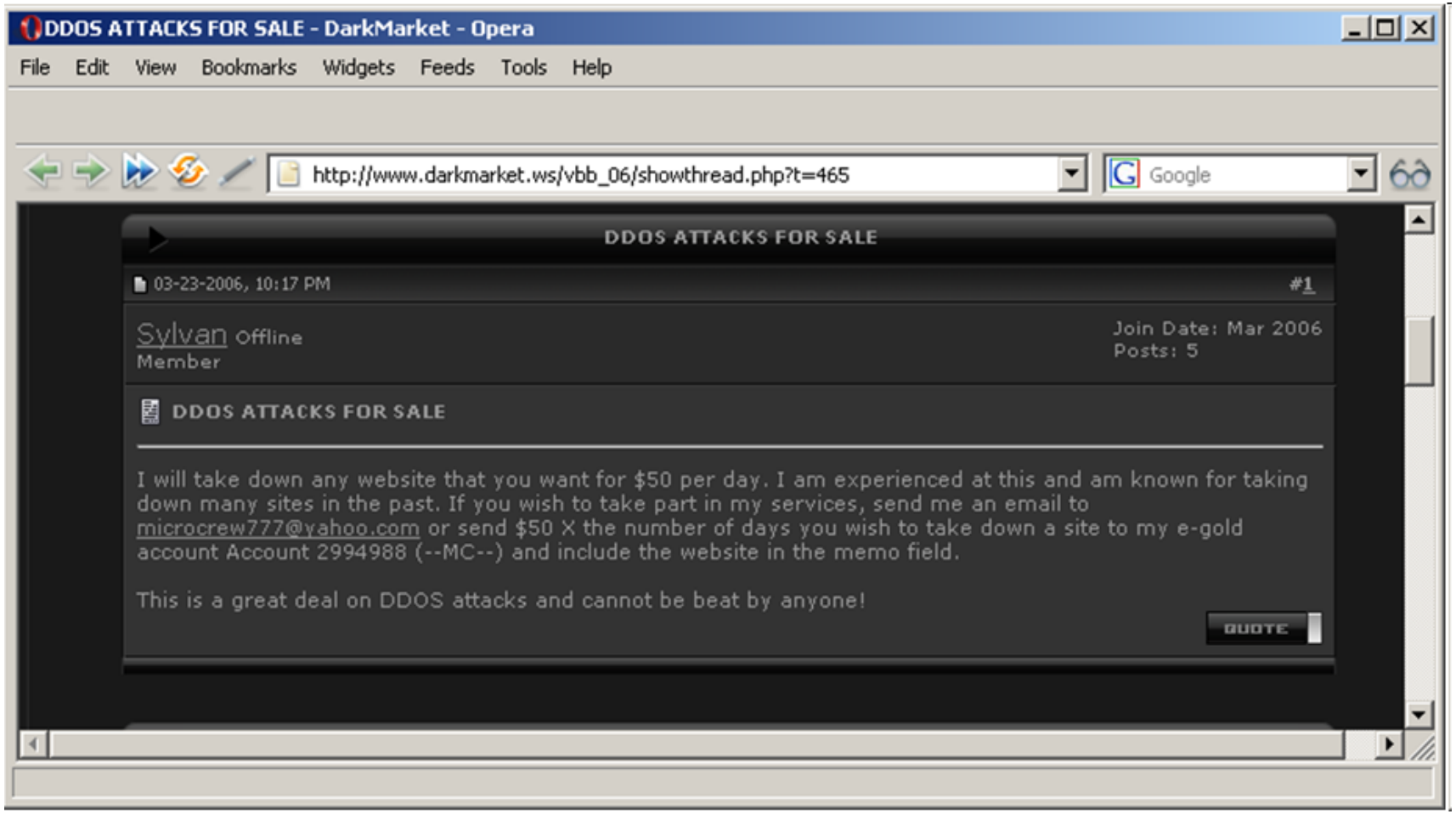
- Top management o quadri della società
- Freelance / dipendenti a termine
- Venditori / Fornitori
- Agenti e/o intermediari
- Nuovi assunti

Cause dell'aumento del crimine informatico

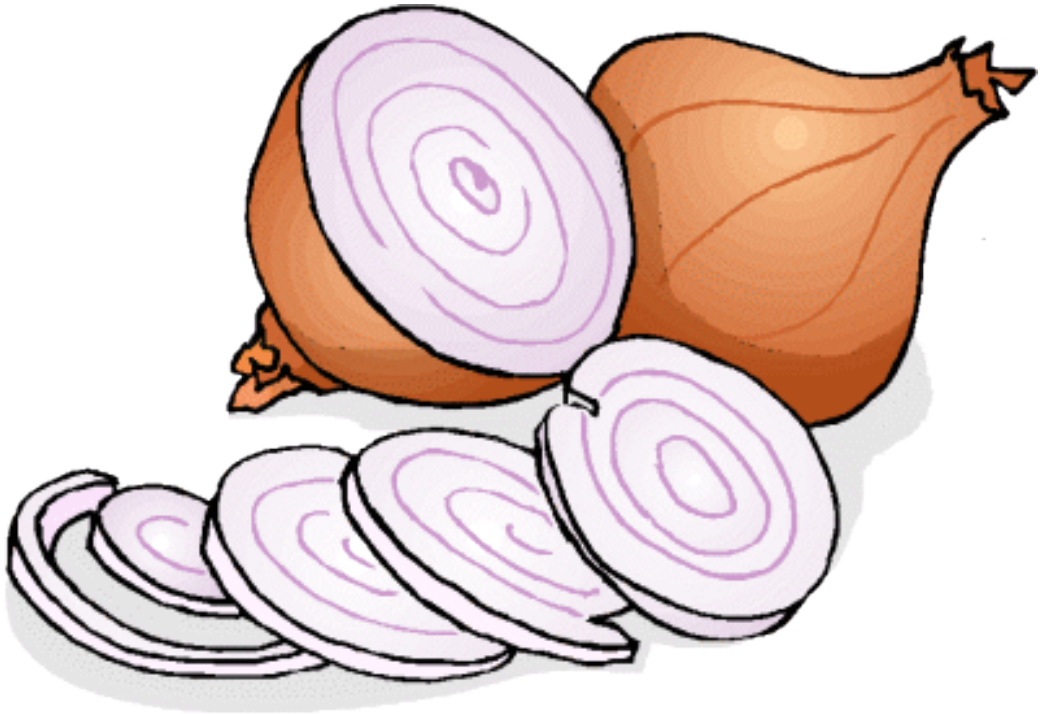
- Grandi vantaggi rispetto al crimine "tradizionale"
- Meno persone coinvolte
  - Meno problemi organizzativi
  - Più difficile infiltrare le organizzazioni criminali
  - Meno informazioni rivelate agli organi di controllo
- Costi organizzativi bassi
- Gli attacchi possono facilmente essere commessi in remoto anche da un paese terzo

- Chance ridotte di essere rintracciati
- Pene previste basse
- Denaro sottratto è in forma elettronica quindi più facile da spostare
- Alto livello di impunità
- Molto facili da perpetrare (off the shelf software, hacker che offrono le loro competenze sul mercato)

Attacchi in vendita

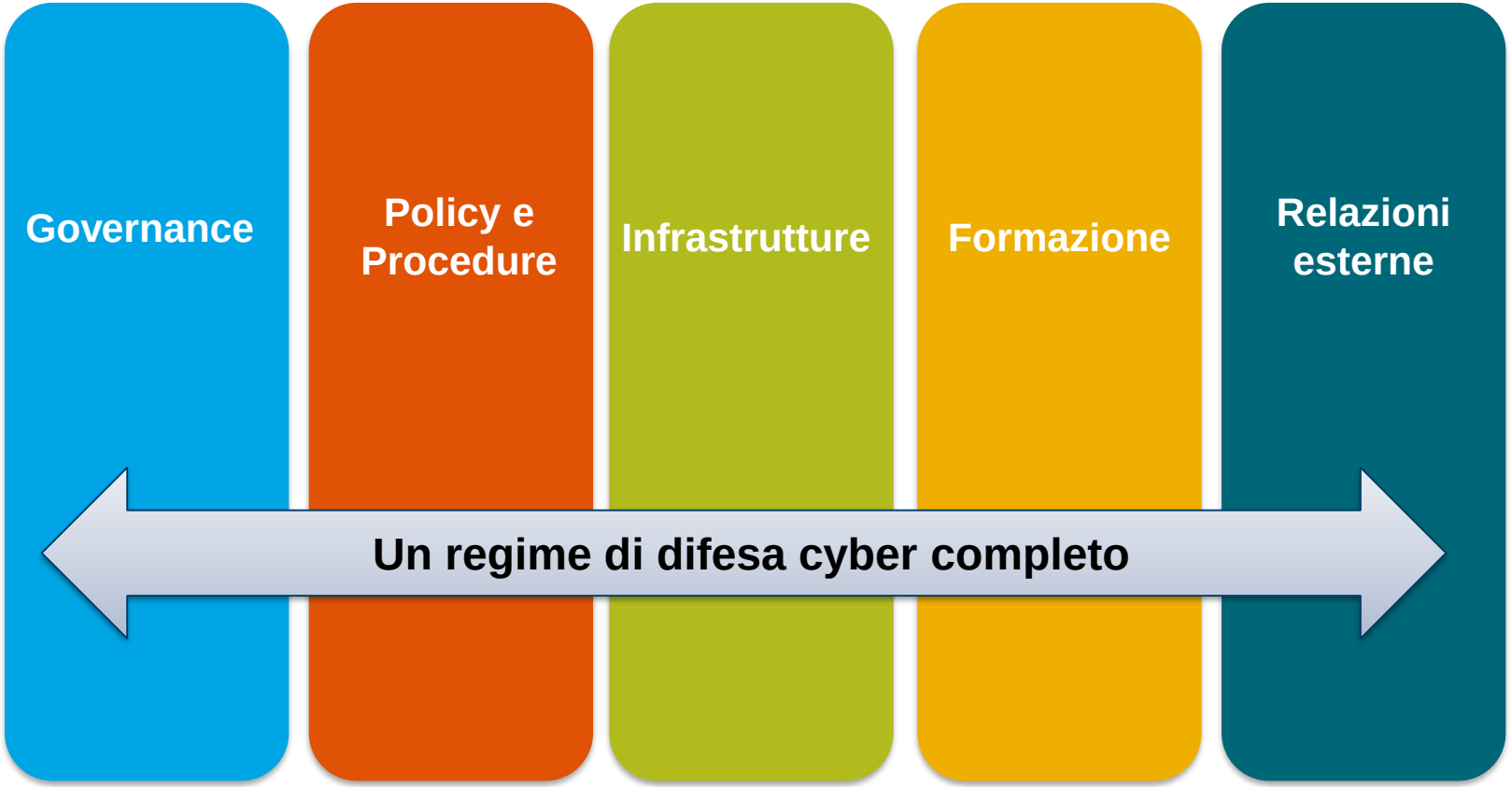


Il principio fondamentale della (cyber) sicurezza



Come affrontare il problema

La cyber security non è un problema solamente tecnico ma è un problema aziendale.



Lo scenario in Italia

- Poca attenzione da parte della stampa
- Gli utenti e le aziende sono generalmente poco preparati
- Gli errori degli utenti persistono
  - Password troppo semplici e cambiate poco frequentemente
  - Abitudine a scrivere le password
  - Inoltro di documenti di lavoro sull'account personale per lavorare da casa
  - Documenti cartacei non distrutti
- Errori di IT *policy*
  - Esposti spesso a causa di mancati aggiornamenti software (gratuiti)
  - Dischi di computer dismessi che non vengono ripuliti
  - Dischi e chiavette USB raramente criptati

Cosa vediamo in Italia

- Conoscenza specifica assente nei CdA
- Le decisioni di manager e amministratori spesso portano agli errori
  - Analisi dei rischi tipicamente assente
  - Poca formazione
  - Poca collaborazione tra divisioni interne per creare regolamenti comprensibili e buone abitudini
  - Poco budget allocato (costo perdita sottovalutato)
  - Scarsa attitudine delle imprese a fare *due diligence* sui sistemi di terze parti
  - Poche imprese sono assicurate
- Concezione inadeguata della formazione

Marianna Vintiadis

Managing Director & Head of Southern Europe

Piazza della Repubblica 24
20124 Milan, Italy

mvintiadis@kroll.com
Phone: +39 02 8699 8088

Marianna Vintiadis è Managing Director e responsabile Kroll per il Sud Europa. Dalla sede di Milano dirige l'attività di Kroll in Italia, nella penisola Iberica, in Austria, in Grecia e nei Balcani. Nell'area europea ha seguito in prima persona alcuni tra i progetti di *business intelligence* più delicati e di alto profilo dell'azienda, spaziando all'interno di molteplici giurisdizioni e settori.

Marianna, insieme al suo *team*, ha maturato competenze in molte aree tra cui la valutazione dei rischi in operazioni di M&A; la gestione di crediti in sofferenza (NPL); *intelligence* strategica; indagini volte a portare alla luce attività economiche in violazione a sanzioni internazionali e attività della criminalità organizzata; supporto in contenziosi; consulenza per ridurre la propria esposizione verso terzi e a tutela della reputazione; fughe di notizie, riciclaggio, corruzione e frodi interne; contabilità forense e sicurezza. In questi ambiti Marianna si è trovata a lavorare con le più dinamiche aziende operanti sul territorio nazionale, le istituzioni finanziarie e numerosi studi legali.

Le specifiche aree di competenza di Marianna includono il settore marittimo, il settore energetico e quello bancario. È stata inoltre tra i primi professionisti in Sud Europa a supportare i clienti in tema di *cyber security*, quindi, nella prevenzione e gestione di crisi in caso di violazione dei dati.

Prima di entrare a far parte di Kroll, Marianna ha lavorato nella divisione Marine di Navale Assicurazioni. Precedentemente, per otto anni, ha svolto attività di ricerca, insegnato economia e lavorato sullo sviluppo di nuove tecnologie presso l'Università di Cambridge, sua *alma mater*.