# LA TECNOLOGIA A SERVIZIO DELLA TESORERIA: OPPORTUNITÀ DA COGLIERE, RISCHI DA GESTIRE

FABIO PUGINI
22/09/2017

BNL
GRUPPO BNP PARIBAS

La banca per un mondo che cambia

# In principio era il caos

## Come eravamo prima dell'Euro e della SEPA:

- Standard diversi nei vari paesi europei
- Presenza di molteplici divise
- Tempi e costi transazioni differenziati e poco comparabili

# Dove siamo ora

## Un unico mercato dei pagamenti

**34 Paesi**

**500 milioni cittadini**

**20 milioni imprese**

**Standardizzazione, omogeneità di qualità e livello di servizio, comparabilità, concorrenza**

# La nuova sfida tecnologica

**Abbattimento dei tempi di esecuzione**
*(SEPA Instant Payment)*

**Efficientamento dei processi**
*(Blockchain)*

**Tracciabilità E2E dei pagamenti internazionali**
*(SWIFT GPI)*

**Incremento competizione con l'ingresso di nuovi player di mercato**
*(PSD2)*

**Identità Digitale**
*(SPID)*

# Le implicazioni di un mondo "veloce"

**Più rapidità e semplicità nella esecuzione transazioni implica una riduzione dei tempi di risposta.**
**Non possiamo "reagire", dobbiamo "prevenire" i rischi:**

- Danni materiali (sottrazione fondi, interruzione ciclo produttivo)
- Danni immateriali (reputazionale)
- Perdita o danneggiamento di documenti
- Violazione diritti proprietà intellettuale
- Furto dati sensibili e coperti da privacy

# Siamo preparati per affrontare la sfida?

Cybercrime
Hacktivism
Sabotage
Espionage
DDOS
Brute Force
Cyber warfare
Botnet
Booter Stresser
Malware
Trojan Horse
Keylogger
Phishing
Spyware
Rootkit
Social Engineering
Pharming
Malvertising
Vishing
Man in the Middle

# Ciascuno deve fare la sua parte

## Cosa fa l'Information Technology

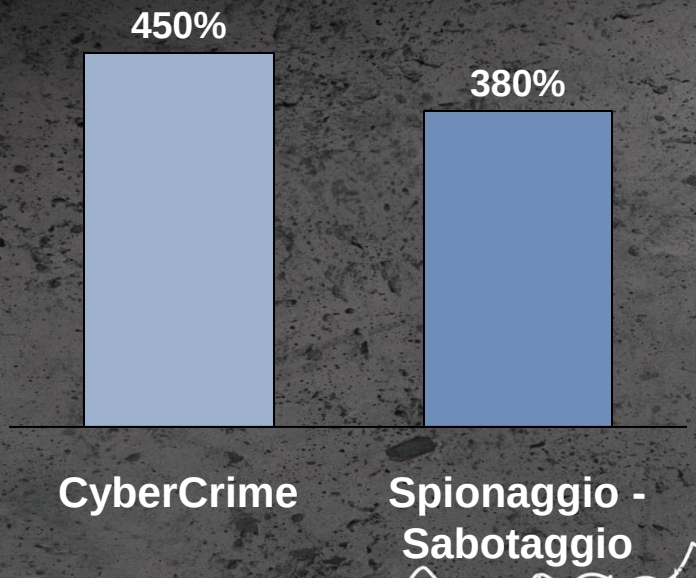
Antivirus
Firewalling
Motori antifrode
Analisi semantica
Crittografia
Monitoraggio attivo
Networking/community con altre aziende
Asset Recovery Plan
Simulazione "Cyber Attack"

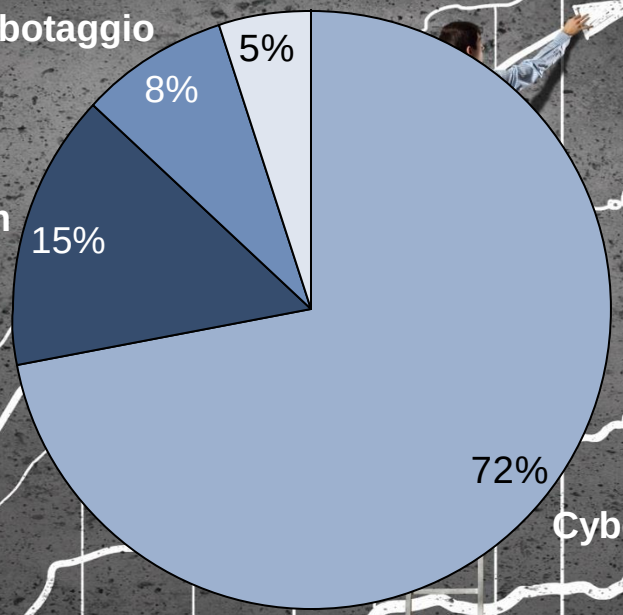
## Cosa possiamo fare noi

Processi strutturati + Consapevolezza
Procedure call-back
Anagrafiche protette
Separazione ruoli e competenze
Uso responsabile social
Condivisione delle informazioni

"Una catena è forte quanto il suo anello più debole"

# La diffusione del "Cyber Attack"




**Trend attacchi globali 2011-2016**
*(Attacchi gravi di pubblico dominio)*

**Principali tipologie "Cyber Attack"**

# I rischi della rivoluzione digitale

## Principali forme di "Cyber Attack"

**Attacco mediante virus informatico**
*(Malware, ramsonware, etc.)*

**Attacco mediante tecniche di Social Engineering**

# I rischi della rivoluzione digitale

## Principali forme di "Cyber Attack"

**Attacco mediante virus informatico**

*(Malware, ramsonware, etc.)*

# Attacco mediante virus informatico: caratteristiche principali

**Attacchi massivi con mail generiche**
*(Phishing)*

**Ricezione di file apparentemente innocui**
*(Fogli di calcolo o di testo)*

**Richiesta di download da siti non conosciuti**

**Inviti ad intraprendere azioni da mittenti sconosciuti**

**Improvviso rallentamento del computer**

# Attacco mediante virus informatico: come difendersi

- Separare ambiente digitale professionale e personale
- Aggiornamento antivirus non appena richiesto
- Tenersi aggiornati sulle nuove tecniche di attacco
- Effettuare back-up e usare server aziendali
- Custodire opportunamente password e strumenti sicurezza (token)

# I rischi della rivoluzione digitale

## Principali forme di "Cyber Attack"

**Attacco mediante tecniche di Social Engineering**

# Social Engineering: caratteristiche principali

Contatti da mittenti noti abilmente contraffatti

Richieste urgenti e a ridosso di scadenze

Comunicazioni mirate con testi coerenti

Il destinatario viene invitato alla massima discrezione

Richieste atipiche di informazioni o documenti

# Social Engineering: come difendersi

- Verifica puntuale indirizzi mittenti e/o pagine web, anche se apparentemente noti e coerenti
- Diffidare da richieste invio duplicati di documenti, codici sicurezza, informazioni, etc.
- Definire processi aziendali robusti per gestione/creazione/modifica anagrafiche clienti/fornitori
- Usare canali bancari securizzati per i pagamenti
- Effettuare "double check" con colleghi e/o superiori in caso di richieste atipiche
- Diffidare dalle "urgenze brucianti" a ridosso di scadenze
- Cautela e riservatezza nell'uso dei social

# Le nuove tecnologie e la tesoreria: in sintesi

| PROS | CONS |
| --- | --- |
| ☑ Maggiore rapidità | ☒ Tempi di reazione più brevi |
| ☑ Strumenti più efficaci | ☒ Tecnologia malevola sofisticata |
| ☑ Maggiore capacità analisi | ☒ Patrimonio dati da securizzare |
| ☑ Nuovi player di mercato | ☒ Maggiori rischi di intrusione |

# Grazie