KPMG

cutting through complexity

Cyber Security & PCI DSS

WORKSHOP : "TURISMO E SICUREZZA"

ASSOLOMBARDA – SALA FALK

Milano , 01 Aprile 2014

Relatore: Dott. Stefano Volante

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

Introduzione - Reati Informatici

- Un **‘crimine’** o **‘reato’ informatico** è un **fenomeno criminale** che ha come **caratteristica principale** '**abuso** della **tecnologia informatica** (**hardware** e **software)**.
- Con il termine di ‘**crimine informatico’** o **‘reato informatico’** si intende **ogni comportamento previsto** e **punito** dal **codice penale** o da leggi speciali **in cui** qualsiasi **strumento informatico** o telematico rappresenti un **elemento determinante** ai fini della **qualificazione** del fatto di **reato**.
- Si considera quindi un **‘crimine’ o ‘reato informatico’** sia la **frode** commessa **attraverso** il **computer** sia il **danneggiamento** del **sistema informatico**.

Introduzione - Reati Informatici

- I principali **articoli** contenuti nel **Codice Penale** italiano che trattano di **'reati informatici'** sono i seguenti:
  - ✓ Art. 615-ter – **Accesso abusivo** ad un **sistema informatico** o telematico;
  - ✓ Art. 615-quater – **Detenzione** e **diffusione abusiva** di **codici** di **accesso** ai sistemi informatici o telematici;
  - ✓ Art. 615-quinquies – **Diffusione** di **apparecchiature**, dispositivi o programmi informatici **diretti** a **danneggiare** o **interrompere** un sistema informativo o telematico;
  - ✓ Art. 617-quater – **Intercettazione**, **impedimento** o **interruzione** illecita di **comunicazioni** informatiche o telematiche;
  - ✓ Art. 617-quinquies – **Installazione** di **apparecchiature** atte ad **intercettare**, **impedire** od **interrompere** **comunicazioni** informatiche o telematiche.
  - ✓ Art. 635-bis – **Danneggiamento** di **informazioni**, **dati** e **programmi** informatici;
  - ✓ Art. 635-ter - **Danneggiamento** di **informazioni**, **dati** e **programmi** informatici utilizzati dallo **Stato** o da altro **ente pubblico** o comunque di pubblica utilità;
  - ✓ Art. 635-quater - **Danneggiamento** di **sistemi informatici** o telematici di **pubblica utilità**;
  - ✓ Art. 640-quinquies – **Frode informatica** del soggetto che presta servizi di **certificazione di firma elettronica**;
  - ✓ Art. 491-bis – **Falsità** di **documenti informatici**.

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

Cyber Security Overview - Soggetti che compiono attacchi informatici

Cyber Crime

Identifica **associazioni criminali** che compiono **attacchi** attraverso l'**abuso** di tecnologie informatiche *hardware* o *software*.

Tali attacchi vengono generalmente compiuti con lo scopo di trarre vantaggi a livello economico.

Hacktivism

Identifica **gruppi di *hacker*** che compiono attacchi mirati **verso governi** e **multinazionali** usando reti e computer.

Tali attacchi vengono generalmente compiuti con scopi attivisti e mirati alla libera comunicazione ed informazione elettronica.

Cyber War

Identifica **attacchi** volti all'alterazione e alla distruzione dell'informazione e **dei sistemi di comunicazioni "nemici".**

Tali attacchi utilizzano tecnologie elettroniche, informatiche e sistemi di telecomunicazione.

Cyber Espionage

Identifica l'**accesso abusivo** al patrimonio **informativo** di **proprietà altrui**.

Tali attacchi vengono generalmente compiuti con lo scopo di sottrarre informazioni riservate o comprometterne la disponibilità **per trarre vantaggi economici e di competitività nel mercato.**

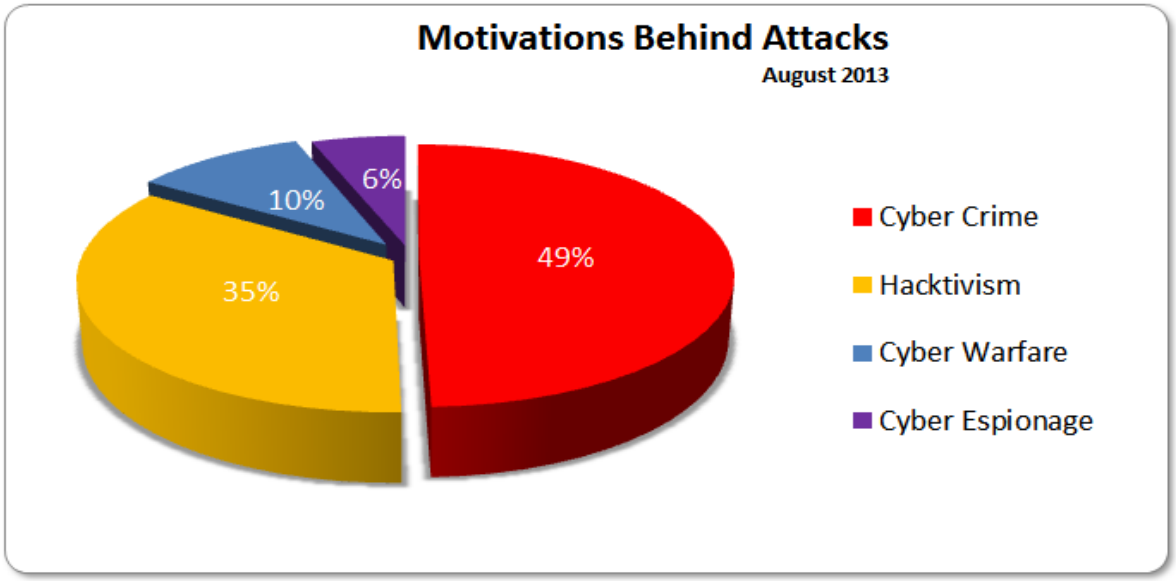
Cyber Security Overview – Soggetti che compiono attacchi informatici

- I **soggetti che compiono attacchi** con lo scopo di **distruggere**, compromettere, rendere non disponibili, o **rubare** informazioni possono essere:

1. **singoli hackers;**
2. **gruppi di persone** e/o **associazioni** aventi diversi obiettivi e scopi strategici;
3. **criminalità organizzata**.

- I principali **attacchi** informatici **provengono** da:

1. **Cyber Crime (49%)**
2. **Hacktivism (35%)**
3. **Cyber Warfare (10%)**
4. **Cyber Espionage (6%)**



Source: hackmageddon.com

Cyber Security Overview – Fonti delle minacce informatiche

- Le principali **Fonti** da cui provengono **minacce** o **attacchi** informatici possono essere di **due** (2) tipologie:

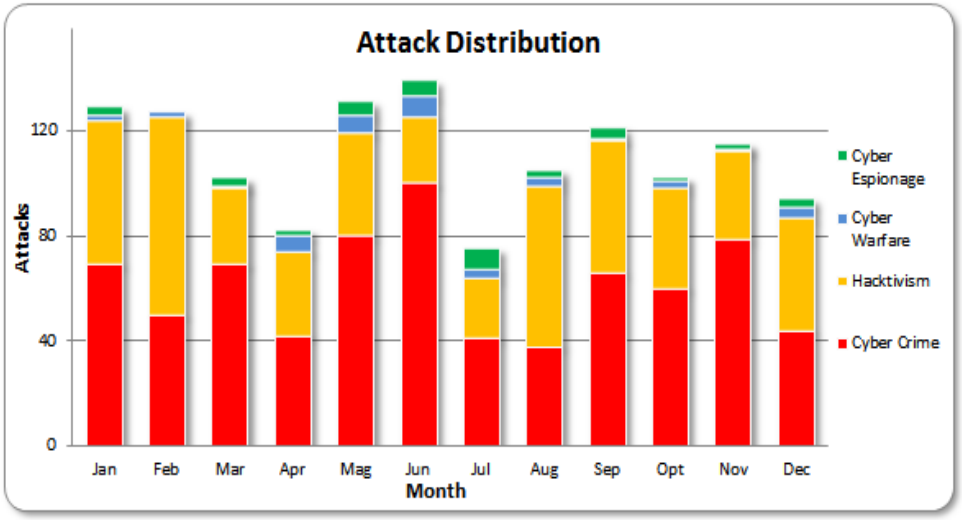
  1. **Interne** - provengono dall'interno della struttura (es: dipendenti aziendali/enti, ecc.);

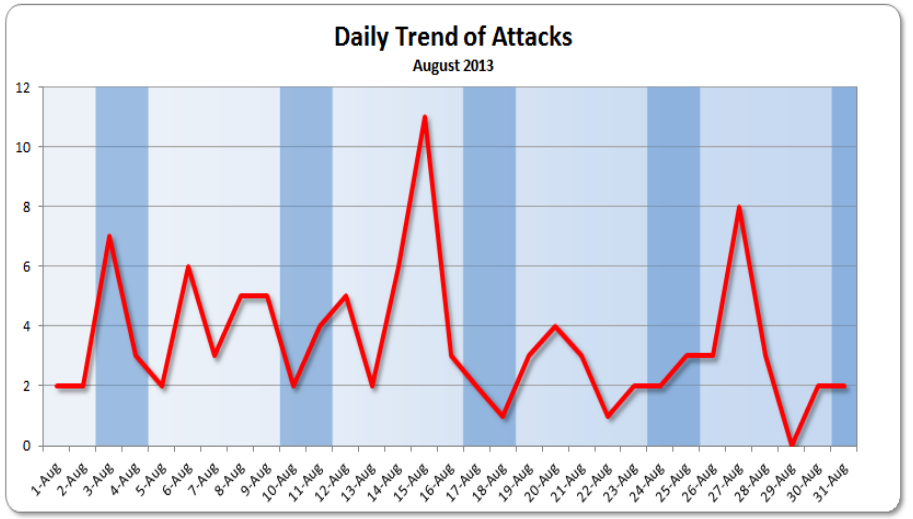
  2. **Esterne** - provengono dall'esterno della struttura (es: hackers, criminalità organizzata, ecc.).

- La maggior parte delle **contromisure** è **focalizzata** sulle **minacce esterne** poiché più **facili da individuare** e contrastare.

- Secondo le rilevazioni annue il numero di **attacchi esterni** è in costante **aumento** e vengono utilizzati **mezzi** sempre più **sofisticati**.

- Il **web** è il **principale vettore d'attacco** anche se il rapido afflusso di **smartphone** e **tablet** sta dando spazio a nuove modalità di attacco basate sui dispositivi mobili, su cui il controllo esercitabile è inferiore.



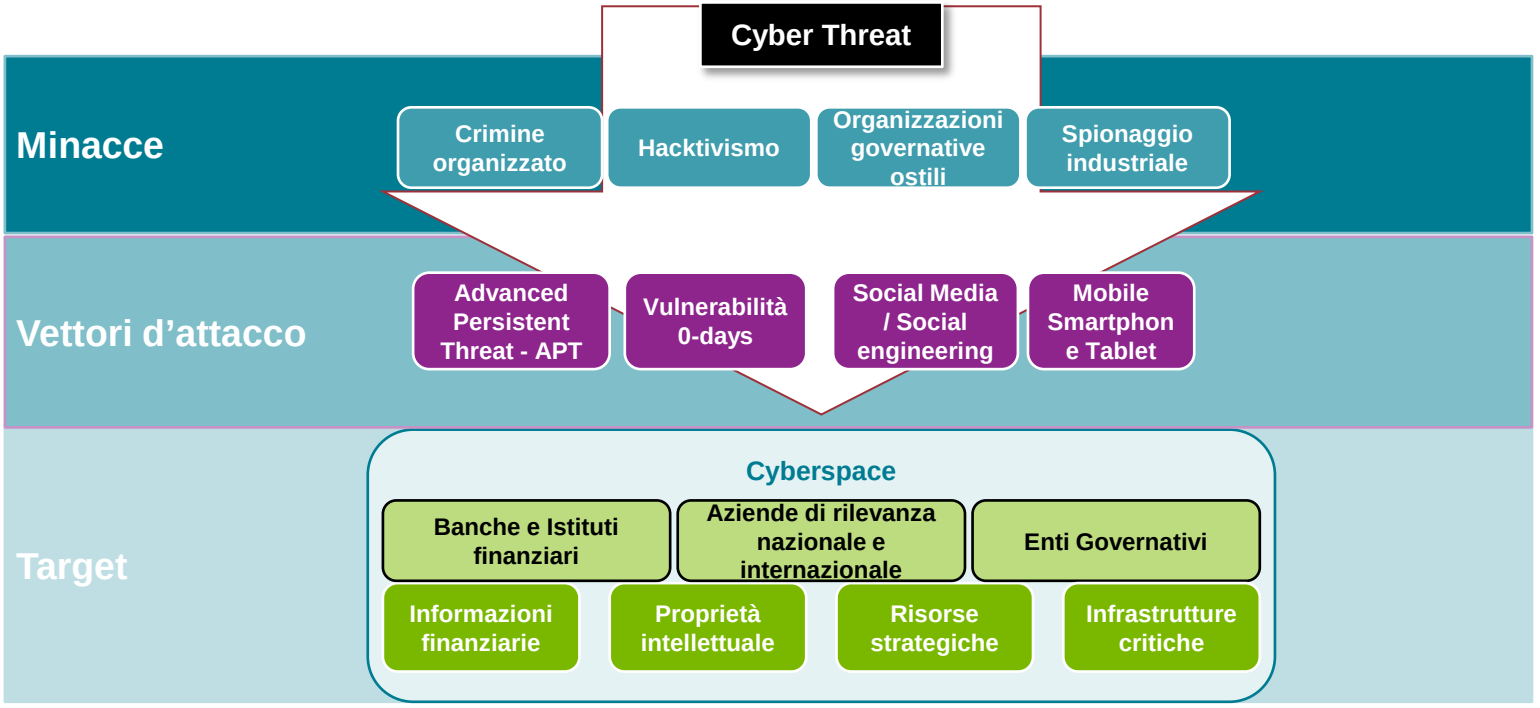


Source: hackmageddon.com

Cyber Security Overview – Scenari evoluzione minacce informatiche

- Gli attuali **scenari** di **minaccia in** continua **evoluzione:**

1. **Nuovi vettori d'attacco** – Attacchi ad Elevata Complessità (**APT**), **Social Media/Engineering**, **Mobile**;
2. **Rapidità** d'**evoluzione** degli **attacchi** – **vulnerabilità 0-days**, **attacchi "su misura"** non rilevabili;
3. **Evoluzione** del **Cyber Crime** – da **Hacker** isolato **a crimine organizzato**, **attacchi** sempre più **sofisticati**;
4. **Obiettivi** mirati – **infrastrutture critiche**, ***hacktivismo***, **spionaggio** di segreti **governativi** e **industriali**.



Cyber Security Overview – Impatti, Perdite e Costi

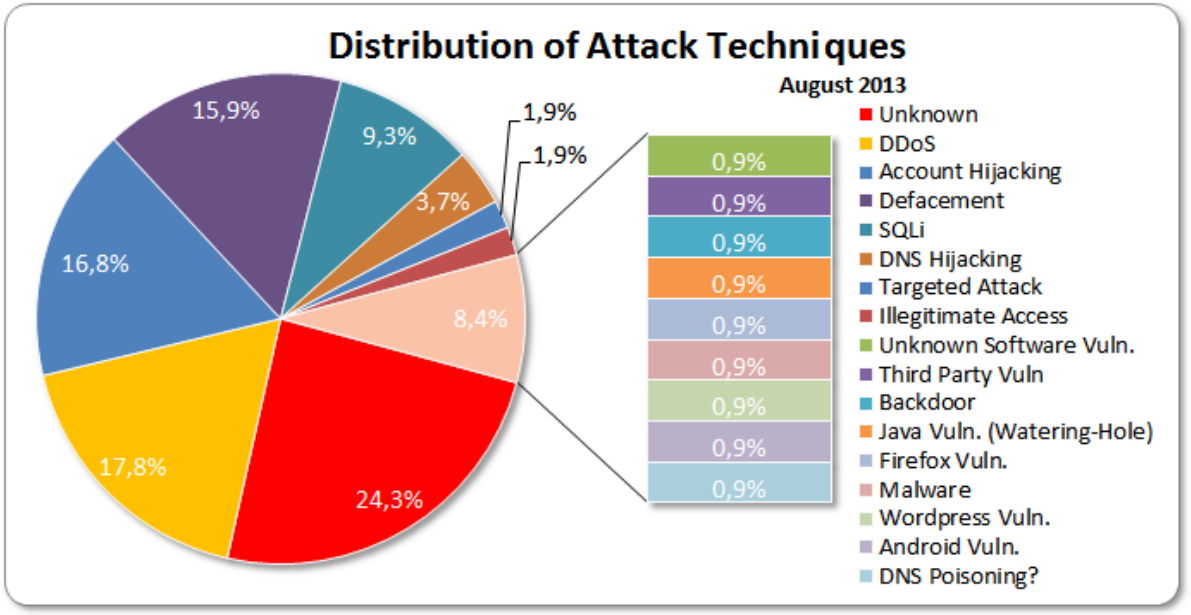
- I **danni** provocati da un **attacco** subito possono essere **molteplici** e **non** sempre sono **quantificabili**.
- I **danni** provocati da un attacco informatico possono avere **diversi 'Impatti'** quali:

Impatti Economici	■ **Costi** diretti di **ripristino**. ■ **Perdite** legate alla **indisponibilità** e/o **interruzione** della **continuità** operativa **aziendale**.
Impatti Legali	■ Sanzioni **amministrative** per infrazione di leggi e/o norme. ■ Sanzioni **penali** e provvedimenti accessori.
Impatti di Immagine	■ Pubblicazione **dati sensibili** o strettamente **personali** . ■ **Svantaggio** in termini di **competitività**. ■ Svalutazione della **reputazione** del **marchio**.

- A livello globale (mondiale) negli **ultimi tre anni** il numero di **attacchi gravi** di pubblico dominio è **cresciuto** del **+245%** ;
- Le **perdite** totali (dirette ed indirette) **causate** dal **Cyber Crime** ~ **500 Miliardi $** (**+26%** rispetto al **2012**).
- La **spesa** globale legata alla **Cyber Security** nel **2013** ~ **70 Miliardi $** (**+16%** rispetto al **2012**);
- Gli **attacchi** verso il settore **Banking/Finance** nel 2013 sono aumentati del **+97%** rispetto al **2012** .

Cyber Security Overview – Tecniche di Attacco Informatico

- Le **tecniche** di **attacco** utilizzate sono **molteplici** e il loro utilizzo varia **in base** alla **finalità** dell'**attacco**.
- Le **tecniche** di attacco **maggiormente diffuse** (riportate nel grafico sotto) riguardano:
  - ✓ Nel **24,3%** dei casi, le **tecniche** di **attacco** informatico **non** sono state ancora ben **identificate**..
  - ✓ Nel **17,8%** dei casi si tratta di **Denial of Service** - DoS (**blocco** sistema **hw/sw**, creando un **disservizio** e/o l'**inaccessibilità** al sistema informativo);
  - ✓ Nel **16,8%** dei casi si tratta di **Account Hijacking** (**dirottamento** dell'**account** e relativo **accesso non autorizzato** al sistema informativo al fine di apportare **modifiche** di vario genere).

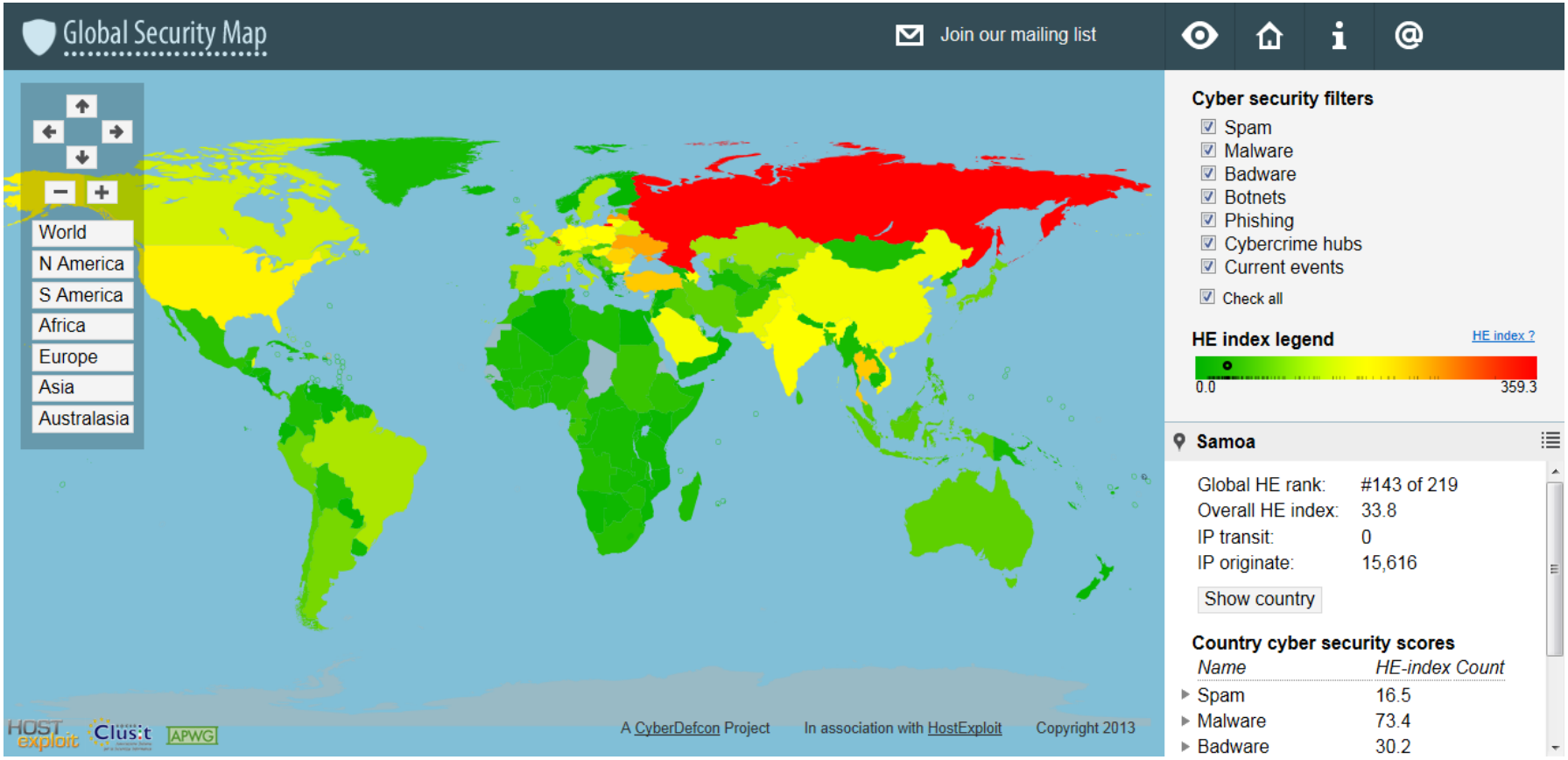


Source: hackmageddon.com

Cyber Security Overview – Diffusione attacchi informatici

- Gli **attacchi** informatici possono **coinvolgere qualsiasi categoria** di **soggetti** in ogni parte **del mondo**.
- La **Russa** è al **1° posto** per ciò che riguarda gli attacchi informatici … al **2° posto** vi è il **Lussemburgo,** al **3° posto** la **Lettonia** seguita da **Ucraina** e **Virgin Islands** (UK)..

Global Security Map 2013

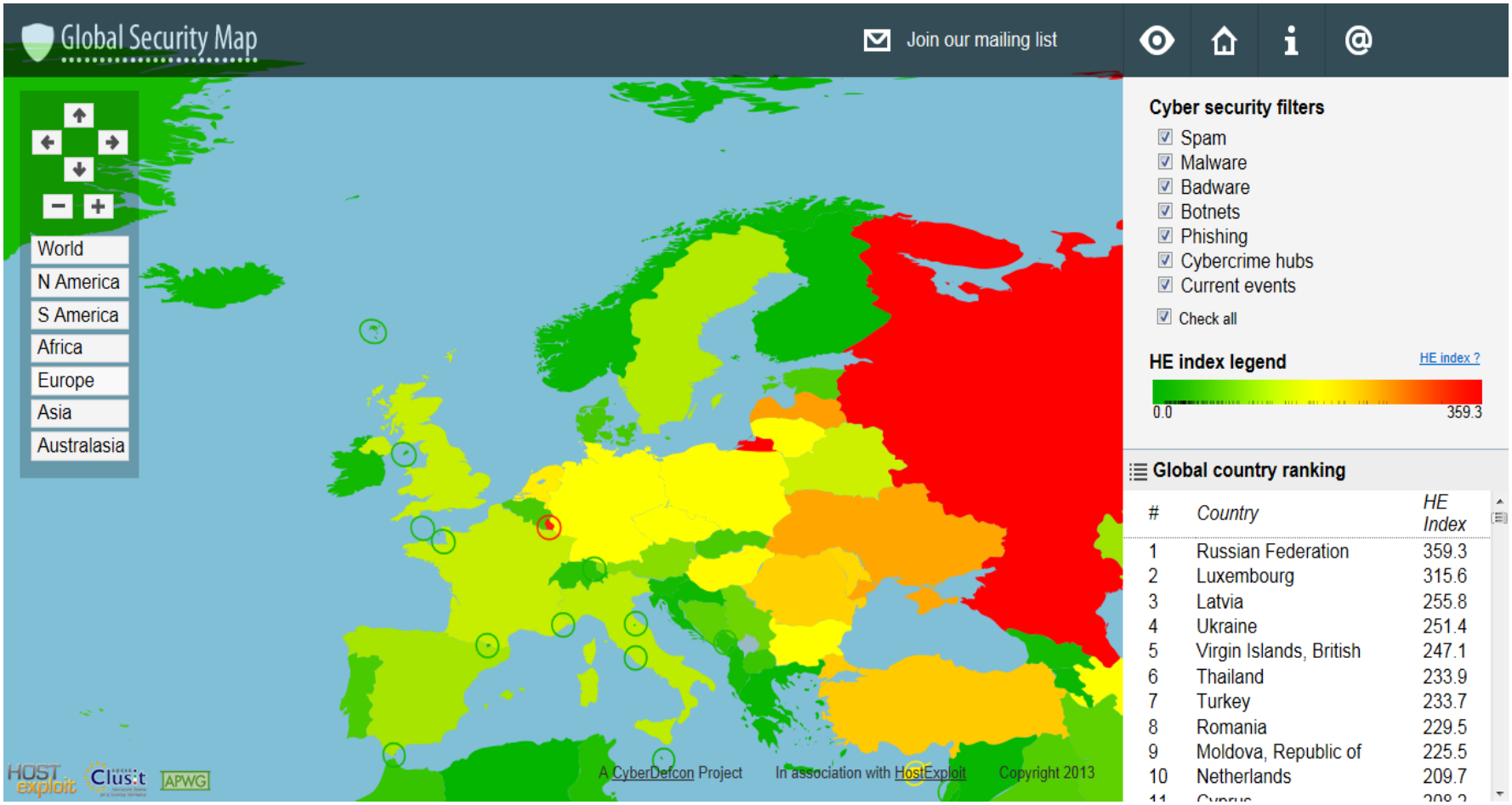


Source: globalsecuritymap.com

Cyber Security Overview – Diffusione attacchi informatici

- Gli **attacchi** informatici in **Europa** sono prevalentemente **concentrati** nell'**Europa** dell'E**st..**

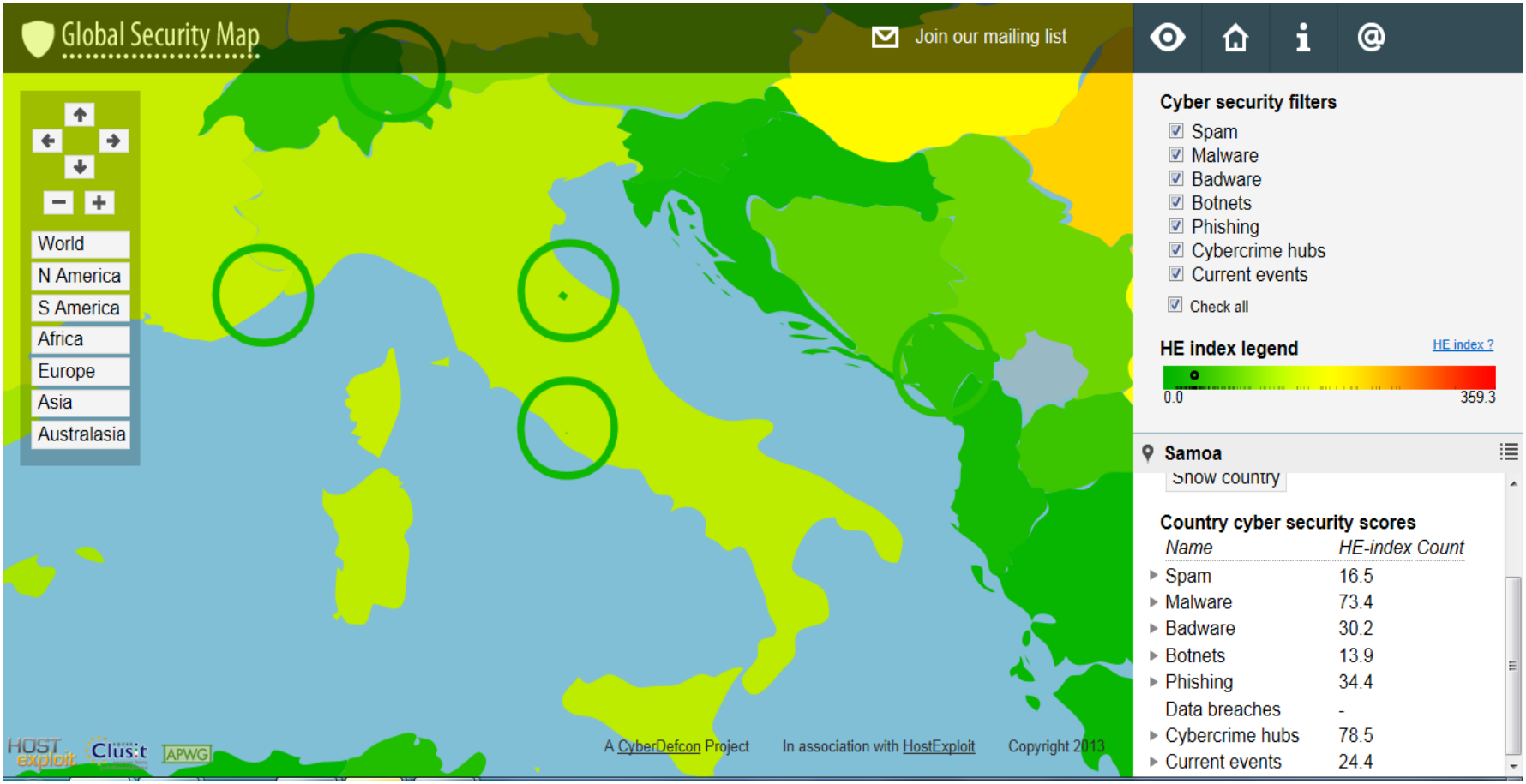
Global Security Map 2013



Cyber Security Overview – Diffusione attacchi informatici

- L'**Italia** è al **31° posto** su **219 Paesi** e gli **attacchi** informatici nel **nostro Paese** sono **da imputarsi** prevalentemente in **'Phishing ', 'Malware' ...**

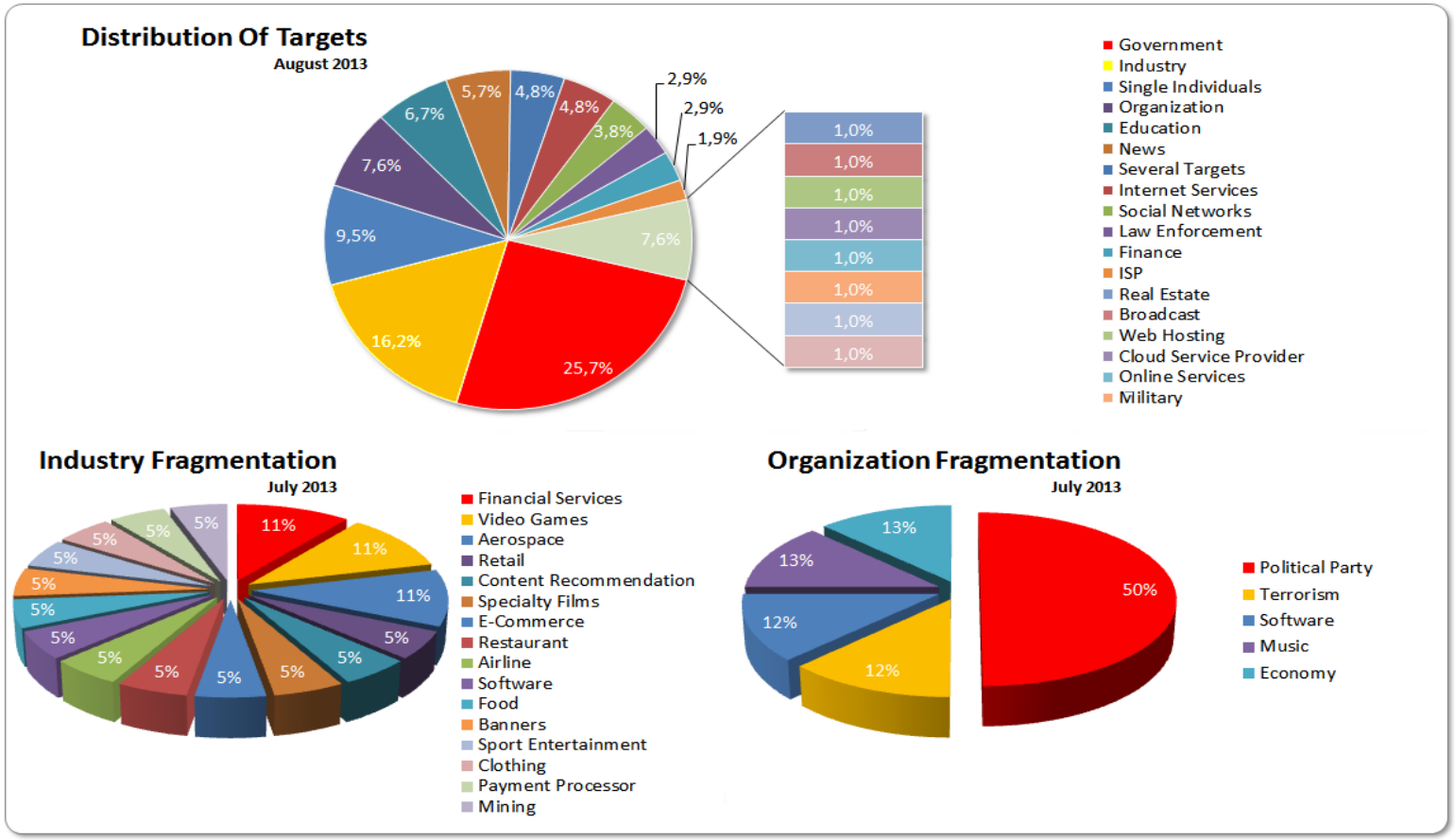
Global Security Map 2013



Source: globalsecuritymap.com

Cyber Security Overview – Target principali degli attacchi informatici

- Gli **attacchi riguardano diverse** tipologie di **Target**: **Government** (25,7%); **Industry** (16,2%)..
- I **settori** più colpiti riguardano: **Financial Services** (11%); **Video Games** (11%); **Aerospace** (11%)..
- Gli **obbiettivi** sono di tipo/carattere **politico** (50%); **economico (13%); terroristico** (12%)..



Source: hackmageddon.com

Cyber Security – Rischi di sicurezza informatica

- Con il termine **'rischio sicurezza informatica'** si intende la **possibilità** che un **attacco** informatico **sfrutti** una o più **debolezze** intrinseche dell'**organizzazione** (c.d. **vulnerabilità**) per effettuare **furti,** provocare **perdite** o **danni** ad un **bene** o ad un **insieme di beni** costituiti da **dati** e **informazioni**.

Cyber Security Overview – Contromisure attacchi informatici

- Per garantire un **adeguato** l**ivello** di **sicurezza** sono adottate **specifiche contromisure** che consentono di **mitigare i rischi** correlati alla **sicurezza** delle **informazioni.**
- Alcune delle **contromisure maggiormente diffuse** in particolare per Aziende/Enti governativi sono:
  - ✓ **Adeguamento** dei **processi** interni seguendo le linee guida definite da **Standard** Internazionali di riferimento in tema **Sicurezza** Informatica (es. ISO/IEC 27001), **Modelli** di **Governance** dei **Controlli** interni sui **Sistemi** Informativi (es: COBIT5 by ISACA), altri **Modelli** di riferimento per la **gestione** delle **risorse informatiche** (es: ITIL, ecc..)
  - ✓ **Definizione** di **policy/e/o procedure di Sicurezza** informatica **(**es: **DPS -** Documento Programmatico Sicurezza; **BCP** – Business Continuity Plan, ecc..);
  - ✓ Uso di **antivirus / firewall**;
  - ✓ **Cifratura** dei **dati** e delle **informazioni**;
  - ✓ **Adeguata** gestione delle **Password** di accesso;
  - ✓ **Back-up** dei **dati ed eventuale**
  - ✓ Predisposizione **Sito** di **Disaster recovery (DR)**
  - ✓ **Tracciamento** delle **operazioni** svolte sui **dati**;
  - ✓ Utilizzo di **canali** di **comunicazione sicuri;**
  - ✓ Etc…

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

PCIDSS – Payment Card Industry Data Security Standard

- Alla **luce** dell'**attuale situazione** in termini di **sicurezza** informatica a livello **globale**, caratterizzata da un forte **aumento di crimini informatici,** è **opportuno** e/o necessario **adottare** e **seguire** le **'linee guida'** contenute all'interno di **standard internazionali** di riferimento.
- Oltre allo Standard **ISO/IEC 27001** che rappresenta il principale **riferimento** per tutti gli **aspetti** riguardanti la **sicurezza** delle **informazioni**, e lo Standard **COBIT 5** che rappresenta il principale f**ramework** per la **Governance** e la **Gestione** dell'**Information Technology**….
- Per la **gestione** in **sicurezza** dei **dati** e delle **informazioni** dei **titolari** delle **carte** di **credito**, si è ritenuto necessario creare uno **Standard** 'ad hoc'**:** '**Payment Card Industry Data Security Standard'**.
- Lo **Standard PCI-DSS:**
  - E' uno **Standard contenente** le **norme internazionali** di **sicurezza**, **creato** da un **consorzio** formato dai principali **operatori** del **settore carte** di **pagamento**;
  - E' stato **sviluppato** per **ridurre** i **rischi** di **sicurezza** (furto, frode, ecc..) riguardanti il **dati** e informazioni dei **titolari** delle **carte** di **pagamento**;
  - Si **applica** a tutte le **entità coinvolte** nell'**elaborazione** di **carte** di **pagamento** (**esercenti**, **elaboratori**, **acquirenti**, **emittenti** e **provider di servizi)**, e a tutte le **altre entità** che si occupano di **memorizzare**, **elaborare** o **trasmettere dati** dei **titolari** di **carta**;
  - **Contiene** N.12 **requisiti tecnici** e **operativi** minimi di **base** per **proteggere** i **dati** dei **titolari** di **carta;**
  - **Contiene** anche un **test** di **valutazione** della **sicurezza** per **verificare** la **compliance** allo standard stesso (vd. '**Self Assessment Questionnaire**' – SAQ).

PCIDSS – Payment Card Industry Data Security Standard

PCIDSS – Payment Card Industry Data Security Standard

Sommario

PCIDSS – Payment Card Industry Data Security Standard

PCIDSS – Payment Card Industry Data Security Standard

PCI Data Security Standard – Panoramica di alto livello

Sviluppo e gestione di una rete sicura	1. Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta 2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati di titolari di carta	3. Proteggere i dati di titolari di carta memorizzati 4. Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche
Utilizzo di un programma per la gestione delle vulnerabilità	5. Utilizzare e aggiornare regolarmente il software o i programmi antivirus 6. Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	7. Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario 8. Assegnare un ID univoco a chiunque abbia accesso a un computer 9. Limitare l'accesso fisico ai dati dei titolari di carta
Monitoraggio e test delle reti regolari	10. Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta 11. Eseguire regolarmente test di sistemi e processi di protezione
Gestione di una politica di sicurezza delle informazioni	12. Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

PCIDSS – Tabella Requisiti e Procedure Valutazione Sicurezza

REQUISITI PCI-DSS PROCEDURE VALUTAZIONE SICUREZZA	DESCRIZIONE N.12 REQUSITI	PROCEDURE TEST	RISULTATO TEST (Presente/Non Presente)	DATA SCADENZA / COMMENTI
SVILUPPO E GESTIONE RETE SICURA	1. Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta	….	P/NP	31.12.2014
	2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	…..	P/NP	..
PROTEZIONE DATI TITOLARI CARTA	*3. Proteggere i dati di titolari di carta memorizzati*	….	P/NP	..
	4. Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche	….	P/NP	..
UTILIZZARE PROGRAMMA GESTIONE VULNERABILITA’	*5. Utilizzare e aggiornare regolarmente il software o i programmi antivirus*	….	P/NP	..
	6. Sviluppare e gestire sistemi e applicazioni protette	….	P/NP	..
IMPLEMENTAZIONE RIGIDE MISURE CONTROLLO ACCESSO	*7. Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario*	….	P/NP	..
	8. Assegnare un ID univoco a chiunque abbia accesso a un computer	….	P/NP	..
	9. Limitare l'accesso fisico ai dati dei titolari di carta	….	P/NP	..
MONITORAGGIO E TEST RETI REGOLARI	*10. Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta*	….	P/NP	..
	11. Eseguire regolarmente test di sistemi e processi di protezione.	…	P/NP	..
GESTIONE POLITICA SICUREZZA INFORMAZIONI	*12. Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale*	…	P/NP	..

PCIDSS – Self Assessment Questionnaire (SAQ)

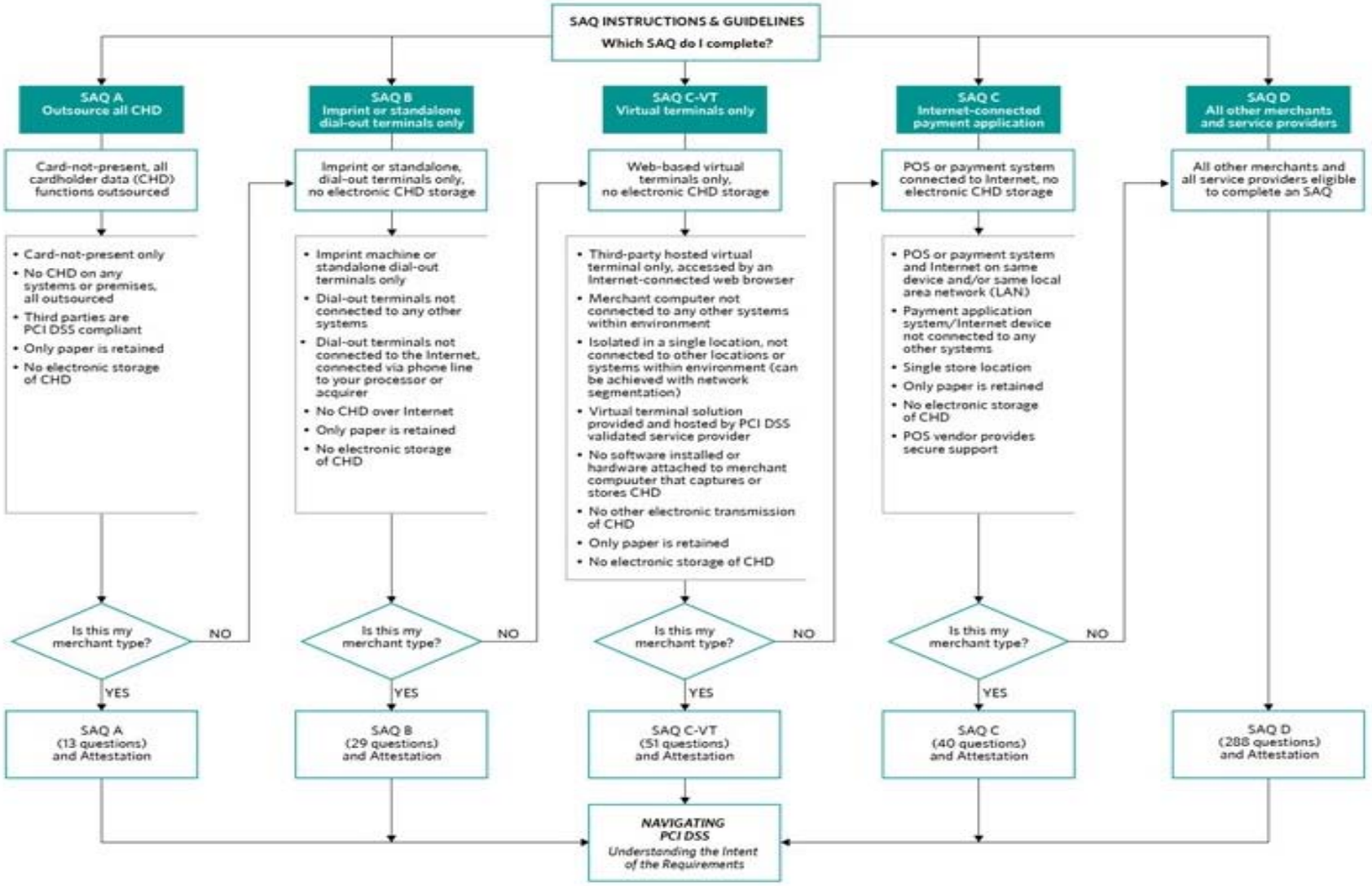
- Lo Standard **PCI DSS** è composto da n.2 parti/componenti principali:

  1. **'Self Assessment Questionnaire'** – **SAQ**
  2. **'Attestation of Compliance'**

     - Il **SAQ** è uno strumento che **assiste** i **soggetti** interessati (entità **coinvolte** nell'**elaborazione** di **carte** di **pagamento**: esercenti, elaboratori, acquirenti, emittenti e provider di servizi);
     - Il**SAQ** consiste in un'**auto-valutazione** in termini di **'compliance'** ai **12 requisiti** del **PCI DSS**;
     - Esistono **diverse versioni** del **'SAQ' in base** all'organizzazione del **soggetto/entità** interessata.
     - Ogni '**SAQ'** include **domande** (da 13 a 288) con risposte 'Yes/No' **circa** la situazione attuale (**As-Is**) in cui un soggetto/entità si trova in termini di **policy** e **procedure** di **sicurezza** informatica.
     - Esistono **n.5 categorie** per capire **quale SAQ** è **più adatto** ad ogni singolo soggetto interessato.

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment brand as eligible to complete an SAQ.

PCIDSS – Self Assessment Questionnaire (SAQ)



PCIDSS – Attestation of Compliance

2. ‘Attestation of Compliance’

- L’Attestation of Compliance è un’**auto-certificazion**e ai requisiti dello Standard PCI-DSS in seguito ai risultati ottenuti grazie all’effettuazione del **SAQ** di cui sopra.
- Al fine di ottenere l’Attestation of Compliance è **opportuno** il **coinvolgimento** di **società ed enti esterni specializzati** nello svolgimento di attività di certificazione, assurance e security risk assessment.
- Tali **società esterne** hanno il compito fondamentale di **supportare** il **soggetto/entità** interessato che vuole **‘certificarsi’** e diventare **‘PCI DSS Compliant’**.

PCIDSS – Qualified Security Assessor (QSA)

- Le entità denominate **‘Qualified Security Assessor’ (QSA**) sono **organizzazioni, riconosciute** dal **‘PCI Council’,** al cui interno operano **professionisti ‘certificati’** dal ‘PCI Council’.
- Tali **professionisti** possono **validare** e accertare se un soggetto/entità è **‘compliant’** o meno ai **requisiti** contenuti e disciplinati nello Standard **PCI DSS**.
- Le organizzazioni **‘QSA’ certificate** dal **PCI Counsil,** allo stato attuale, sonon **n. 330** in tutto il mondo.

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

Standard ISO-IEC 27001- Approccio metodologico

- Per la Gestione della Sicurezza delle Informazioni di solito si fa riferimento allo standard **ISO-IEC 27001** .
- L'**ISO-IE 27001** è uno **Standard Internazionale** correlato alla **definizione** e alla **gestione** di un **"Sistema di Gestione della Sicurezza delle Informazioni"** (SGSI o ISMS).
- Tale sistema si pone come **obiettivo** fondamentale quello di **garantire** un **adeguato livello** di **sicurezza** dei **dati** e delle **informazioni** correlati ai processi in ambito.

Standard PCI-DSS – Approccio Metodologico

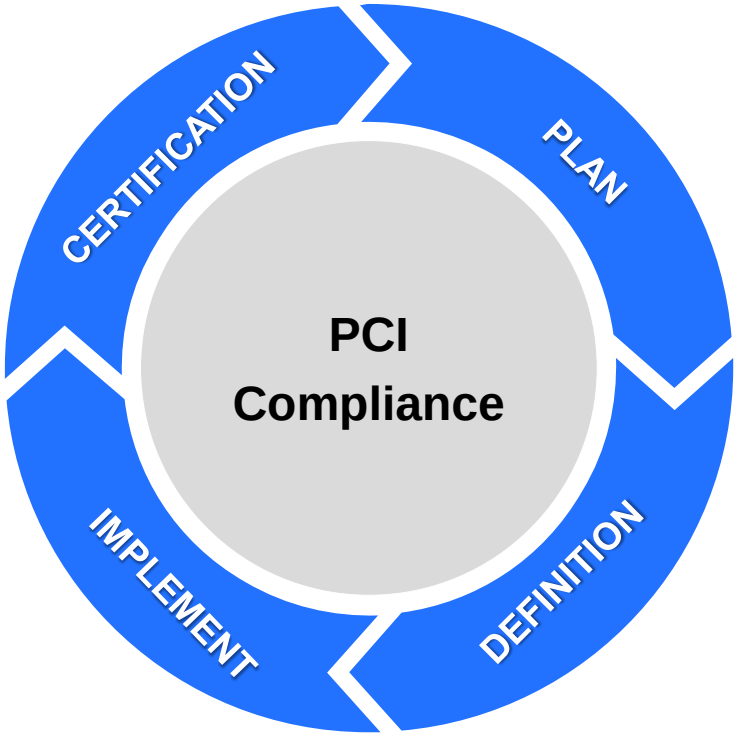
- In relazione allo Standard **PCI-DSS**, l'approccio metodologico consiste in N.**4 "Macro Fasi" (Plan; Definition; Implement; Certification)** e relativi **"Moduli e/o Attività"** che, considerati nel complesso, **coprono** tutte le **fasi** del **processo** di **adeguamento** e/o **certificazione** allo **standard PCI-DSS**.

Accompagnamento alla certificazione

- Accompagnamento alla certificazione tramite **supporto nelle fasi di verifica** da parte dell'ente certificatore

Assessment e Gap Analysis

- Identificazione del **livello di conformità**
- Identificazione di **azioni di adeguamento**
- Definizione di un **remediation plan**



Supporto nell'implementazione dei presidi di controllo

- Supporto nell'**implementazione e nella verifica delle misure di sicurezza:**
  - Ambito organizzativo
  - Ambito tecnologico

Supporto nella definizione dei presidi di controllo

- Supporto nella **definizione di misure di sicurezza** finalizzate a garantire i presidi di controllo richiesti:
  - Ambito organizzativo
  - Ambito tecnologico

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

Q&A Session

Grazie per l’attenzione

Agenda

- Introduzione
- Cyber Security
- PCI DSS
- KPMG Approach
- Q&A Session
- KPMG in sintesi

Una presenza globale

KPMG nel Mondo

155	155.000	$23,7 Mld
Paesi	Professionisti	Ricavi

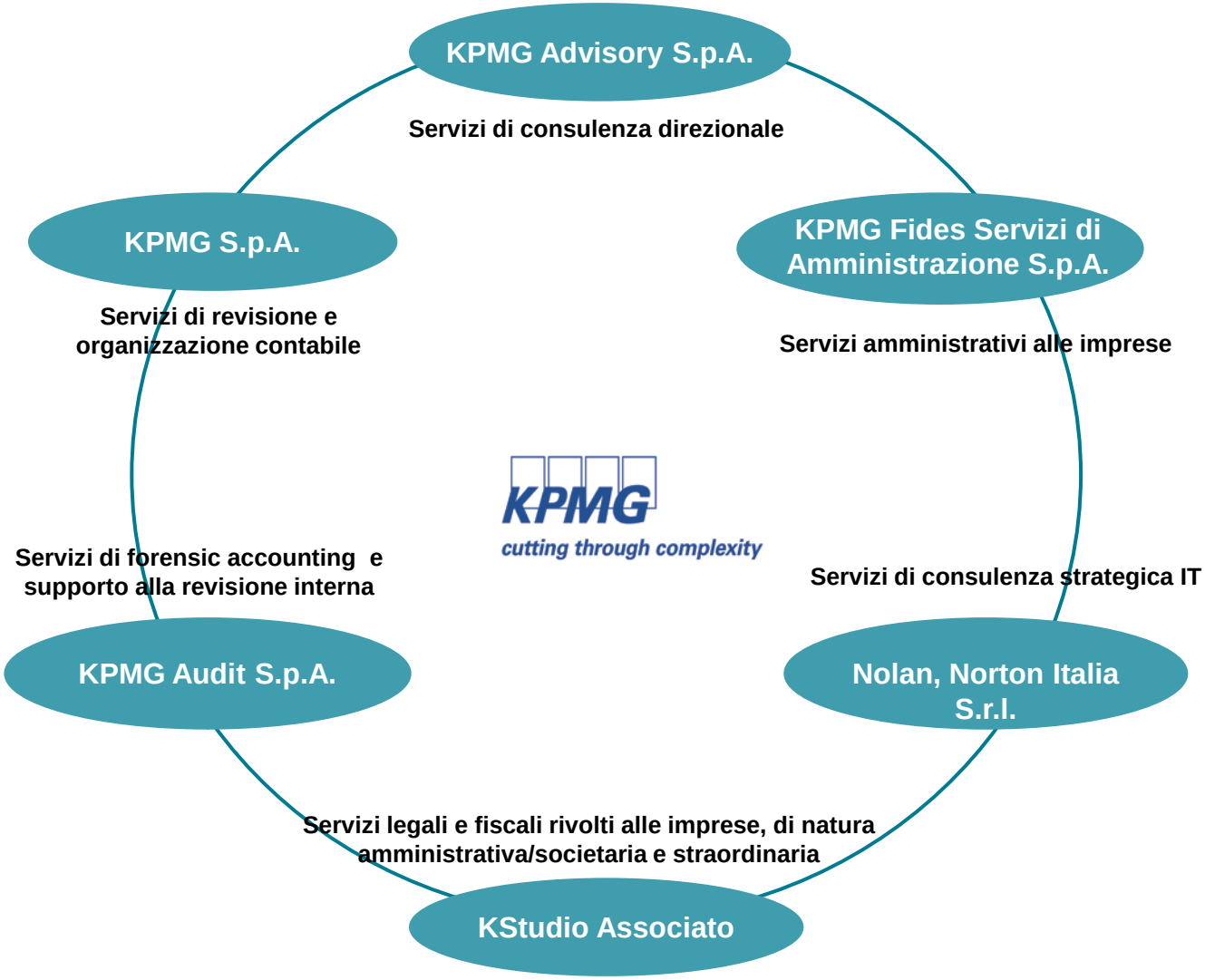
Network KPMG in Italia

27	3.000	€507 Mil
Uffici	Professionisti	Ricavi

"Global Reach – Local Knowledge"

Una grande struttura globale di servizi professionali che accompagna i processi di integrazione economica in atto a livello internazionale

Il network KPMG in Italia



L'offerta dei servizi

Management Consulting (Performance & Technology)

Risk Consulting

Transaction & Restructuring

- Business Performance Services
- IT Advisory
- Accounting Advisory Services
- Financial Risk Management
- Risk & Compliance
- Forensic
- Restructuring
- Transaction
- Corporate Finance

Consumer & Industrial Markets

Food & Beverage	Automotive	Transportation
Settore tessile e moda	Farmaceutico	Media
Retail	Energy	….

Public Sector & Infrastructures

Istituzioni pubbliche nazionali	Enti territoriali
Istituzioni pubbliche locali	Aziende sanitarie

Financial Sector

Istituzioni Bancarie e Finanziarie

Assicurazioni

Real Estate

Alcune referenze

Financial Sector

Consumer and Industrial Market

Public Sector & Infrastructures

Contatti

Davide Grassano

Partner - IT Advisory

KPMG Advisory S.p.A.

dgrassano@kpmg.it

Stefano Volante

Senior Manager - IT Advisory

KPMG Advisory S.p.A.

svolante@kpmg.it