LA NOSTRA ESPERIENZA CON WANNACRY

L'EVOLUZIONE DELLA DATA PROTECTION

Elisa Garavaglia – Chief Security Officer

Responsabile Security e IT Governance, Quixa

CYBERTECH PRACTICAL WORKSHOP
"MALWARE E CYBER CRIME PREVENTION"

Milano, 26 ottobre 2017

quixa
Diretta. Personale. AXA.

Agenda

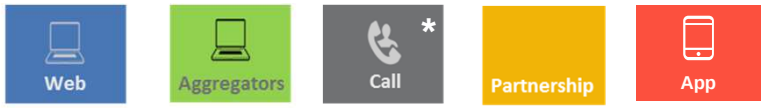
- Chi siamo e come siamo organizzati
- L'esperienza *WannaCry*
- Il programma di *Data Leakage Prevention*

quixa
Diretta. Personale. AXA.

Chi siamo

Un ottimo valore per un ottimo prezzo!

Il brand principale dedicato ai **clienti diretti**



**Only for prospects with a saved quotation*

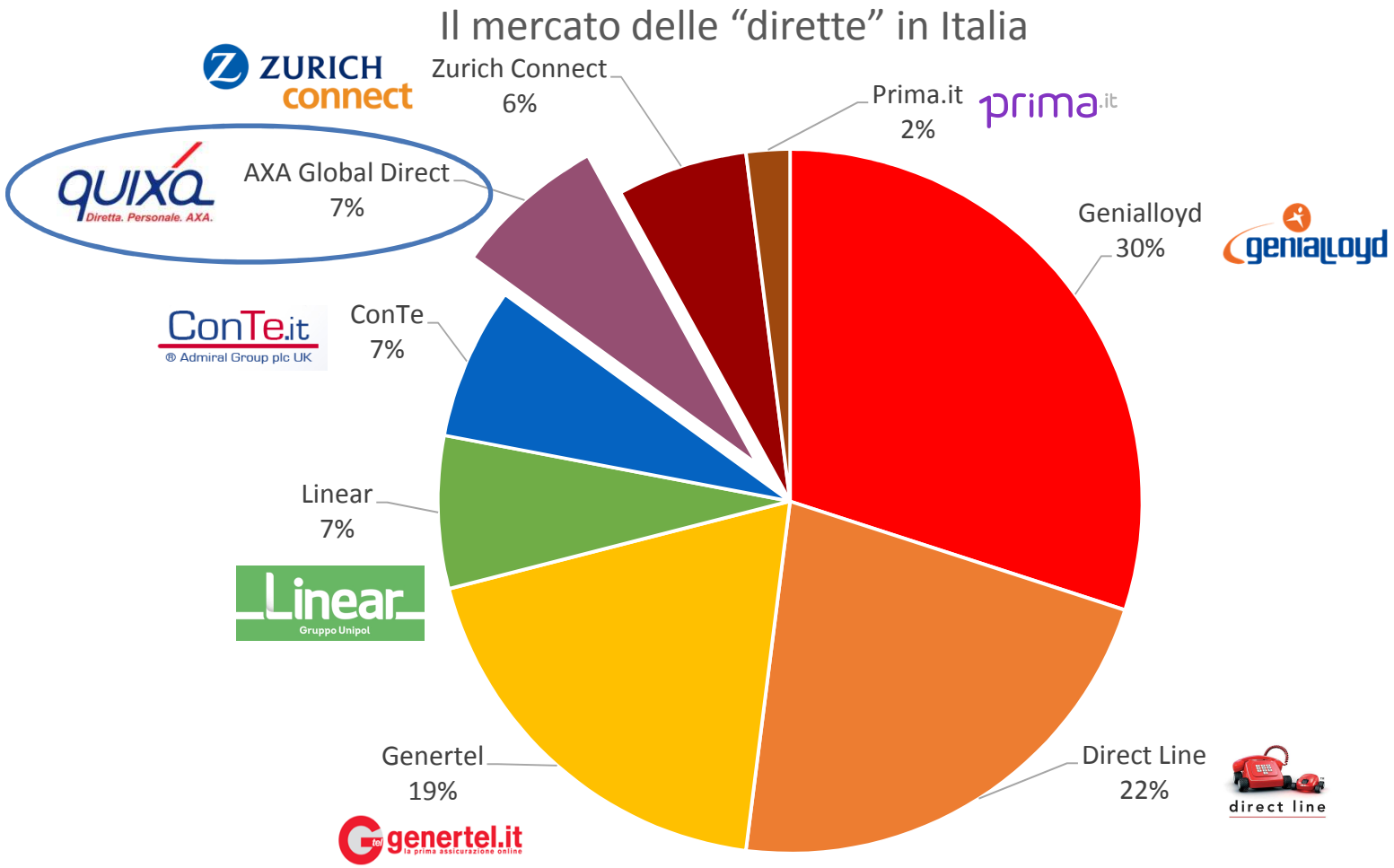
Un acquisto intelligente: risparmiare denaro senza perdere qualità!

Il secondo brand per competere negli aggregatori e spingere sui servizi *fai da te* (per i **clienti diretti più smart**)

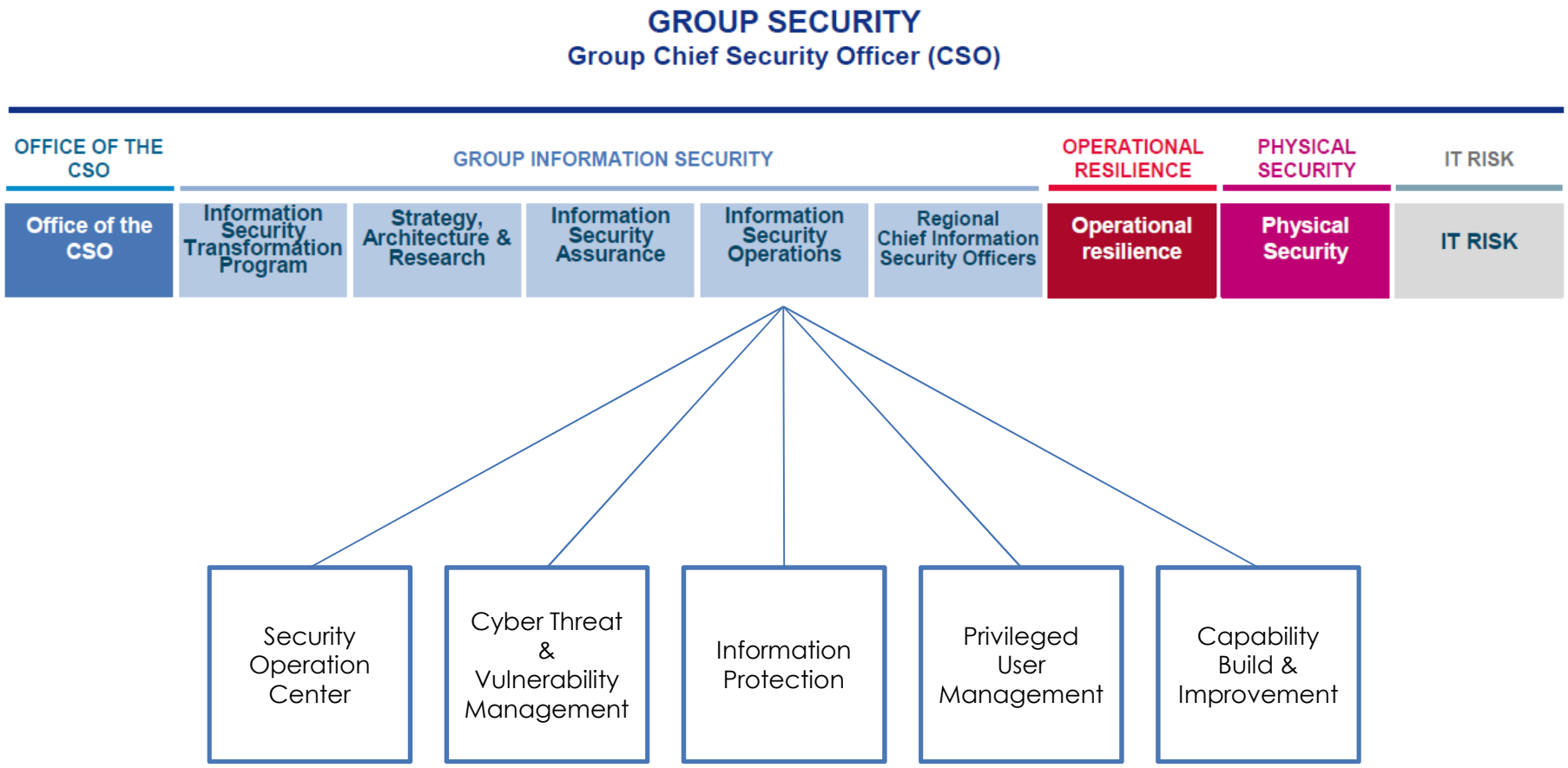
Il giusto mix tra un'assicurazione tradizionale e una diretta!

Vendite nelle agenzie (per i **clienti ibridi**)

Il mercato "diretto" in Italia



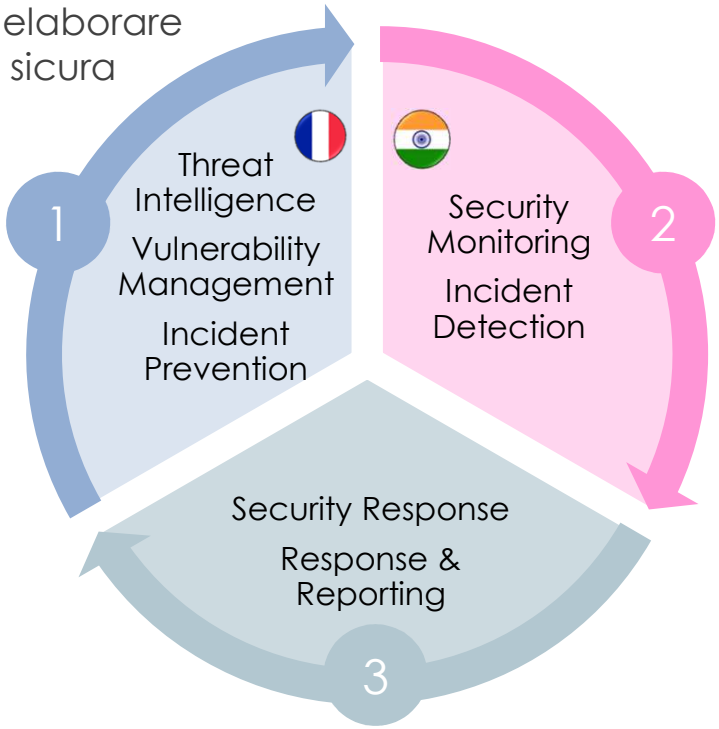
AXA Group Information Security - organizzazione



quixa
Diretta. Personale. AXA.

Il SOC di Gruppo

- Analisi di *threat intelligence*
- Report accurati e aggiornati sulle vulnerabilità
- Correlazione di rischi per elaborare una risposta adeguata e sicura



- 24/7 monitoraggio *real time*:
  - Firewalls & WAF
  - Access Management
  - Intrusion Prevention
  - DDOS
  - AV e Endpoint
  - Infrastruttura dei Server
  - Applicazioni
  - Middleware

- Correlazione di eventi mediante analisi accurate e *business-driven*
- Risposta agli incidenti rapida ed efficace grazie a un coordinamento centralizzato
- Analisi dettagliata e investigazioni forensi avanzate

L'Esperienza Wanna Cry

quixa
Diretta. Personale. AXA.

L'esperienza *WannaCry* 1/2

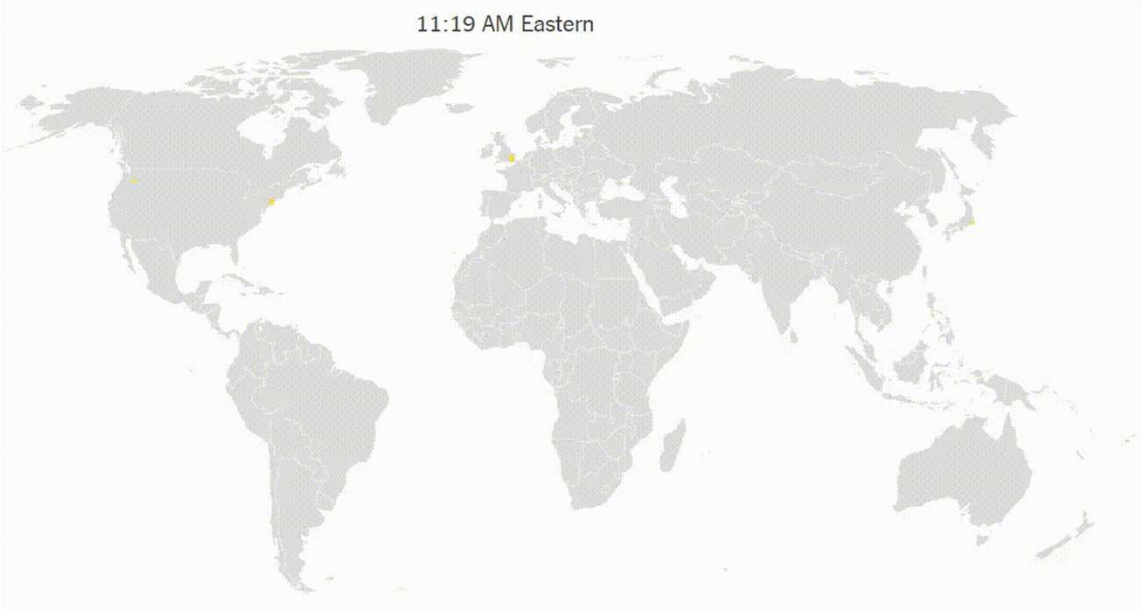
prima di maggio
2017

I gruppi di ricerca MalwareHunterTeam, GData e Malwarebytes hanno osservato il malware Trojan.Encoder.11432 (conosciuto anche come WannaCry) alcune settimane prima dell'attacco, ma senza rilevare una distribuzione tale da far pensare ad un attacco imminente.

12 maggio
2017

Inizia l'attacco

Venerdì 12 maggio è iniziato l'attacco, con i primi segnali registrati nella mattinata quando Telefonica (il noto ISP spagnolo) dirama un avviso in cui chiede raccomanda ai propri clienti di spegnere i computer per via di un attacco informatico in corso. In poche ore il *ransomware* inizia a mietere vittime in tutto il mondo.



quixa
Diretta. Personale. AXA.

L'esperienza *WannaCry* 2/2

13 maggio
2017

Parte l'*alert* dalla Security spagnola

Il CISO spagnolo ci contatta a proposito delle piattaforme condivise gestite in Spagna: vengono identificati i server che potrebbero essere stati impattati.

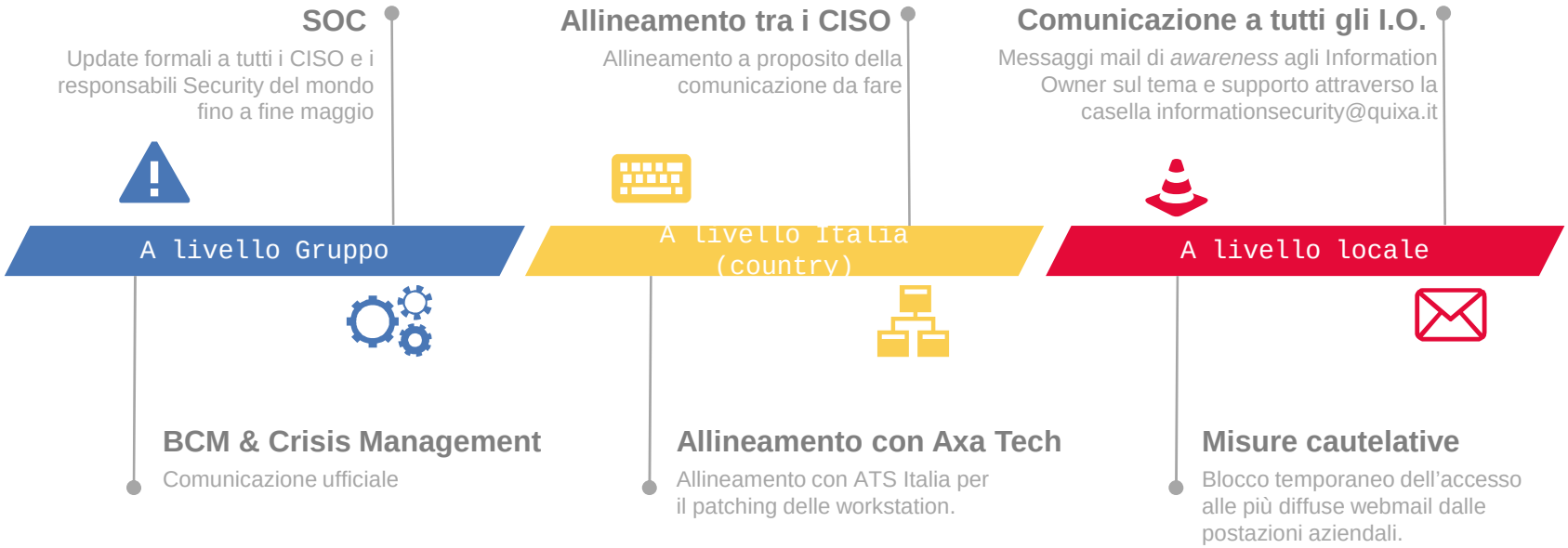
13-29 maggio
2017

Iniziano le azioni di contrasto

Avviene l'ingaggio da parte del Portogallo: comincia il patching dei server.
A livello locale partono varie attività sulla workstation e sulla NAS.

quixa
Diretta. Personale. AXA.

Cosa è stato fatto ai diversi livelli



quixa
Diretta. Personale. AXA.

Next step: data protection

Data Protection

Rischio globale

Il Data Leakage è stato identificato da AXA come “rischio globale”.

Il Group Security ha definito le line guida per il DLP, identificando vari obiettivi da raggiungere per mettere in sicurezza la compagnia.

Report trimestrale

Il piano prevede raccomandazioni a breve/medio termine che devono essere rendicontate al Gruppo con cadenza trimestrale.

Obiettivi suddivisi per livelli

A tutte le Compagnie è richiesto il raggiungimento di alcuni obiettivi BASE mentre gli obiettivi AVANZATI sono richiesti o meno in base all’esposizione della Compagnia al *Cyber Risk* (valutazione effettuata dal *Risk Committee*).

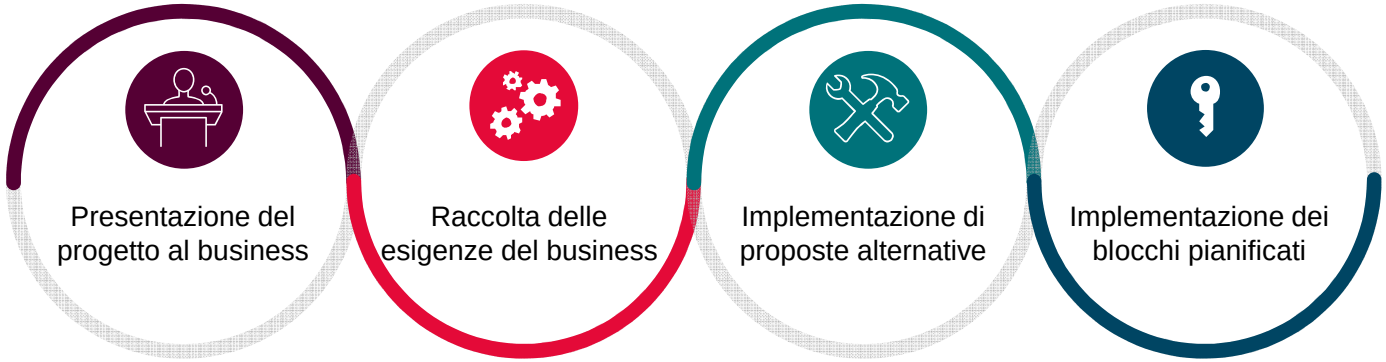
Identificazione di priorità

Tra le principali azioni identificate come fondamentali ci sono:

- Classificazione dei dati
- Identificazione dei *Crown Jewels*
- External network protection
- Email & Cloud protection
- Mobile device protection

Data Protection – Tactical Plan 2017

Obiettivo: non solo ridurre il rischio di sottrazione/diffusione illecita di informazioni aziendali ma anche proteggersi dalla diffusione di malware



01 PRESENTAZIONE PROGETTO
02 RACCOLTA DEROGHE
03 PROPOSTE ALTERNATIVE
04 BLOCCO PIANIFICATO

SITI WEB
FILE SHARING

WEBMAIL
GMAIL, YAHOO, …

HARDWARE
PORTE USB E SUPPORTI ESTERNI