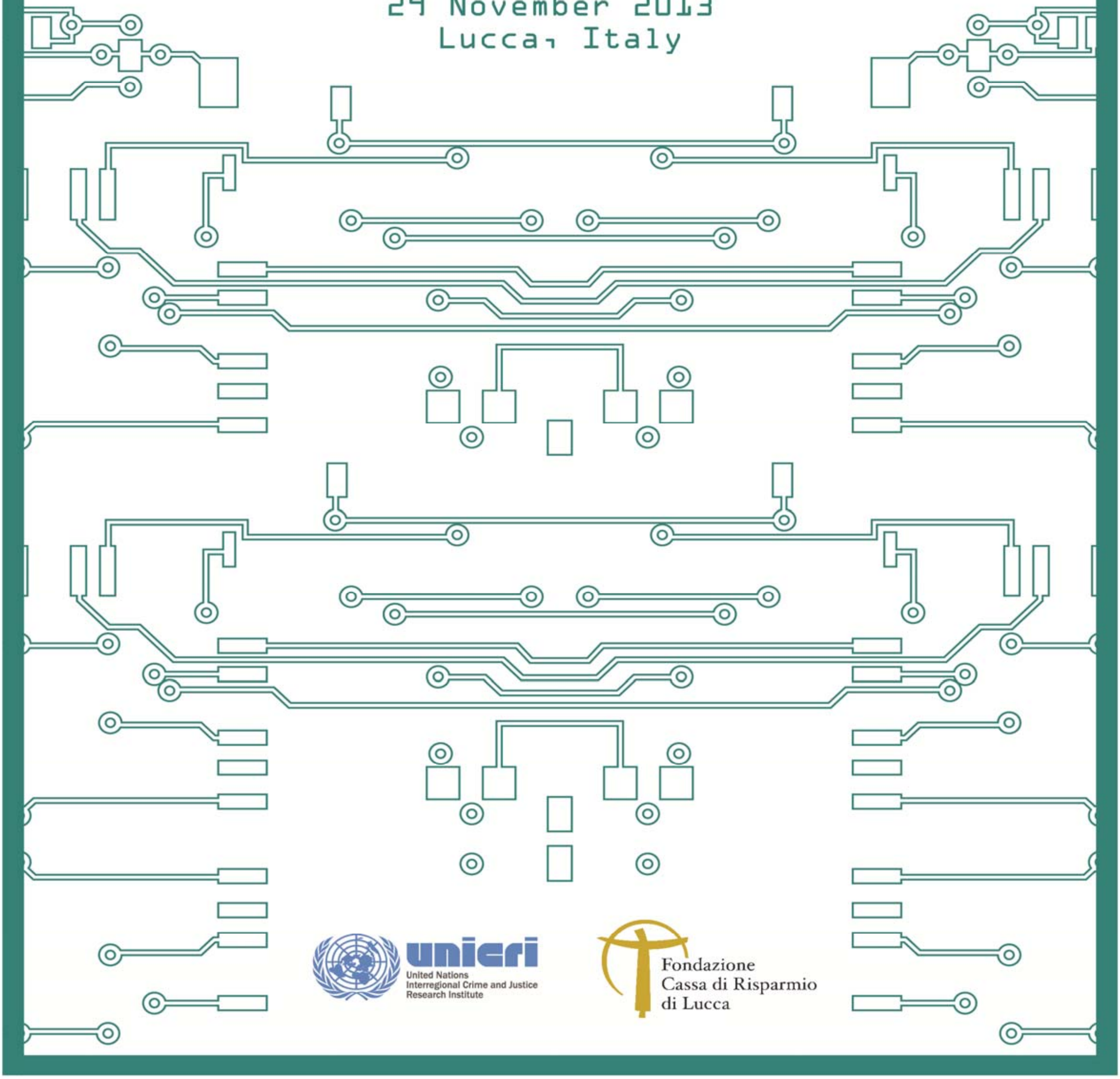
CYBER CRIME:
RISKS FOR THE ECONOMY AND ENTERPRISES

Proceedings of UNICRI roundtable

29 November 2013
Lucca, Italy



unicri
United Nations
Interregional Crime and Justice
Research Institute

Fondazione
Cassa di Risparmio
di Lucca

Acknowledgments

We would like to express our appreciation and thanks to the distinguished speakers and the participants of the roundtable event.

We would especially like to thank *Fondazione Cassa di Risparmio di Lucca* for its support and commitment to UNICRI's activities to enhance justice and security worldwide.

Sincere thanks to UNICRI's team, who coordinated the organization of the event. And a special thanks to Arthur Brocato of UNICRI for editing the document.

Index

List of Acronyms

AISE	*Agenzia informazioni e sicurezza esterna*
AISI	*Agenzia informazioni e sicurezza interna*
ANITEC	*Associazione Nazionale Industrie Informatica, Telecomunicazioni ed Elettronica di Consumo*
CaaS	Crime as a Service
CERT	Computer Emergency Response Team
CISR	*Comitato interministeriale per la sicurezza della Repubblica*
CNAC	National Anticounterfeiting Council (Italy)
CRM	Customer Relationship Management
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DG	Directorate General
DIS	*Dipartimento delle informazioni per la sicurezza*
DPCM	*Decreto del Presidente del Consiglio dei Ministri*
EBF	European Banking Federation
EPC	European Payment Council
EC	European Commission
EC3	European Cybercrime Centre
EECTF	European Electronic Crime Task Force
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Union Agency for Network and Internet Security
EU	European Union
FI-ISAC	Financial Institution Information Sharing & Alerting Center
IB	Interactive Broker
ICE	United States Immigration and Customs Enforcement
ICT	Information and Communication Technology
IPC	Intellectual Property Crime
IT	Information Technology
LEA	Law Enforcement Agency
MLAT	Mutual Legal Assistance Treaty
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCI	National Cybersecurity Institute
NCIRC NATO	Computer Incident Response Capability
NISP	*Nucleo interministeriale situazione e pianificazione*
OSSTMM	Open Source Security Testing Methodology Manual
OTP	One Time Password
OWASP	Open Web Application Security Project
PC	Personal Computer
PCI-DSS	Payment Card Industry-Data Security Standard
PSD	Payment Service Directive
SMEs	Small and Medium Enterprises
TIA	Total Information Awareness
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNINDUSTRIA	Union of Industrialists and Enterprises
UNODC	United Nations Office on Drugs and Crime
USA	United States of America
WEF	World Economic Forum

Introduction: the Purpose of the Event

Advancements in the field of information technology over the past decade have created countless opportunities for growth in the global economy. These developments have, of course, not only affected large, transnational corporations, but also small and medium enterprises (SMEs) at the local level, delivering greater efficiency and sustainability measures to SMEs in an unprecedented period of economic crisis. Unfortunately, along with increased reliance on cyber technology comes an increased risk for cybercrime. SMEs, often relying on limited resources, are now faced with a complex threat that knows no borders. In Clusit 2013 report on Information and Communication Technology (ICT) Security in Italy, the group stressed the risks Italian, and also global, society face as they enter the digital age; "our society is switching from an analogical to a digital approach, from a physical world to the cyber space, IT security threats rise in an exponential manner in terms of both quantity and impact, whilst experts meet large difficulties in reducing these threats, and consequentially the hypothetical short-medium term scenarios are not encouraging."[1]

The proliferation of cybercrime in the modern age is a phenomenon that must be addressed and which has an effect on our everyday lives. Moreover, cybercrime is increasingly being linked to organized criminal networks, effectively raising the costs associated with being vulnerable. When stressing the importance of UNICRI's roundtable on cybercrime, UNICRI Director, Dr. Jonathan Lucas, stated that:

"Cybercrime's zeroing in on the financial sector and small and medium enterprises comes at a delicate time, particularly in Europe where businesses hit by the recession are trying to cope with tight austerity measures and low revenues."

Dr. Lucas went on to map out the objectives of the event, explaining that:

"Our roundtable today aims at generating a clear understanding of the impact of cybercrime on businesses and economy both from a practical and legislative perspective. The experts of the roundtable will discuss best practices in the field of cybersecurity and possible engagement with Lucca's significant business sector."

[1] Clusit (2013), "Italian information Security Association 2013 Report on ICT security in Italy," p. 6. Available online at: http://clusit.it/docs/Rapporto_Clusit%202013_ENG.pdf

Background Information

What are today's cyber threats?

The European Union Agency for Network and Internet Security (ENISA) in its 2013 Threat Landscape Report identified 15 major threats to cybersecurity, ranging from botnets and identity theft to data breaches and phishing schemes, while also specifically pointing out the following negative developments for 2013:

- "Threat agents have increased sophistication of their attacks and their tools."[2]

- "It has become clear that maturity in cyber activities is not a matter of a handful of nation states. Rather, multiple nation states have now developed capabilities that can be used to infiltrate all kinds of targets both governmental and private ones in order to achieve their objectives."[3]

- "Cyber-threats go mobile: attack patterns and tools that targeted PCs a few years ago, have been migrated to the mobile ecosystem."[4]

- "Two new digital battlefields have emerged: big data and the Internet of Things."[5]

In the report's concluding remarks, the importance of end-user involvement is considered vital to tackling cyber threats. This means that SMEs and the general public must be informed of these new threats, making events like the roundtable at Lucca all the more important. In addition, ENISA stressed the need for public-private partnerships to act as coordination mechanisms for sharing information and developing strategies to counter cyber threats in the future.

These same sentiments are echoed in the World Economic Forum's (WEF) 2014 report on *Risk and Responsibility in a Hyperconnected World*. The report claims that "large companies lack the facts and processes to make effective decisions about cyber resilience"[6] and that "concerns about cyberattacks are starting to have measurable negative business implications in some areas."[7] This is arguably even more true for SMEs that lack the resource base of larger corporations. Finally, as an effort to secure cyberspace, the WEF takes a similar position to ENISA, arguing that "the biggest impact

[2] European Union Agency for Network and Information Security (ENISA) (2013), "ENISA Threat Landscape 2013: Overview of current and emerging cyber-threats," p. iii. Available online at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[3] *Ibid.*

[4] *Ibid.*

[5] *Ibid.*

[6] World Economic Forum, in collaboration with McKinsey & Company (2014), "Risk and Responsibility in a Hyperconnected World," p. 13. Available online at: http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

[7] *Ibid*, p. 18.

would come from a combination of efforts involving policy-makers, industry associations such as the Financial Services Information-sharing Analysis Center and individual institutions."[8]

How is cybercrime defined?

Due to the rapidly evolving nature of cybercrime, many governments and international organizations have shied away from adhering to a strict definition of the term. The Council of Europe, United Nations Office on Drugs and Crime (UNODC), and the US Government, amongst others, have taken a comprehensive approach to the subject, including the categorization of a wide variety of acts as constituting elements of the blanket term, "cybercrime." For the UNODC, cybercrime is composed of three main categories, each containing multiple subcategories of cyber criminal activity, which are not considered to be exhaustive. The three main categories are "Acts against the confidentiality, integrity, and availability of computer or data systems"; "Computer-related acts for personal or financial gain or harm"; and "Computer-content related acts."[9] However, some international actors have been more specific in terms of a singular definition of cyber criminal activities. In its Comprehensive Study on Cybercrime, the UNODC makes note of definitions by other prominent organizations attempting to define crime in cyberspace, "the Commonwealth of Independent States Agreement, without using the term 'cybercrime,' defines an '*offence relating to computer information*' as a '*criminal act of which the target is computer information.*' Similarly, the Shanghai Cooperation Organization Agreement defines '*information offences*' as '*the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.*'"[10]

In an environment where the concept of cybercrime is still evolving, the risks of being victimized are even greater. Understanding the dangers of cybercrime is the first step in safeguarding vital information and adopting good practices at the local level. Developing this understanding was a key objective of UNICRI's roundtable discussion.

Understanding the Risks

Approximately 47% of cyber-attacks are inextricably tied to organised crime syndicates. These operate an "underground economy" located within the "dark internet". The term "dark internet" (sometimes also cited as "dark web") refers to websites which have been intentionally concealed from the "normal" web and can be accessed only through the use of anonymizing software. The cyber underground economy works against licit markets

[8] *Ibid.*
[9] UNODC (2013), "Comprehensive Study on Cybercrime," p.16. Available online at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
[10] *Ibid*, p. 12.

on two levels, firstly by affecting supply and demand like traditional undergrounds markets and secondly by trading hacking tools that are used against individuals, financial institutions, businesses and governments. On average, hacking tools are purchased on the dark web for anywhere between $0.40 and £3000 and include trojans used to monitor activities, botnets to launch Distributed Denial of Service (DDOS) attacks and pre-packaged spam attacks.

The global impact of the cyber underground economy has yet to be fully accounted for; however, in its July 2013 report entitled *The Economic Impact of Cybercrime and Cyber Espionage,* the Center for Strategic and International Studies and McAfee estimated the cost of global cybercrime to be somewhere between $300 million and $1 trillion.[11] A more concentrated notion of the dark web's economic scale can be derived through a recent investigation made by Hold Security LLC. In Hold Security's investigation from early 2014, it is estimated that there are currently more than 360 million stolen credentials available for sale on the online black market.[12] In addition, an incredible 1.25 billion stolen email addresses are also for sale online, with credentials come from all the major carriers, including Gmail and Yahoo, inflicting incalculable damage to the global economy.[13]

Cyber-crime's zeroing in on the financial sector and SMEs comes at a delicate time-particularly in Europe where recession-hit businesses try to cope with tight austerity measures and low revenues. These attacks are not cheap; companies need to bear the cost of malware cleanup, lost productivity, investigation and post-incident management. Furthermore, companies may not recover from all cyber-attacks, data loss or the theft of trade secrets can prove fatal for industries that heavily rely on the quality and secrets of their manufacturing.

Moreover, according to the Eurobarometer 404[14], large portions of the general public in Europe are uniformed regarding today's cyber threats. While many people seem to be generally concerned about security, proper measures to safeguard their information are not always taken. This deficiency can easily translate to a lack of knowledge and poor practices in the workplace. Some of the results of the study, conducted across the EU and specifically within the UK, are posted below:

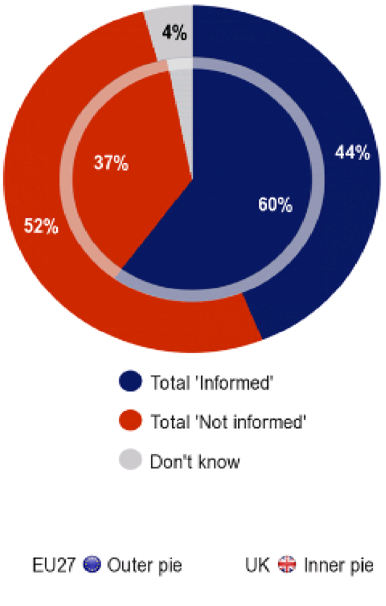
[11] Center for Strategic and International Studies & McAfee (2013), "The Economic Impact of Cybercrime and Cyber Espionage," p. 5. Available online at: http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

[12] Finkle, Jim (2014), "360 million newly stolen credentials on black market: cybersecurity firm." Available online at: http://www.reuters.com/article/2014/02/25/us-cybercrime-databreach-idUSBREA1O20S20140225

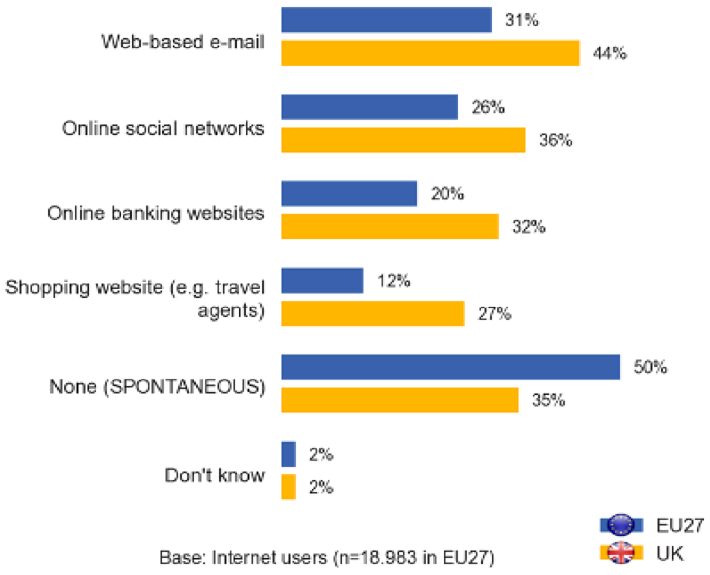
[13] *Ibid.*

[14] The Eurobarometer on Cyber security is available online at: http://ec.europa.eu/public_opinion/archives/eb_special_419_400_en.htm#404

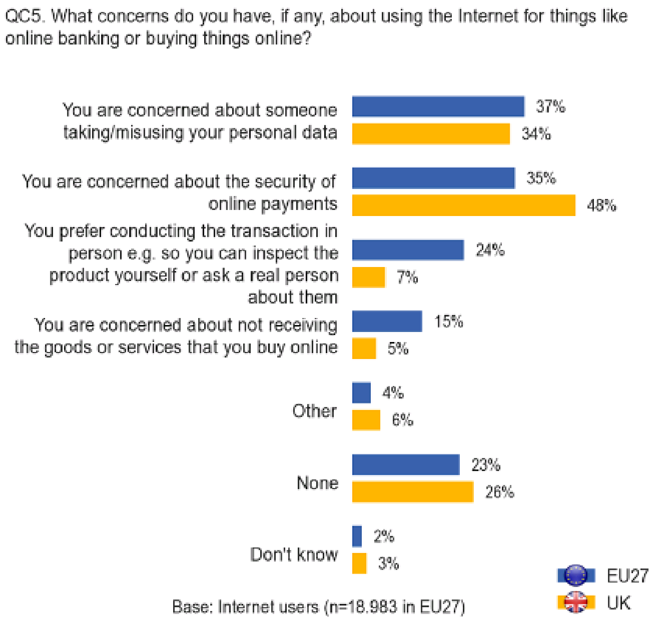
QC8. How well informed do you feel about the risks of cybercrime?

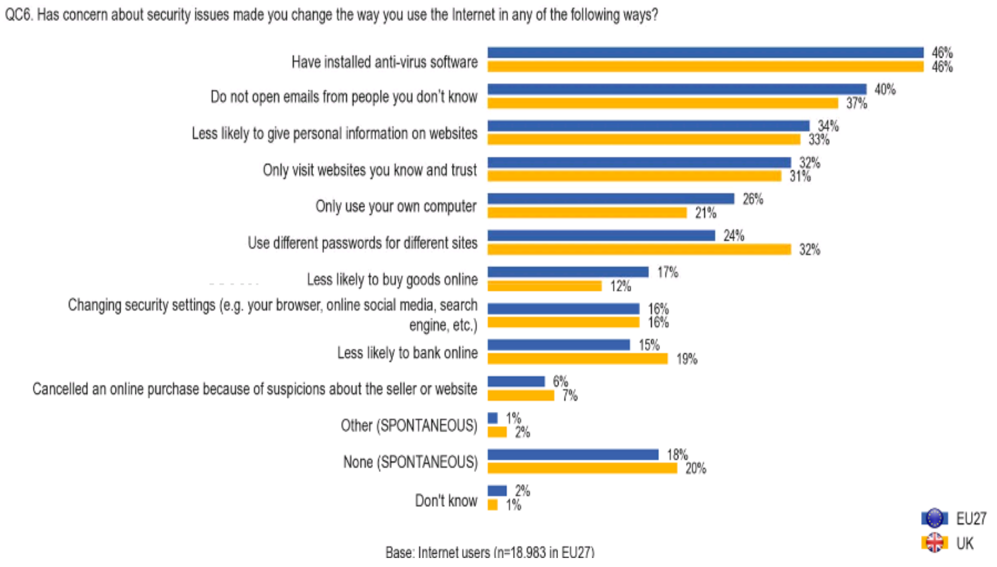


QC13. Have you changed your password to access to any of the following online services during the past 12 months?



Base: Internet users (n=18.983 in EU27)





The roundtable held in Lucca represents the consolidation of UNICRI's commitment to tackling cyber threats and securing cyberspace. The closed door workshop resulted in the production of a paper aimed at defining the international dimension of the Cyber Dark Market. Secondly, it hosted an open forum aimed at generating an understanding of the impact of organized cybercrime on business, finance and critical infrastructure, both from a practical and a legislative perspective.

The topic for the roundtable was selected after careful consideration of the practical and financial challenges that have arisen for governments and private institutions as a result of the financial crisis. On one hand, tight austerity measures and rising unemployment rates have encouraged a new wave of precarious cyber-criminals that view the cyber dark market as a relatively accessible and low-risk way of 'earning' income. On the other hand, they have led to funding cuts for law enforcement agencies and tighter budgets for private security, who therefore struggle to keep up with technological innovations and the large number of threat agents. In the wake of this power shift, enhanced international cooperation and increased public private partnerships ought to take a central role in the creation of sustainable resilience strategies.

The roundtable represented a harmonizing platform that has enabled the exchange of key experts' experiences and resolutions. Furthermore it has been an opportunity for UNICRI to fulfill its mandate by furthering an understanding of the dimension of cyber-crime, fostering efficient justice systems and facilitating international law enforcement.

Summary of the Event

UNICRI's roundtable, entitled "Cybercrime: the Risks for the Economy and the Enterprises", took place in Lucca, Italy on 29 November 2013. The event brought together experts from a range of organizations in both the private and public sectors to discuss the risks for businesses in regard cybercrime, while also discussing legal options and the implementation of good practices.

Following the opening remarks, the all-day event commenced with a presentation by Benoit Godart of EC3, Europol's Cybercrime Centre. Mr. Godart's presentation offered an overview of today's cyber landscape, while highlighting active challenges to security. Within this framework, Mr. Godart explained EC3's role, partnerships, and scope of operations.

Michele Socco of the European Commission then gave background information on cybercrime, assessing current cyber threats and their links to organized crime, mapping out the EU's policy response to these phenomena, and also looking at the road ahead.

Matteo of Lucchetti of the European Electronic Crime Task Force (EECTF) presented on the activities of his organization as a hub for experts, law enforcement agencies (LEAs), and private actors to come together to analyze and tackle cybercrime issues. Mr. Lucchetti proceeded to discuss emerging trends in cybercrime, the EU, and specifically Italy's, cyber strategies, and the creation and function of Poste Italiane's Computer Emergency Response Team (CERT).

Francesca Arra, of Italy's Ministry of Economic Development, focused on the issue of cyber counterfeiting, effectively the infringement of industrial property rights through the use of the internet. Ms. Arra expounded upon the detrimental effects of cyber counterfeiting on businesses, whole economies, and nations, while also describing anti-counterfeiting measures taken by Italy and various corporations.

Cybercrime in the banking sector was the focus of Romano Stasi's presentation. Mr. Stasi of ABI Lab, a banking and research innovation centre, discussed a variety of issues including the evolution of the legal framework of cyber security, institutional work on cyber security, e-crime in the Italian banking sector, and the action being taken to block and prevent internet fraud.

Following a working lunch, Giuseppe Vaciago, a lawyer from R&P Legal, presented on the fundamentals of cyber security. Mr. Vaciago expanded on three elements as being crucial aspects of the cyber security environment, namely technology, the human element, and legal instruments and policy.

The head of eBay's legal department in Italy, Andrea Moretti, then took the floor. His presentation focused on the legal aspects and good practices associated with cyber security in enterprises. His presentation also provided a case study, based in Italy, which described cyber attacks carried out against eBay sellers' accounts from 2012 to 2013.

Giancarlo Grasso, Vice President of the *Associazione Nazionale Industrie Informatica, Telecomunicazioni ed Elettronica di Consumo* (ANITEC) presented the activities of his organization in regard to cyber security and explained, in detail, the development of the Italian Government's cyber security strategy.

Finally, Guido Sandonà, Chief Information Security Officer for Bulgari, made a presentation entitled, "Cyber security in Enterprises – Legal Aspects and Good Practices." Mr. Sandonà focused on six areas, specifically Security Domains, Security Framework and Approach, Data Protection – Privacy, PCI-DSS, Fraud Prevention and Protection, and Compliance Management.

The complete agenda of the roundtable has been listed below, followed by the presentations of the speakers.

The Agenda

Friday, 29 November 2013

1. Works opening and working day presentation

- Fondazione Cassa di Risparmio di Lucca, Arturo Lattanzi, President
- Città di Lucca, Alessandro Tambellini, Mayor
- Provincia di Lucca, Stefano Baccelli, President
- Camera di Commercio di Lucca, Claudio Guerrieri, President
- IMT Institute for Advanced Studies, Guido Caldarelli, Associate Professor
- UNICRI, Jonathan Lucas, Director
- UNICRI, Angela Patrignani, Head of Unit
- UNICRI, Francesca Bosco, Project Officer
- UNICRI, Elena D'Angelo, Project Officer

2. Cyber crime and risks for economy and enterprises

- EC3 (Europol Cybercrime Center), Benoit Godart, Head of Outreach & Support
- European Commission - Directorate General Home Affairs , Michele Socco, Unit A2 - Organised crime and relations with EMCDDA
- European Electronic Crime Task Force (EECTF), Stefano Grassi, Chairman (presentation given by Matteo Lucchetti, Technical Leader)
- Ministero dello Sviluppo Economico, Francesca Arra, Assistant to the President of the Italian Anticounterfeiting Council at the Ministry of Economic Development
- ABI Lab, Romano Stasi, Managing Director

3. Cyber security in enterprises: legal aspect and good practices

- R&P Legal, Giuseppe Vaciago, Lawyer
- eBay, Andrea Moretti, Head of Legal Italy
- ANITEC - Confindustria, Giancarlo Grasso, Vice President
- Bulgari, Guido Sandonà, Chief Information Security Officer

The Presentations

Benoit Godart– EC3 (Europol Cybercrime Center)

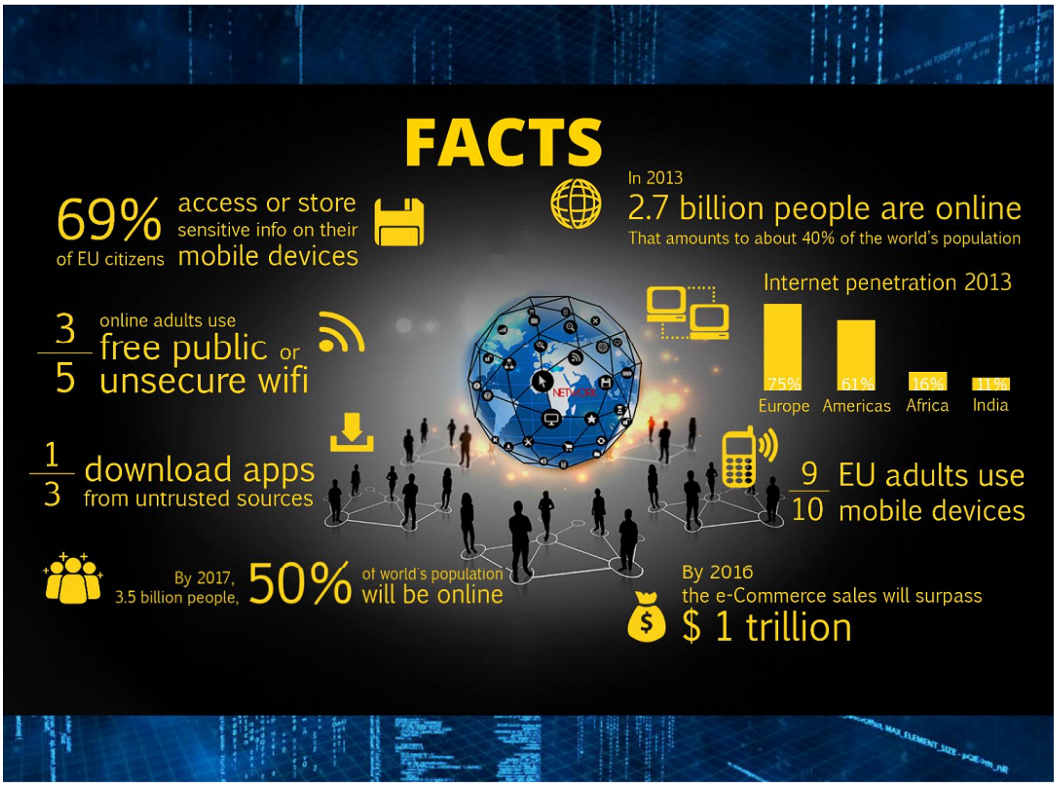
EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Combating Crime in a Digital Age

Thank you



FACTS

69% of EU citizens access or store sensitive info on their mobile devices

3/5 online adults use free public or unsecure wifi

1/3 download apps from untrusted sources

By 2017, 3.5 billion people, 50% of world's population will be online

In 2013 2.7 billion people are online

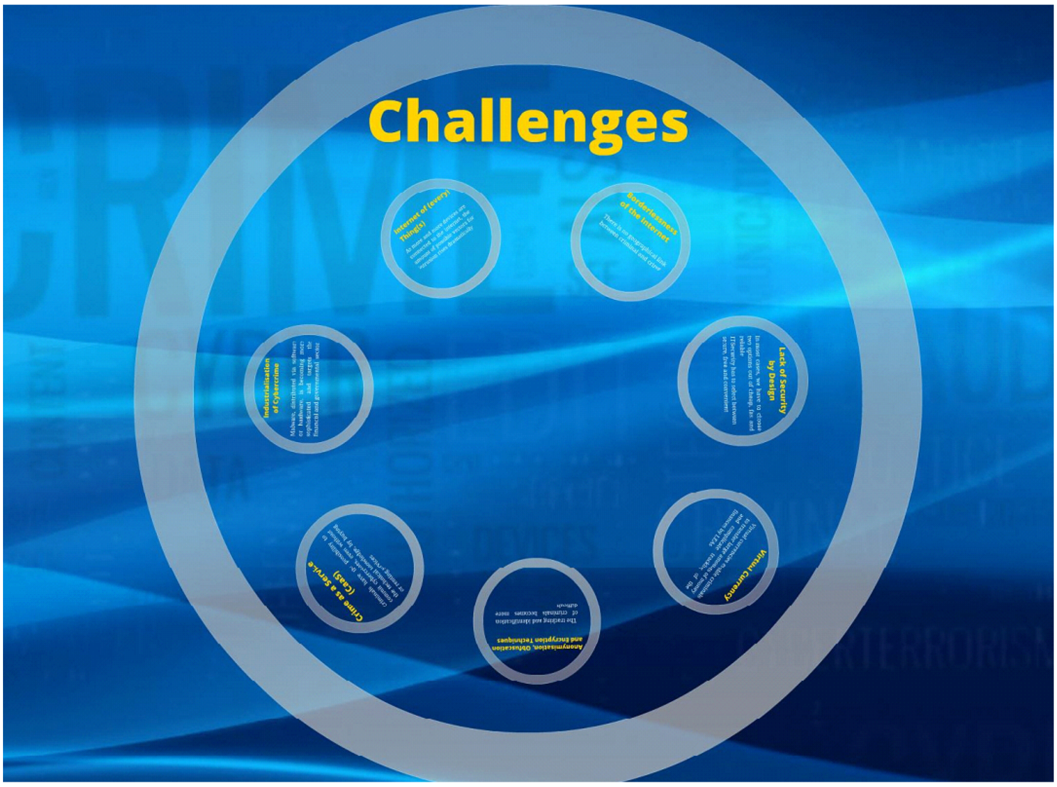
That amounts to about 40% of the world's population

Internet penetration 2013

Europe	Americas	Africa	India
75%	61%	16%	11%

9/10 EU adults use mobile devices

By 2016 the e-Commerce sales will surpass $ 1 trillion



Challenges

Internet of (every) Thing(s)
As more and more devices are connected to the internet, the amount of possible vectors for intrusion rises dramatically

Borderlessness of the Internet
There is no geographical link between criminal and crime

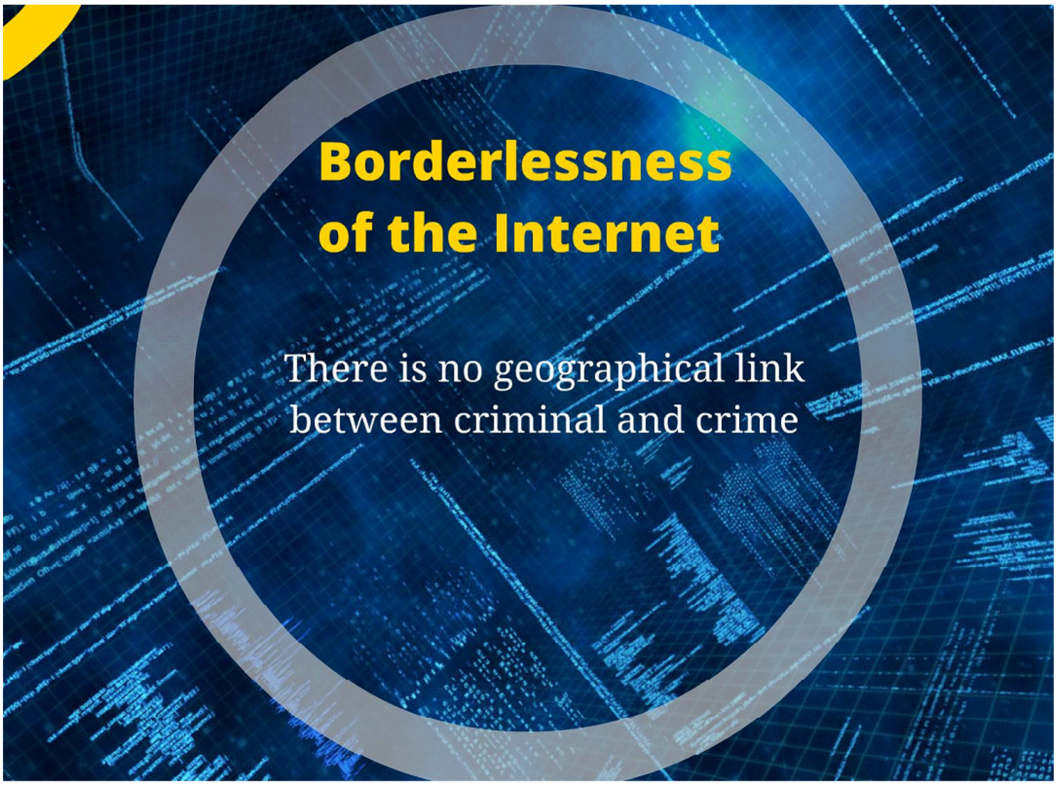
Lack of Security by Design
In most cases, we have to choose two options out of cheap, fas and reliable
IT Security has to select between secure, free and convenient

Virtual Currency
Virtual currencies enable criminals to transfer large amounts of money and complicate tracking of the finances by LEAs

Anonymisation, Obfuscation and Encryption Techniques
The tracking and identification of criminals becomes more difficult

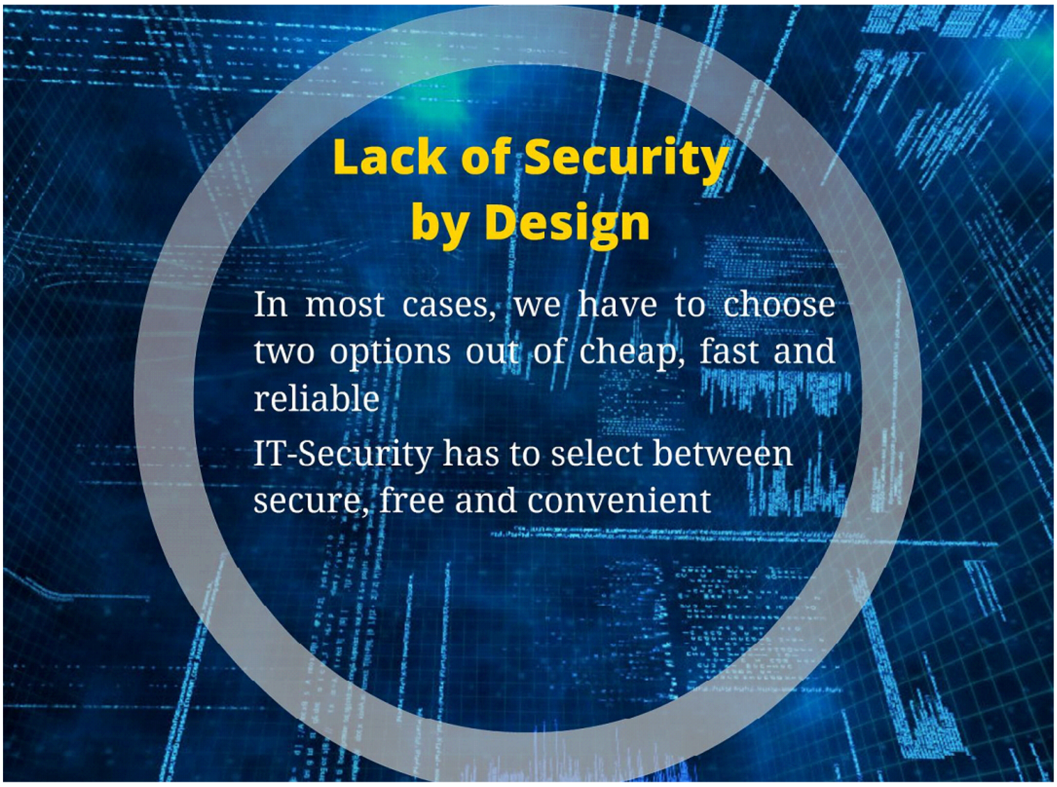
Crime as a Service (CaaS)
Criminals have the possibility to commit cybercrimes, even without the technical knowledge, by buying or renting services

Industrialisation of Cybercrime
Malware, distributed via software or hardware, is becoming more sophisticated and targets the financial and governmental sector



Borderlessness of the Internet

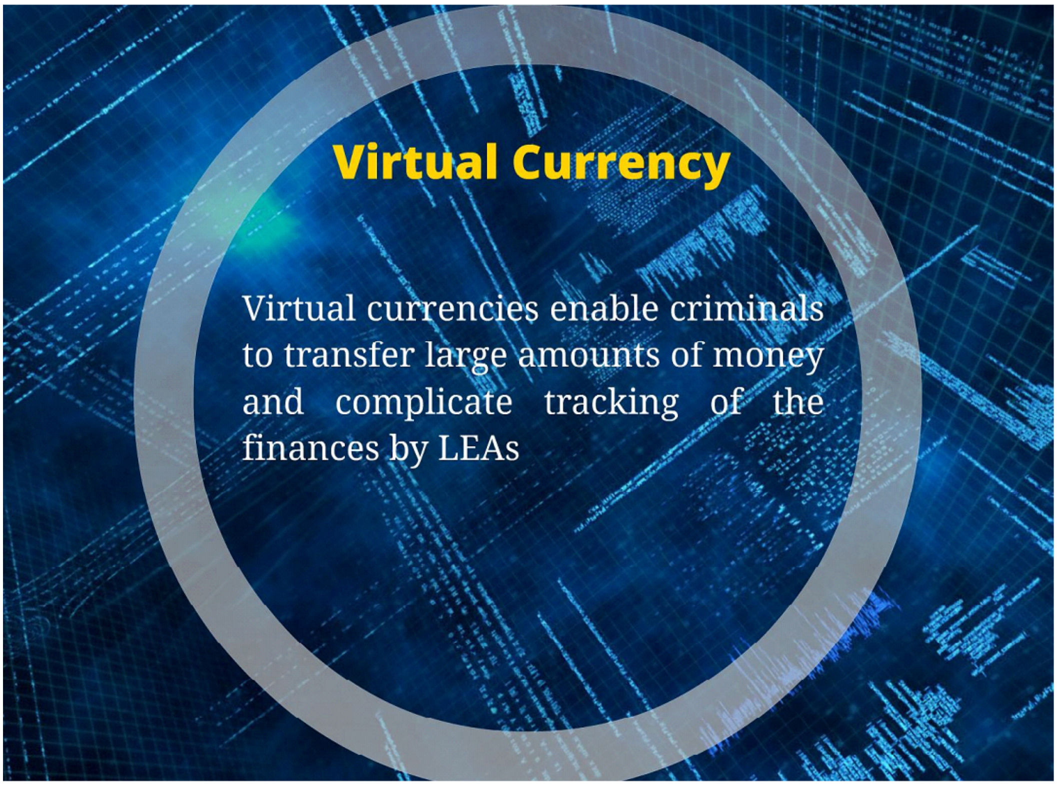
There is no geographical link between criminal and crime



Lack of Security by Design

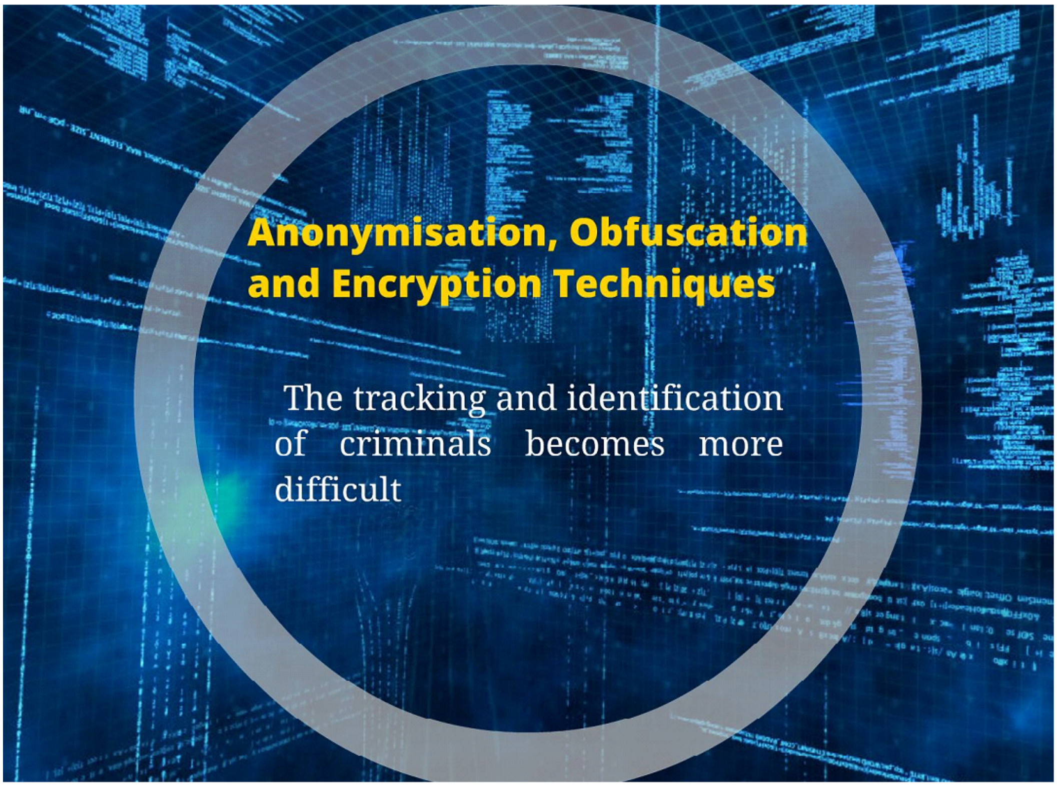
In most cases, we have to choose two options out of cheap, fast and reliable

IT-Security has to select between secure, free and convenient



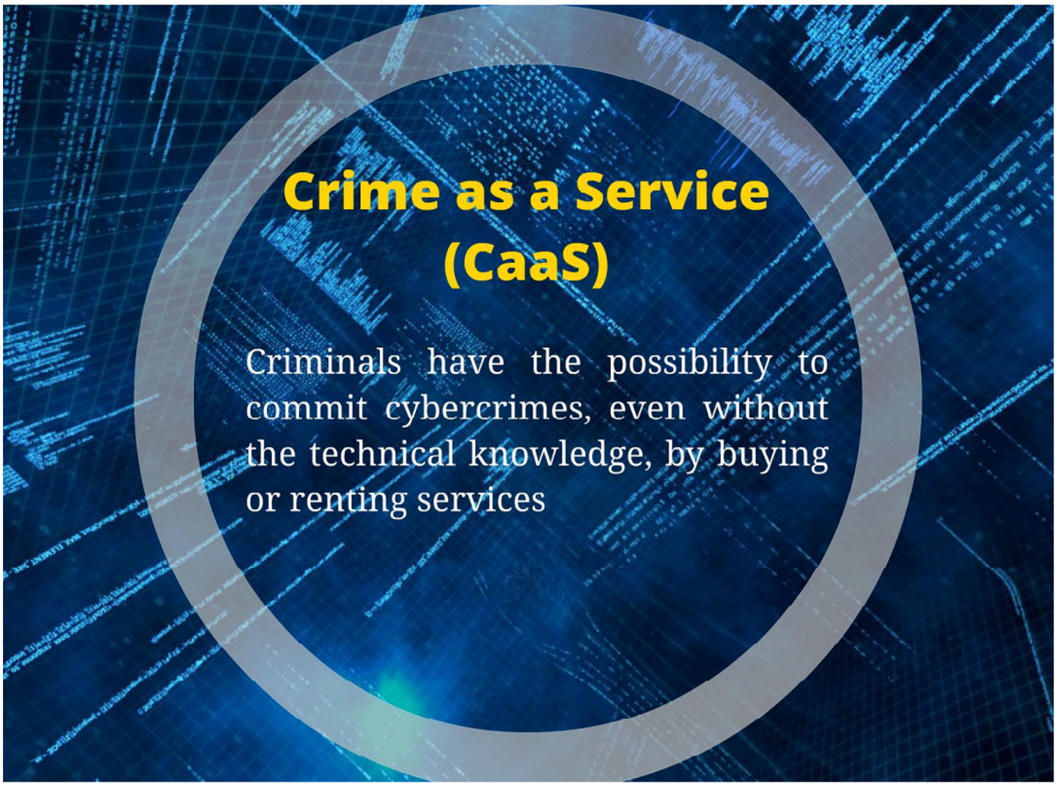
Virtual Currency

Virtual currencies enable criminals to transfer large amounts of money and complicate tracking of the finances by LEAs



Anonymisation, Obfuscation and Encryption Techniques

The tracking and identification of criminals becomes more difficult

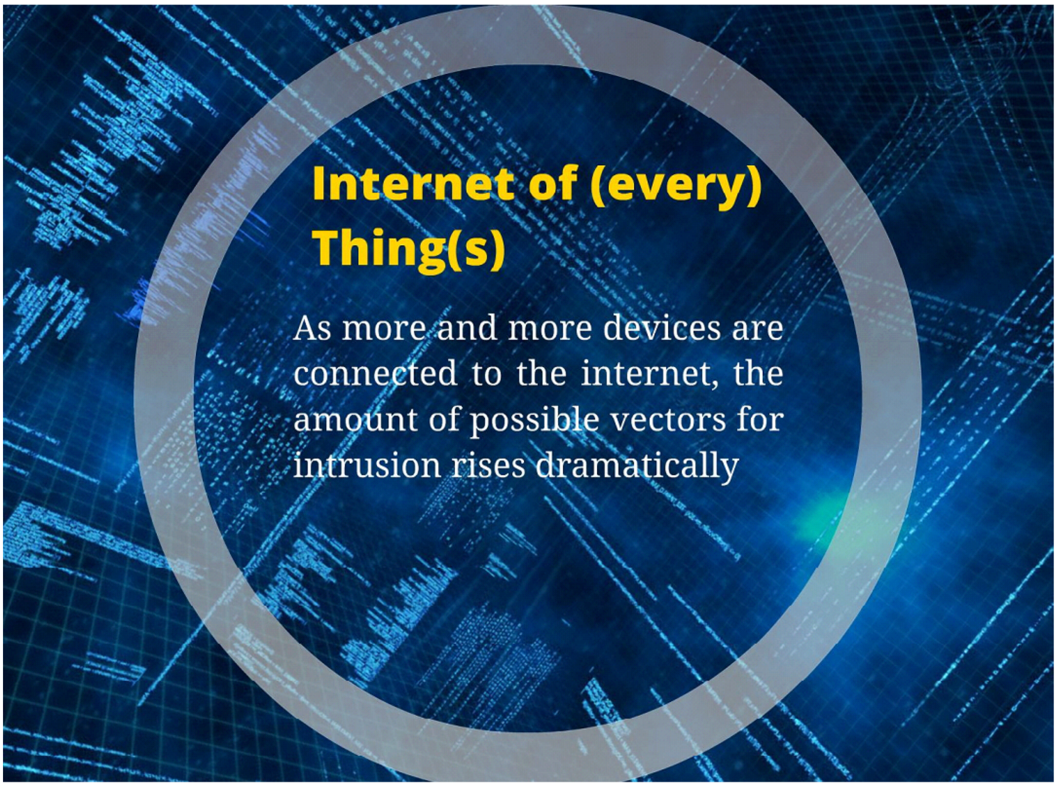


Crime as a Service (CaaS)

Criminals have the possibility to commit cybercrimes, even without the technical knowledge, by buying or renting services

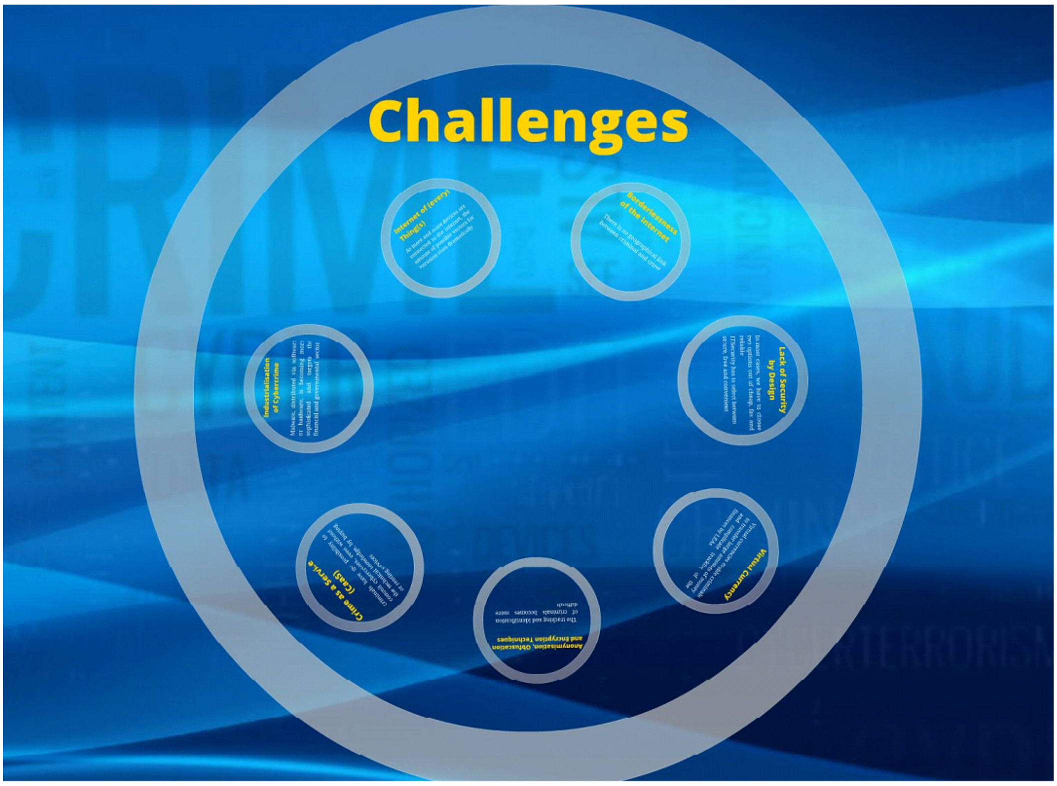
Industrialisation of Cybercrime

Malware, distributed via software or hardware, is becoming more sophisticated and targets the financial and governmental sector



Internet of (every) Thing(s)

As more and more devices are connected to the internet, the amount of possible vectors for intrusion rises dramatically



Challenges

Internet of (every) Thing(s)
As more and more devices are connected to the internet, the amount of possible vectors for intrusion rises dramatically

Borderlessness of the Internet
There is no geographical link between criminal and crime

Lack of Security by Design
In most cases, we have to chose two options out of cheap, fas and reliable
ITSecurity has to select between secure, free and convenient

Virtual Currency
Virtual currencies enable criminals to transfer large amounts of money and complicate tracking of the finances by LEAs

Anonymisation, Obfuscation and Encryption Techniques
The tracking and identification of criminals becomes more difficult

Crime as a Service (CaaS)
Criminals have the possibility to commit cybercrimes, even without the technical knowledge by buying or renting services

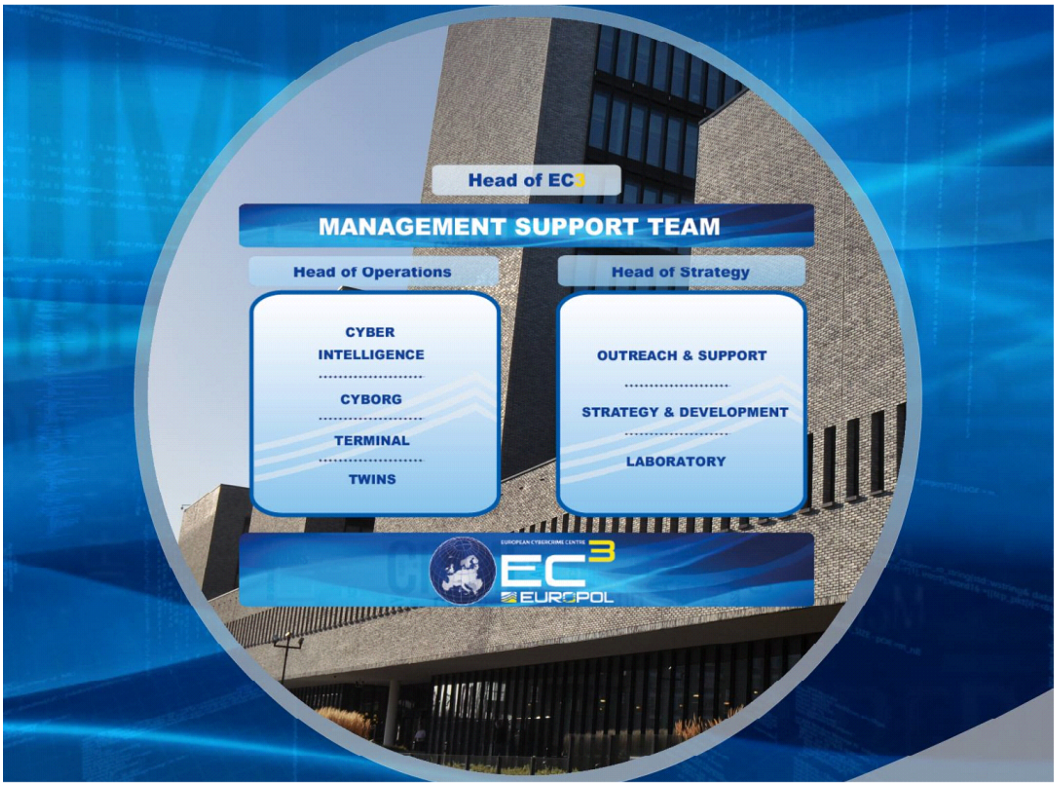
Industrialisation of Cybercrime
Malware, distributed via software or hardware is becoming more sophisticated and targets the financial and governmental sector

Prevention

Protection

Disruption

Recovery



Head of EC3

MANAGEMENT SUPPORT TEAM

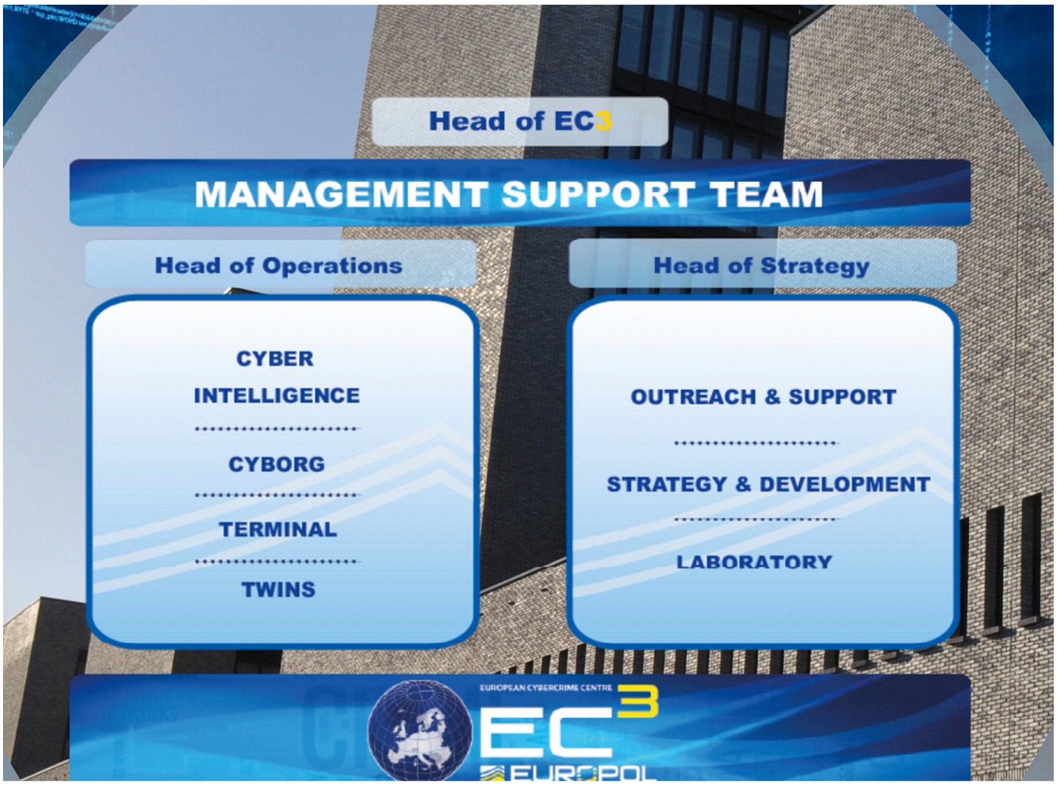
Head of Operations

- CYBER INTELLIGENCE
- CYBORG
- TERMINAL
- TWINS

Head of Strategy

- OUTREACH & SUPPORT
- STRATEGY & DEVELOPMENT
- LABORATORY

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL



Head of EC3

MANAGEMENT SUPPORT TEAM

Head of Operations

CYBER INTELLIGENCE

CYBORG

TERMINAL

TWINS

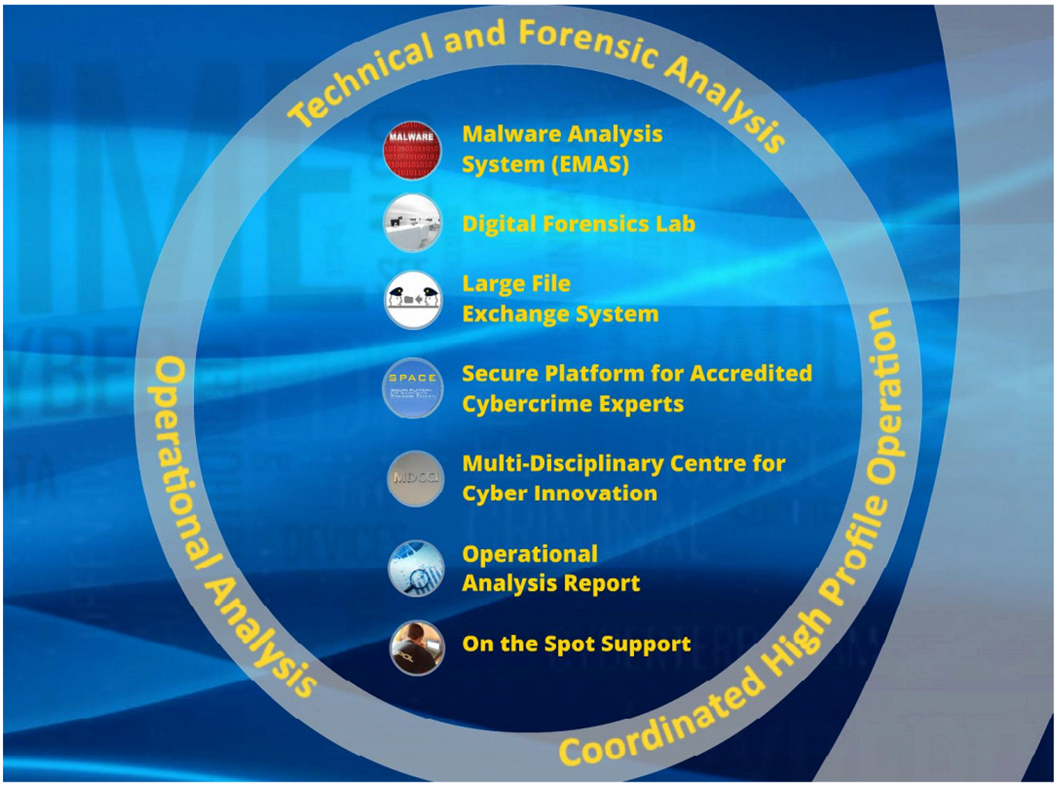
Head of Strategy

OUTREACH & SUPPORT

STRATEGY & DEVELOPMENT

LABORATORY

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL



Technical and Forensic Analysis

Malware Analysis System (EMAS)

Digital Forensics Lab

Large File Exchange System

Secure Platform for Accredited Cybercrime Experts

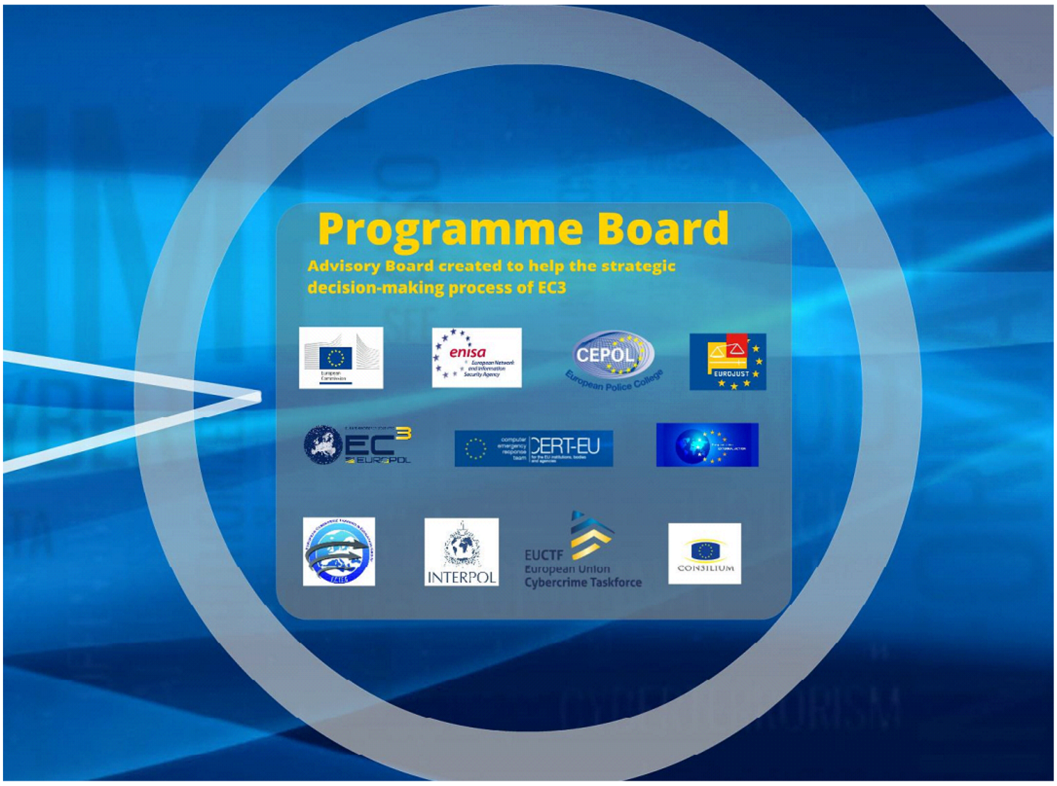
Multi-Disciplinary Centre for Cyber Innovation

Operational Analysis Report

On the Spot Support

Coordinated High Profile Operation

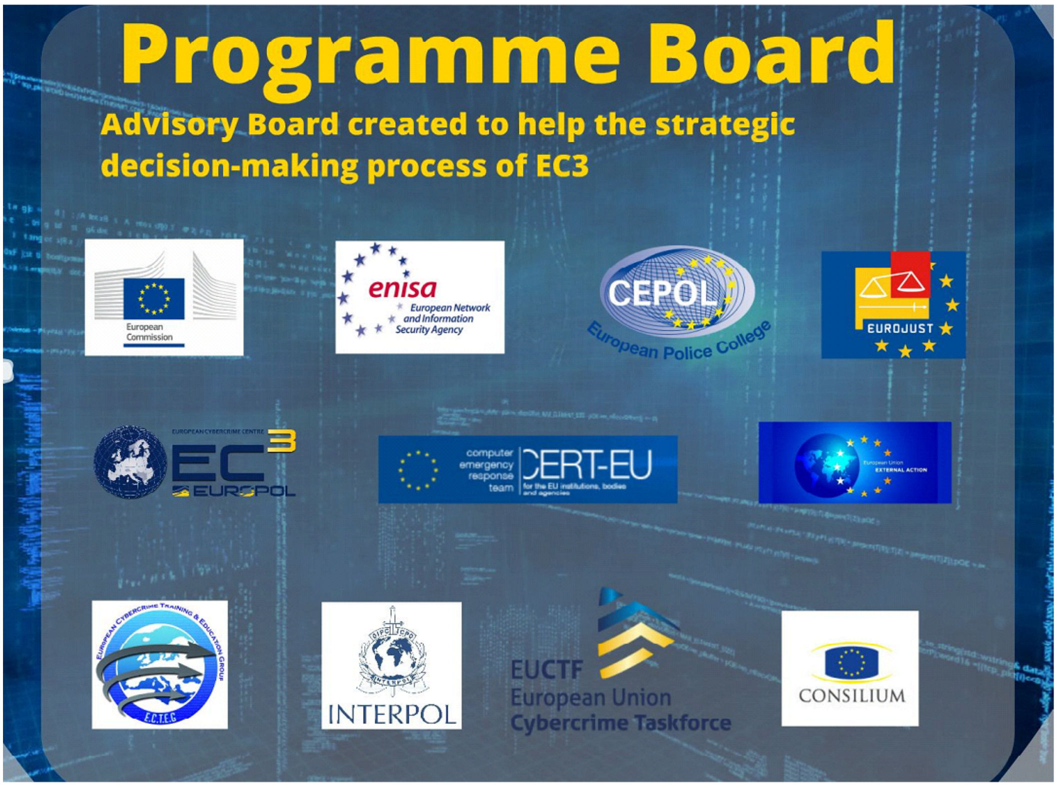
Operational Analysis



Programme Board

Advisory Board created to help the strategic decision-making process of EC3

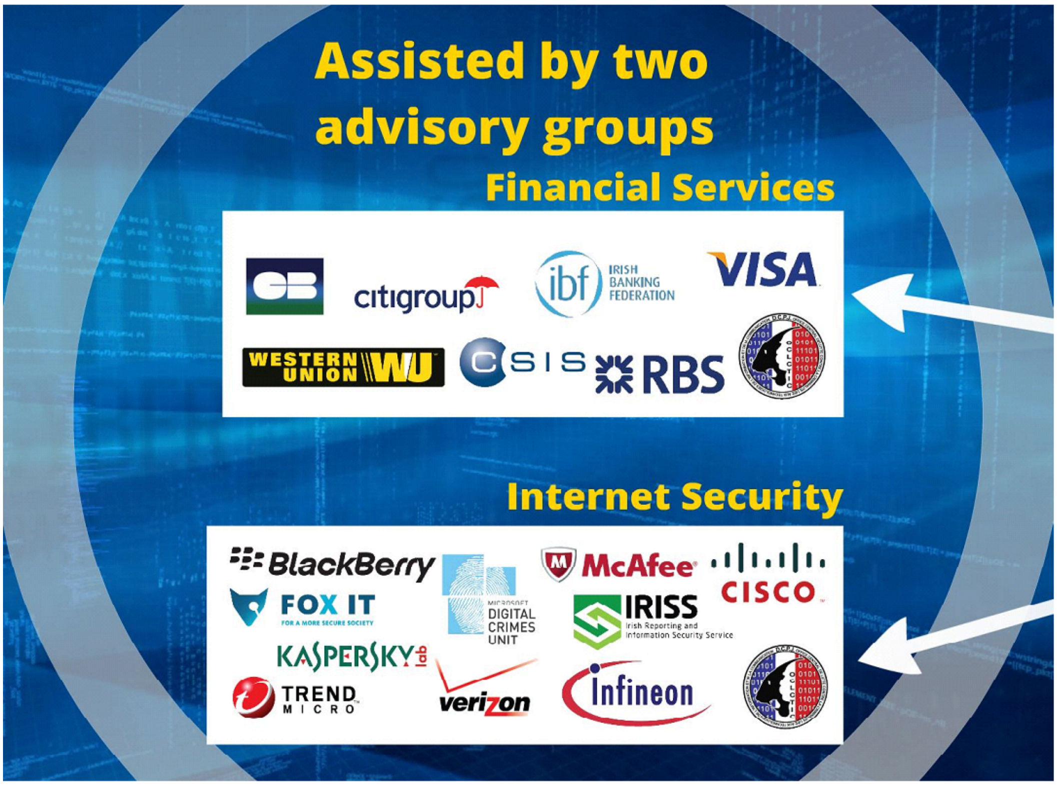
European Commission
enisa European Network and Information Security Agency
CEPOL European Police College
EUROJUST
EC3 EUROPOL
computer emergency response team CERT-EU for the EU institutions, bodies and agencies
European Union External Action
INTERPOL
EUCTF European Union Cybercrime Taskforce
CONSILIUM



Programme Board

Advisory Board created to help the strategic decision-making process of EC3

European Commission
enisa European Network and Information Security Agency
CEPOL European Police College
EUROJUST
EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL
computer emergency response team CERT-EU for the EU institutions, bodies and agencies
European Union External Action
European Cybercrime Training & Education Group E.C.T.E.G
INTERPOL
EUCTF European Union Cybercrime Taskforce
CONSILIUM



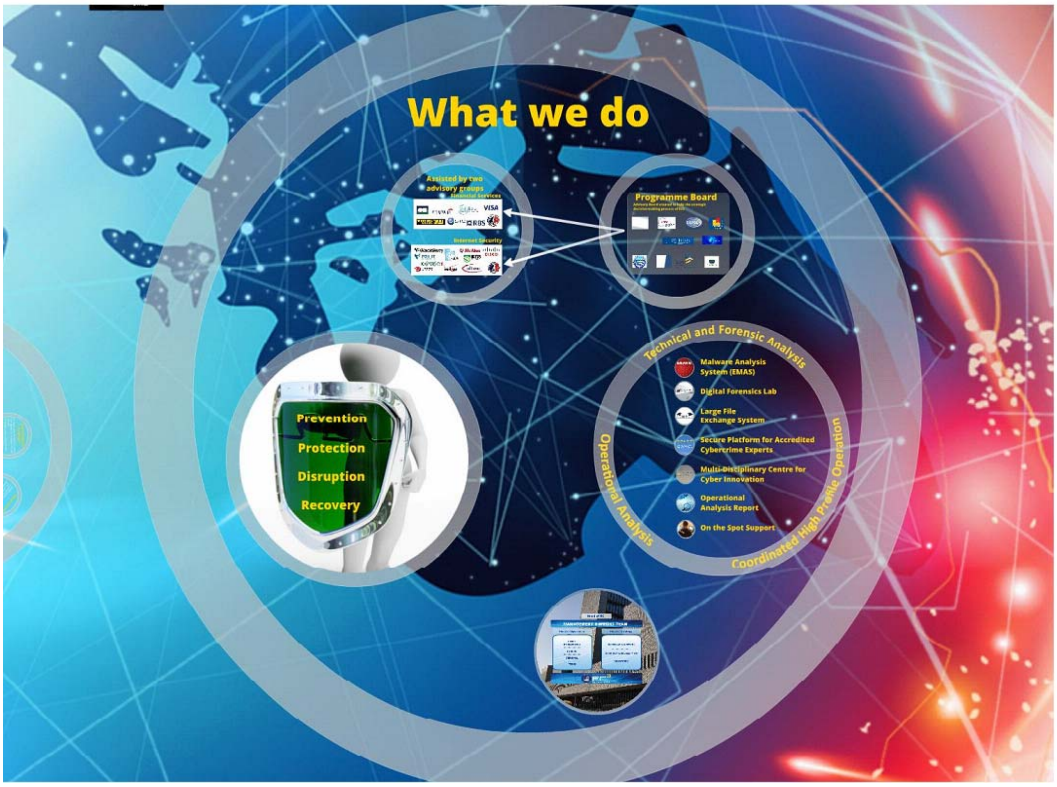
Assisted by two advisory groups

Financial Services

CB
citigroup
ibf IRISH BANKING FEDERATION
VISA
WESTERN UNION WU
CSIS
RBS

Internet Security

BlackBerry
FOX IT FOR A MORE SECURE SOCIETY
MICROSOFT DIGITAL CRIMES UNIT
McAfee
CISCO
IRISS Irish Reporting and Information Security Service
KASPERSKY lab
TREND MICRO
verizon
Infineon



What we do

Prevention

Protection

Disruption

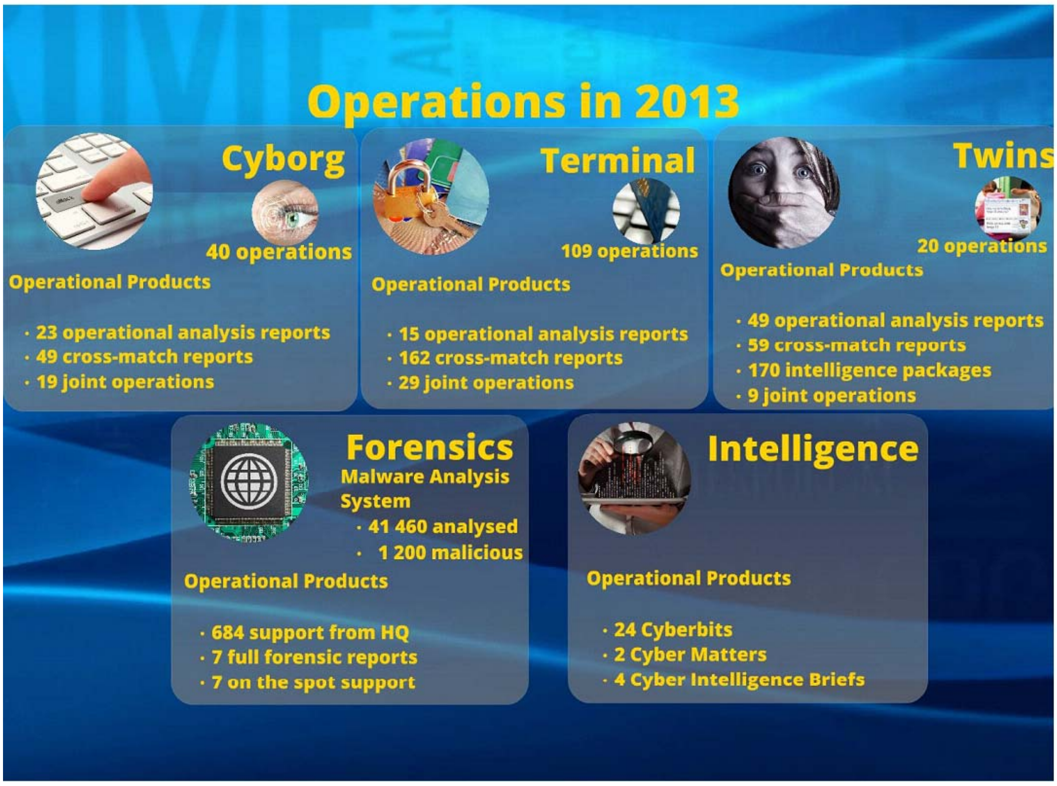
Recovery

Technical and Forensic Analysis

- Malware Analysis System (EMAS)
- Digital Forensics Lab
- Large File Exchange System
- Secure Platform for Accredited Cybercrime Experts
- Multi-Disciplinary Centre for Cyber Innovation
- Operational Analysis Report
- On the Spot Support

Operational Analysis

Coordinated High Profile Operation



Operations in 2013

Cyborg

40 operations

Operational Products

- 23 operational analysis reports
- 49 cross-match reports
- 19 joint operations

Terminal

109 operations

Operational Products

- 15 operational analysis reports
- 162 cross-match reports
- 29 joint operations

Twins

20 operations

Operational Products

- 49 operational analysis reports
- 59 cross-match reports
- 170 intelligence packages
- 9 joint operations

Forensics

Malware Analysis System

- 41 460 analysed
- 1 200 malicious

Operational Products

- 684 support from HQ
- 7 full forensic reports
- 7 on the spot support

Intelligence

Operational Products

- 24 Cyberbits
- 2 Cyber Matters
- 4 Cyber Intelligence Briefs

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Combating Crime in a Digital Age

Thank you

EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Combating Crime in a Digital Age

Thank you

Biography: Benoit Godart

Recently appointed as EUROPOL Head of Outreach & Support at the EC3, Benoit Godart served as Liaison Officer to INTERPOL, supporting the development of operational co-operation between these organisations in the fight against Organised Crime and Terrorism. Prior to this posting, Benoit was seconded by the French Customs Authority to EUROPOL to launch a pan-European project as the Head of the EUROPOL Intellectual Property Crime (IPC) team. Under his leadership since November 2005, supporting trans-national co-operation between Law Enforcement Agencies (LEAs) from European Union Member States and Europol's partners active in the IPC field, the team achieved major successes through several joint operations and co-ordinated actions on counterfeit commodities, piracy and counterfeit medicines.

Benoit is a graduate from the University of Bourgogne (France). He has two Master's degrees, one in Economics & Finances and one in Law. In 1991, he joined the French Customs Authority. From 1995 until 2002, he held the post of Head of National Investigation and Intelligence Units at the "Direction Nationale du Renseignement et des Enquetes Douanières" in Paris, Lille and Toulouse. During this time, his main assignment was to lead investigation teams with national competences targeting criminals involved in drugs trafficking, cigarette smuggling, counterfeiting and other illicit trafficking offences. This task involved technical and operational support, including the handling of informants and the organisation of operational matters, such as surveillance and the collection of evidence.

International co-operation was a significant element of these activities. As such, Benoit has been familiar with special police techniques and tools such as joint investigations, controlled deliveries and cross border surveillance with various LEAs in France and abroad. Promoted to Chief Superintendent in 2002, he was deployed as Chief of Customs in a French territorial department responsible for management and implementation of performance indicators. In 2010, Benoit was appointed as Director of Customs Services.

Michele Socco – European Commission

Fight against Cybercrime: a European perspective

Cybercrime is a multifaceted and still relatively new phenomenon; we still lack a comprehensive understanding of its size, but it seems clear that cybercrime carries very high indirect and defence costs.

It encompasses: traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems; the publication of illegal content over electronic media (e.g., child sexual abuse material or incitement to racial hatred); crimes unique to electronic networks, as for example, attacks against information systems, denial of service and hacking.

I. CHALLENGES

The very nature of cybercrime poses peculiar challenges to law enforcement:

- **Jurisdiction: Victims, criminals and evidence are not in the same country** - It happens seldom (if ever) that the victim of an on-line fraud or the child that has been abused to sell pedo-pornographic material on the Internet are in the same country of the perpetrators of these crimes. Organised crime networks are structured so to exploit legal loopholes and possible inefficiencies in some countries. Moreover, to build a case, investigators need to have access to evidence that very often is stored in another country, if not "in the cloud". Data in the clouds is constantly shifted from one server to the next, moving within or across different countries at any time. Also, data in the clouds might be mirrored for security and availability reasons, and therefore could be found in multiple locations within a country or in several separate countries. Due to this and to cached versions of data, not even the cloud computing provider might know where the sought-after data is exactly located (the so-called "loss of location").

- **Procedures are lengthy and cumbersome**, not adapted to cyber-investigations, where evidence can be lost, deleted and moved quickly from one country to another.

- **Lack of expertise and know-how**: Law enforcement authorities, as well as the judiciary, are still building their expertise in the field. There is often need for training and for adapted technical tools.

- **Building political consensus on the interaction between security and freedom** – Such consensus does not yet exist at EU level (as by the way it does not seem to exist within most of our Member States) and this has led to the need to deal with the problem for each policy proposal in this field.

II. THE EU POLICY RESPONSE

- *Building a consistent Cybersecurity Strategy, encompassing cybercrime*
  EU Member States should make cyber security a priority and work towards achieving a comparable level of capabilities.

  They should engage with each other and with other relevant stakeholders, including in particular the private sector, which plays a key role as the main owner of cyber infrastructure.

  The EU Council endorsed the comprehensive and integrated Cyber Security Strategy that the Commission tabled in February 2013.

  The strategy pursues the overall objective to put in place a robust line of defence against cyber incidents.

  It focuses on the need to improve the overall resilience of network and information systems, stepping up the fight against cybercrime and developing an external EU cyber security policy.

- *Adapting the legal framework and generating a common understanding of the issues*:

  a) the EU has adopted relevant rules against cyber attacks (the Directive on attacks against information systems was adopted in August 2013), providing for an harmonisation of the definition of certain crimes (e.g. the use of botnets, devices to remotely control others' computers and trigger cyber attacks) and related penalties

  b) the Directive on the sexual abuse and sexual exploitation of children and child pornography adopted in December 2011 provides for the harmonisation of the definition and of the level of penalties of a number of offences related to the use of the internet for criminal purposes (diffusion, downloading and viewing child pornography, grooming, use of webcams, …)

- *Enhancing cooperation among law enforcement authorities*: the European Cybercrime Centre (EC3) within Europol has opened its doors in January and is the focal point in the fight against cybercrime in the Union:
  - it provides support to Member States' cybercrime investigations;
  - it can serve as the European cybercrime information focal point;
  - it should pool European cybercrime expertise to support Member States.
  - Further functions of the Centre will include the strengthening of forensic law enforcement capabilities for cybercrime investigations.

- *Providing training and tools*: The EU funding for Cybercrime Centres of Excellence supports the development of national cybercrime capabilities in training, research and education, based on public-private cooperation and across EU MS. To date, centres are operational in Ireland, France, Estonia and Belgium, and have been recently launched in Bulgaria, the Czech Republic, Greece, Poland, Spain, and the UK.

- *Boosting international cooperation beyond the EU borders*: The EU also strongly encourages Member States that have not yet done so to ratify and follow the principles of the Budapest Convention, which serves as the most efficient international instrument in addressing cyber threats

III. LOOKING AHEAD

- Cross-border cooperation between law enforcement bodies remains insufficient, whereas the deep roots of organised crime and its detrimental effects on the economy continue to challenge the EU.

- Citizens remain concerned about their security being put at risk by various specific threats such as possible terrorist attacks, serious crime or daily petty criminality and abuse of IT technologies (cybercrime) but they are also increasingly concerned by the protection of their privacy and personal data and tend to consider that these are put in danger when data are stored and used for security purposes.

- Well-established fundamental rights principles need to be re-thought to be properly applied to new technological developments.

- "Privacy by design" is a key concept of the data protection reform currently under discussion. "Security by design" will also lead to better protection of privacy. Public opinion calls for an EU-wide discussion and setting standards, independently to (uncontested) competence limitations with regard to national security.

- In the area of cybercrime, where the offences involve unlawful processing of personal data and gross privacy violations (for instance in the cases of identity theft, data interception or child pornography), increased security and effective law enforcement are not opposite to privacy, but, on the contrary, security is a necessary means to safeguard privacy.

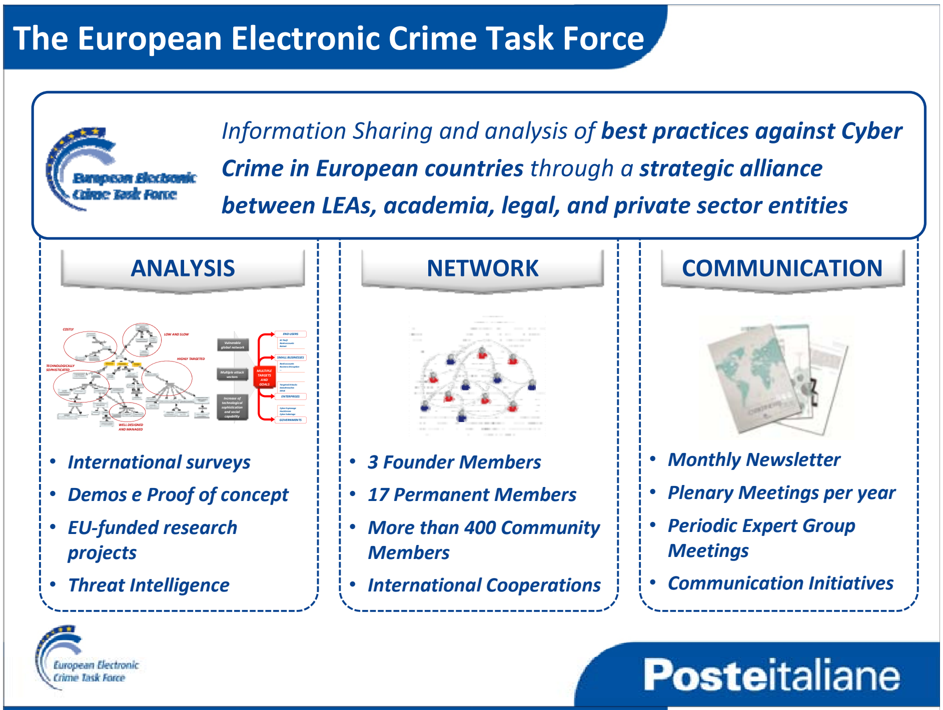
- Given that the Internet infrastructure is largely owned and managed by private actors, there is a patent need to cooperate with these actors for effective law enforcement. Through the establishment of Public-Private Partnerships, law enforcement agencies can incrementally increase the effectiveness of their action. At the same time, it is under the eyes of us all how the commitment of just a few large actors can improve the governance of the Internet: just as an example, the stance taken by Google enhancing the filtering of websites containing child pornography in the search engine dramatically decreases the opportunity to find child sexual abuse material on the open Internet.

- In the area of cybercrime, the number of highly skilled offenders is relatively small; moreover, it is widely accepted that security measures can deter opportunistic crime but cannot withstand a targeted attack. As a result, repression – meaning effective investigation and prosecution, and deterrent sanctions have to go hand in hand with prevention in this domain.

Biography: Michele Socco

Michele Socco is policy officer at the European Commission's Directorate-General Home Affairs, member of the cybercrime team in the unit "Fight against organized crime and relations with EMCDDA". Prior to his current appointment, he was policy assistant in the personal office of Ms Maria Damanaki, Commissioner for Maritime Affairs and Fisheries, and worked for six years as communication officer in the European Commission's Directorate-General for Justice, Freedom and Security. Before joining the European Commission, he was political assistant to Professor Gianni Vattimo, Member of the LIBE Committee of European Parliament. He studied political sciences in Italy and European policies at the Institut d'Études Européennes of the Université Libre de Bruxelles.

Stefano Grassi - European Electronic Crime Task Force (presentation given by Matteo Lucchetti, EECTF)



The European Electronic Crime Task Force

*Information Sharing and analysis of **best practices against Cyber Crime in European countries** through a **strategic alliance between LEAs, academia, legal, and private sector entities***

ANALYSIS

- *International surveys*
- *Demos e Proof of concept*
- *EU-funded research projects*
- *Threat Intelligence*

NETWORK

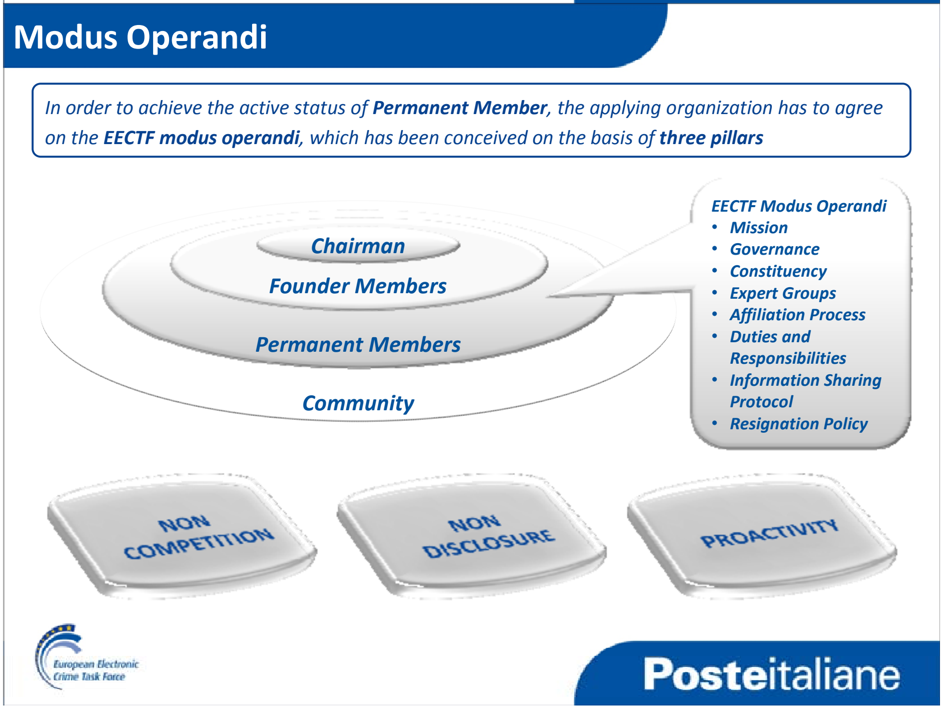
- *3 Founder Members*
- *17 Permanent Members*
- *More than 400 Community Members*
- *International Cooperations*

COMMUNICATION

- *Monthly Newsletter*
- *Plenary Meetings per year*
- *Periodic Expert Group Meetings*
- *Communication Initiatives*

European Electronic Crime Task Force

Posteitaliane



Modus Operandi

*In order to achieve the active status of **Permanent Member**, the applying organization has to agree on the **EECTF modus operandi**, which has been conceived on the basis of **three pillars***

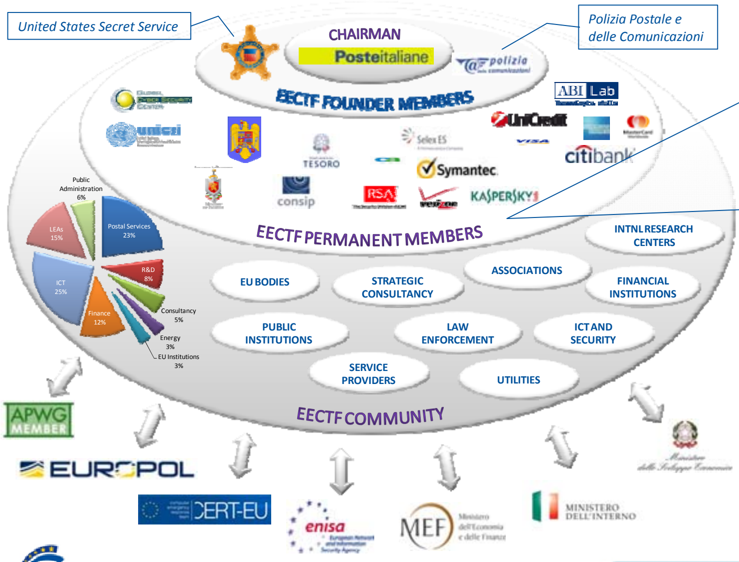
EECTF Modus Operandi

- *Mission*
- *Governance*
- *Constituency*
- *Expert Groups*
- *Affiliation Process*
- *Duties and Responsibilities*
- *Information Sharing Protocol*
- *Resignation Policy*

European Electronic Crime Task Force

Posteitaliane

EECTF Membership



List of EECTF Permanent Members as of July 2013:

- *GCSEC*
- *UNICRI*
- *Bulgarian Police*
- *Romanian Police*
- *Italian Ministry of Economy and Finance*
- *Consip*
- *Selex ES*
- *CA*
- *Kaspersky*
- *NTTDATA*
- *RSA*
- *Symantec*
- *Verizon*
- *ABI Lab*
- *Citibank*
- *Unicredit*
- *American Express*
- *Mastercard*
- *VISA Europe*

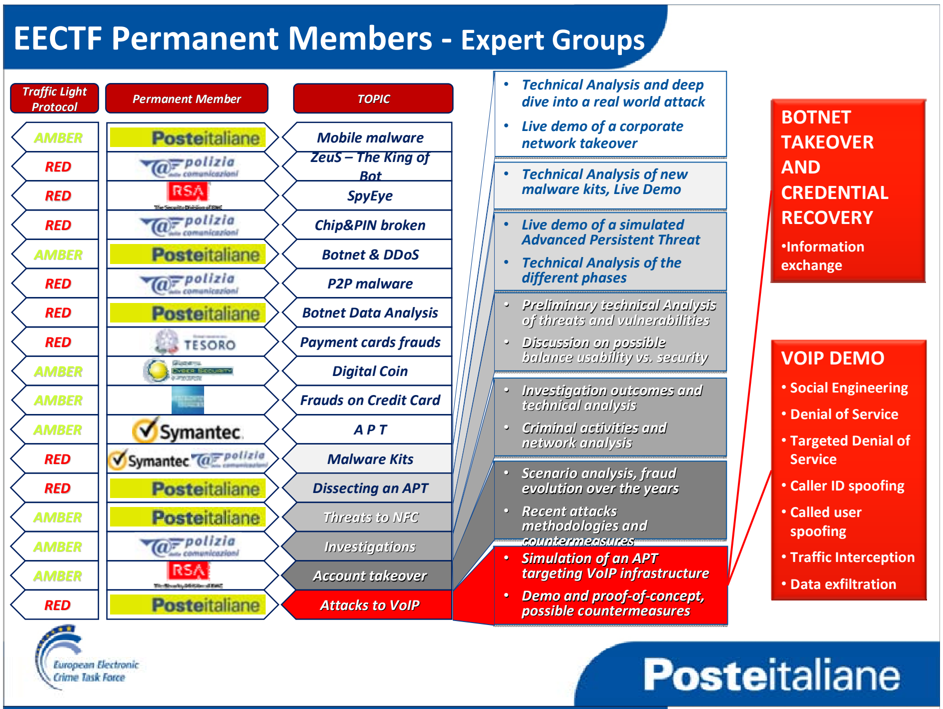
EECTF Community

- An **invitation-only extended Community**, made up of **acknowledged experts and organizations** involved in prevention and contrast of electronic crime, is invited to **three Plenary Meetings per year**
- **Past speakers** include: *European Commission, ENISA, CERT-EU, Europol, European Payments Council, the AntiPhishing Working Group, UNICRI, US Ambassador to Italy, USSS, Italian Data Protection Authority, Italian Ministry of Finance, Italian Ministry of Internal Affairs*
- A **monthly newsletter** is published within the Community to sketch the **most relevant trends in cyber crime**

- **NEXT PLENARY MEETING – February 2013**
  SECURING THE CLOUD

PLENARY MEETINGS

Feb 2011	Trends in Cybercrime and Cyberthreats: Europe and US	91 attendees 35 organizations
May 2011	Identity Theft: Malware, Botnet & Social Networking	98 attendees 38 organizations
Nov 2011	Cyber Crime Underground Economy	108 attendees 40 organizations
Mar 2012	Advanced Persistent Threats	108 attendees 38 organizations
Jul 2012	Secure Identities in Cyber Space	145 attendees 47 organizations
Nov 2012	Security of Innovative Payment Systems	150 attendees 51 organizations
Apr 2013	CERTs and international cooperation networks	165 attendees 52 organizations
Nov 2013	Security of Internet Payments and Digital Services	174 attendees 53 organizations



EECTF Permanent Members - Expert Groups

Traffic Light Protocol	Permanent Member	TOPIC
AMBER	Posteitaliane	Mobile malware
RED	polizia delle comunicazioni	ZeuS – The King of Bot
RED	RSA The Security Division of EMC	SpyEye
RED	polizia delle comunicazioni	Chip&PIN broken
AMBER	Posteitaliane	Botnet & DDoS
RED	polizia delle comunicazioni	P2P malware
RED	Posteitaliane	Botnet Data Analysis
RED	TESORO	Payment cards frauds
AMBER	Global Cyber Security	Digital Coin
AMBER		Frauds on Credit Card
AMBER	Symantec	A P T
RED	Symantec polizia delle comunicazioni	Malware Kits
RED	Posteitaliane	Dissecting an APT
AMBER	Posteitaliane	Threats to NFC
AMBER	polizia delle comunicazioni	Investigations
AMBER	RSA The Security Division of EMC	Account takeover
RED	Posteitaliane	Attacks to VoIP

- *Technical Analysis and deep dive into a real world attack*
- *Live demo of a corporate network takeover*

- *Technical Analysis of new malware kits, Live Demo*

- *Live demo of a simulated Advanced Persistent Threat*
- *Technical Analysis of the different phases*

- *Preliminary technical Analysis of threats and vulnerabilities*
- *Discussion on possible balance usability vs. security*

- *Investigation outcomes and technical analysis*
- *Criminal activities and network analysis*

- *Scenario analysis, fraud evolution over the years*
- *Recent attacks methodologies and countermeasures*

- *Simulation of an APT targeting VoIP infrastructure*
- *Demo and proof-of-concept, possible countermeasures*

BOTNET TAKEOVER AND CREDENTIAL RECOVERY

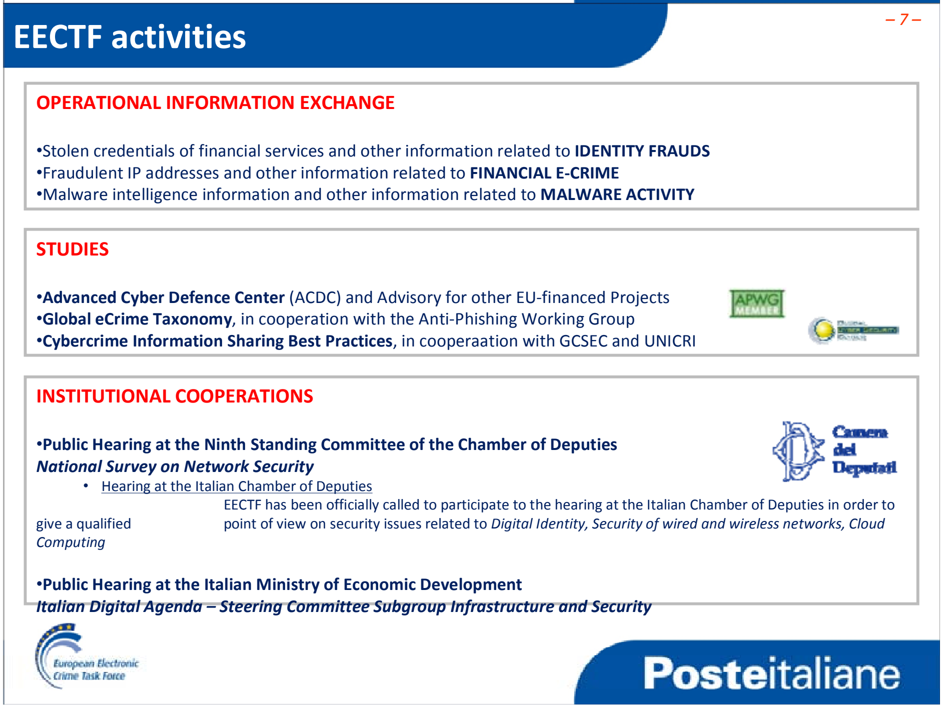
•Information exchange

VOIP DEMO

- Social Engineering
- Denial of Service
- Targeted Denial of Service
- Caller ID spoofing
- Called user spoofing
- Traffic Interception
- Data exfiltration

European Electronic Crime Task Force

Posteitaliane



EECTF activities

OPERATIONAL INFORMATION EXCHANGE

•Stolen credentials of financial services and other information related to **IDENTITY FRAUDS**
•Fraudulent IP addresses and other information related to **FINANCIAL E-CRIME**
•Malware intelligence information and other information related to **MALWARE ACTIVITY**

STUDIES

•**Advanced Cyber Defence Center** (ACDC) and Advisory for other EU-financed Projects
•**Global eCrime Taxonomy**, in cooperation with the Anti-Phishing Working Group
•**Cybercrime Information Sharing Best Practices**, in cooperaation with GCSEC and UNICRI

APWG MEMBER

INSTITUTIONAL COOPERATIONS

•**Public Hearing at the Ninth Standing Committee of the Chamber of Deputies**
National Survey on Network Security

- Hearing at the Italian Chamber of Deputies

EECTF has been officially called to participate to the hearing at the Italian Chamber of Deputies in order to give a qualified point of view on security issues related to *Digital Identity, Security of wired and wireless networks, Cloud Computing*

Camera dei Deputati

•**Public Hearing at the Italian Ministry of Economic Development**
Italian Digital Agenda – Steering Committee Subgroup Infrastructure and Security

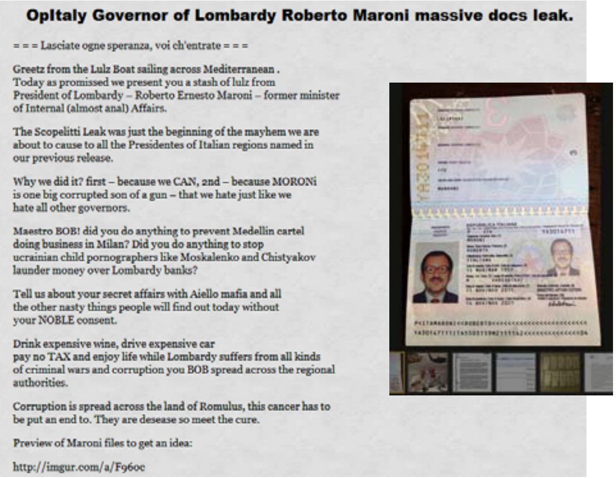
European Electronic Crime Task Force

Posteitaliane

Emerging trends in cybercrime scenario

– 7 –

MASSIFICATION OF **HACKTIVISM** CAMPAIGNS AGAINST VARIOUS TARGETS



OpItaly Governor of Lombardy Roberto Maroni massive docs leak.

= = = Lasciate ogne speranza, voi ch'entrate = = =

Greetz from the Lulz Boat sailing across Mediterranean .
Today as promissed we present you a stash of lulz from
President of Lombardy – Roberto Ernesto Maroni – former minister
of Internal (almost anal) Affairs.

The Scopelitti Leak was just the beginning of the mayhem we are about to cause to all the Presidentes of Italian regions named in our previous release.

Why we did it? first – because we CAN, 2nd – because MORONi is one big corrupted son of a gun – that we hate just like we hate all other governors.

Maestro BOB! did you do anything to prevent Medellin cartel doing business in Milan? Did you do anything to stop ucrainian child pornographers like Moskalenko and Chistyakov launder money over Lombardy banks?

Tell us about your secret affairs with Aiello mafia and all the other nasty things people will find out today without your NOBLE consent.

Drink expensive wine, drive expensive car
pay no TAX and enjoy life while Lombardy suffers from all kinds of criminal wars and corruption you BOB spread across the regional authorities.

Corruption is spread across the land of Romulus, this cancer has to be put an end to. They are desease so meet the cure.

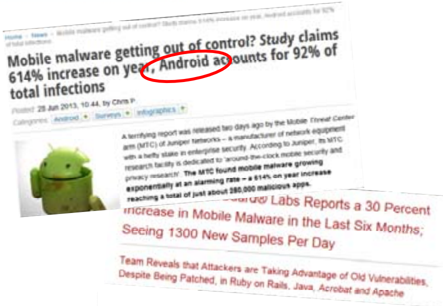
Preview of Maroni files to get an idea:

http://imgur.com/a/F960c

Emerging trends in cybercrime scenario

– 7 –

CONTINUOUS **INCREASE OF (MOBILE) MALWARE** → NEW DETECTION TECHNIQUES



Mobile malware getting out of control? Study claims 614% increase on year, Android accounts for 92% of total infections

Posted: 28 Jun 2013, 10:44, by Chris P.

Categories: Android, Surveys, infographics

A terrifying report was released two days ago by the Mobile Threat Center arm (MTC) of Juniper Networks – a manufacturer of network equipment with a hefty stake in enterprise security. According to Juniper, its MTC research facility is dedicated to "around-the-clock mobile security and privacy research". **The MTC found mobile malware growing exponentially at an alarming rate – a 614% on year increase reaching a total of just about 280,000 malicious apps.**

Labs Reports a 30 Percent Increase in Mobile Malware in the Last Six Months; Seeing 1300 New Samples Per Day

Team Reveals that Attackers are Taking Advantage of Old Vulnerabilities, Despite Being Patched, in Ruby on Rails, Java, Acrobat and Apache

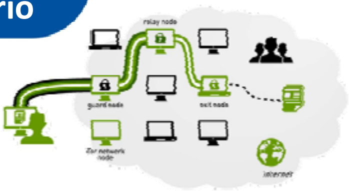
October 2013 malware statistics

Last month we analyzed **more than 5,7 million new malware samples**.
These 5.715.896 new samples, with a total size of 3,8 TB, can be categorized as:

- **Windows PE32 samples: 4.530.984**
- Windows PE32+ (64-bit) samples: 29.427
- Apple Mac Mach-O samples: 30
- Linux ELF samples: 673
- **Android samples: 148.986**
- **iPhone (ipa) samples: 6**
- **Blackberry samples: 1**
- Symbian samples: 93
- PDF samples: 6.319
- Office samples: 8.905
- Macromedia Flash samples: 367
- Java samples: 23.286
- boot sector samples: 5.804

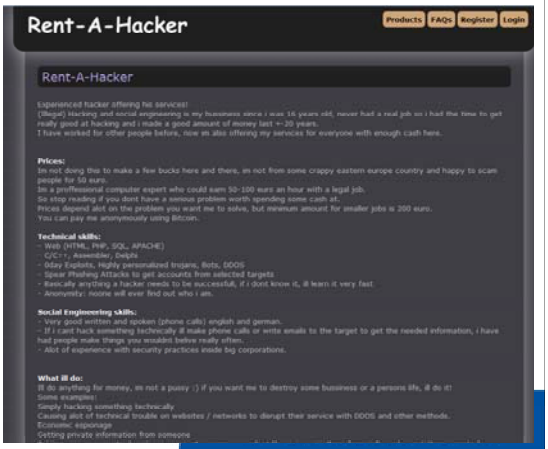
Emerging trends in cybercrime scenario

– 7 –



TOR/ DEEP WEB/ INVISIBLE INTERNET AS A SUPPORT TO CRIMINAL ACTIVITIES AND UNDERGROUND ECONOMY

- **Silk Road**
- **Murder-For-Hire**
- **Financial fraud tools**
  (ATM skimmers, stolen credentials, credit card numbers, etc.)
- …



Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.
Im a proffessional computer expert who could earn 50-100 eurs an hour with a legal job.
So stop reading if you dont have a serious problem worth spending some cash at.
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

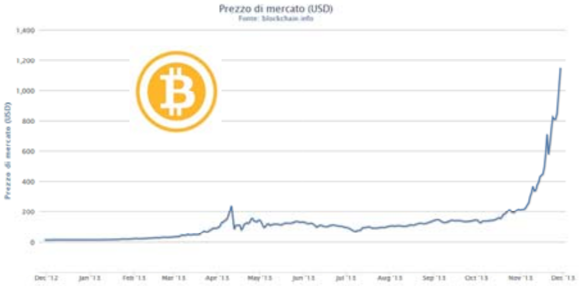
Social Engineering skills:
- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt belive really often.
- Alot of experience with security practices inside big corporations.

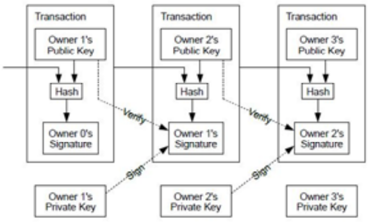
What ill do:
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone

Emerging trends in cybercrime scenario

– 7 –

- **EASY TO USE**
- **ANONYMOUS**
- (ALMOST) INSTANTANEOUS
- RELIABLE
- IRREVOCABLE
- NEAR-ZERO TRANSACTION FEES
- **NO CENTRAL AUTHORITY**





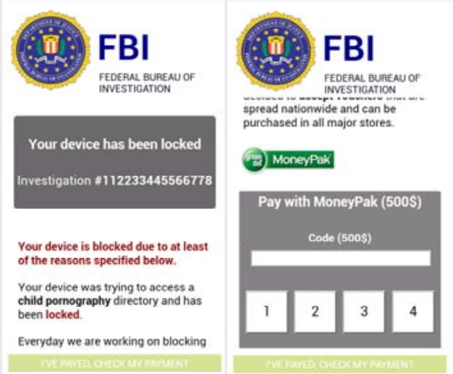
VIRTUAL CURRENCIES AS THE OFFICIAL CURRENCY FOR CYBERCRIME UNDERGROUND ECONOMY

Emerging trends in cybercrime scenario

– 7 –

- Increase in **MALWARE SPAM** activities against non-financial organizations
- **SPEAR PHISHING** attacks against specific non technical functions
- More and more attacks against **Public Administration**
- **RANSOMWARE** on a sharp rise → Cryptolocker, web and mobile
- 2.0 tools to manage **BOTNETS** via micro-blogging

PROLIFERATION OF CLASSICAL SCHEMES AND **SOCIAL ENGINEERING ATTACKS**



FBI
FEDERAL BUREAU OF INVESTIGATION

Your device has been locked

Investigation #112233445566778

Your device is blocked due to at least of the reasons specified below.

Your device was trying to access a **child pornography** directory and has been locked.

Everyday we are working on blocking

I'VE PAYED, CHECK MY PAYMENT

FBI
FEDERAL BUREAU OF INVESTIGATION

spread nationwide and can be purchased in all major stores.

Pay with MoneyPak (500$)

Code (500$)

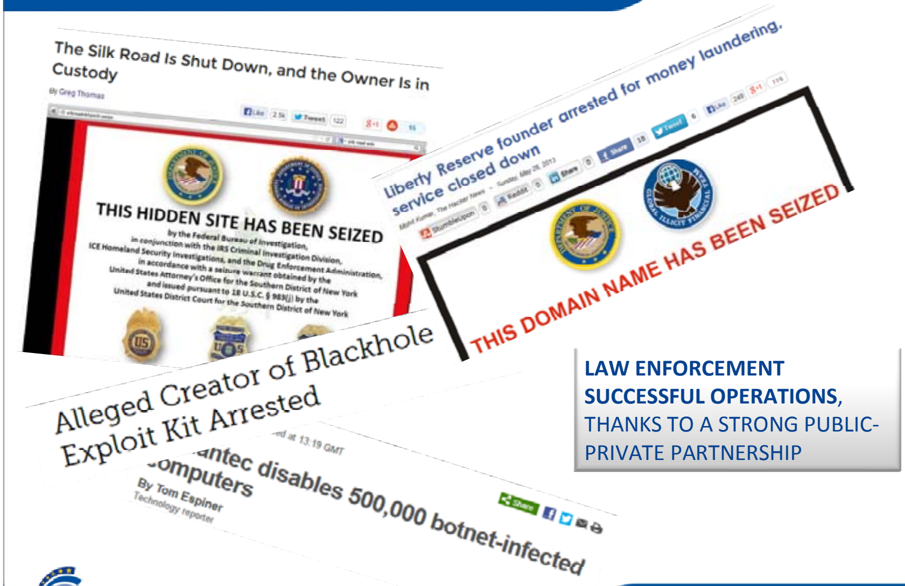
I'VE PAYED, CHECK MY PAYMENT

European Electronic Crime Task Force

Posteitaliane

Emerging trends in cybercrime scenario

– 7 –



The Silk Road Is Shut Down, and the Owner Is in Custody

By Greg Thomas

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Liberty Reserve founder arrested for money laundering, service closed down

THIS DOMAIN NAME HAS BEEN SEIZED

Alleged Creator of Blackhole Exploit Kit Arrested

…ed at 13:19 GMT

…antec disables 500,000 botnet-infected …omputers

By Tom Espiner
Technology reporter

LAW ENFORCEMENT SUCCESSFUL OPERATIONS, THANKS TO A STRONG PUBLIC-PRIVATE PARTNERSHIP

European Electronic Crime Task Force

Posteitaliane

Information Sharing Best Practices

– 7 –

- Joint Research activity between **EECTF and UNICRI to define Information Sharing Best Practices and draw a first inventory of the Information Sharing initiatives at the European level,** along five main drivers

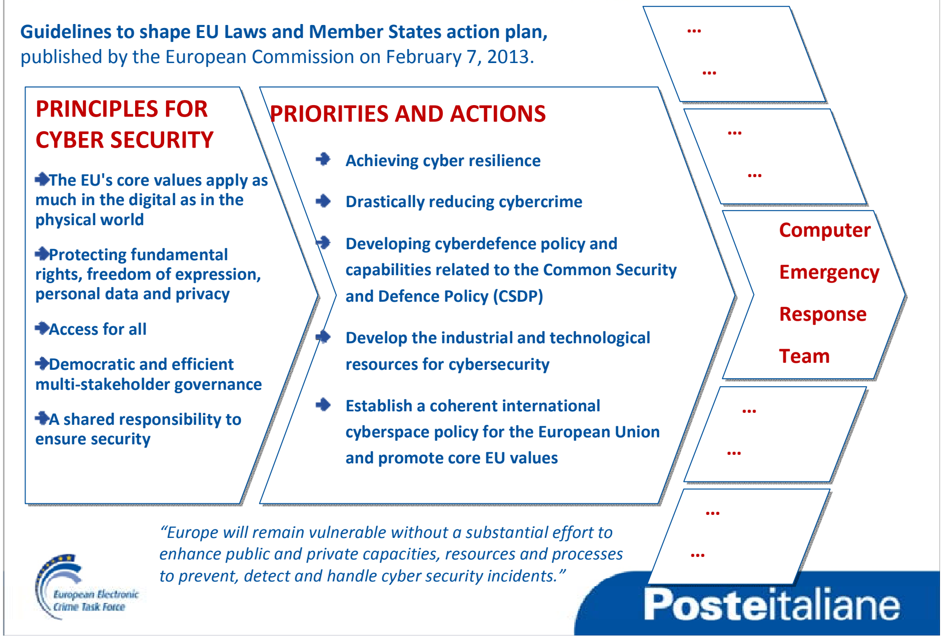
Macro Parameter	Parameters	
References	Name	
References	Acronymn	
References	Link	
References	Date of Birth	
Content	Mission	What is the mission of this information sharing initiative?
Content	Objectives	What are the objectives of the information sharing initiative
Content	Information shared (Topics)	Which topics are discussed, shared in this initiative?
Content	Number of members	How many organizations are involved?
Governance	Sponsorship/Patronage	There is a National Agency/Organization involved sponsorizing the initiative
Governance	Promoter	Who has been the promotere of the initiative
Governance	Constituency - Sectors	Utilities, PA, Military,National Agencies, International Organizations,…
Governance	Constituency - Public	Public, Private, Public/Private
Governance	Constituency - Membership	Professionals only, legal entities only, both
Governance	International law/regulation	There is an international law/regulation at the base of this initiative
Governance	National Law/regulation	There is a national law/regultation at the base of this initiative
Governance	Agreements	There is a formal agreement between members
Governance	Organizational structure (board, steering committee, etc.)	There is a formal organizational structure dealing with this initiative
Governance	Engagement	invitation only, restricted access on specific requirements, free access on a voluntary base, mandatory
Governance	Anonymization	possibility to be not identified and take anyway part to the information exchange
Governance	Trust	all-trust-one (centralized coordination), all-trust-all (distributed)
Governance	Formal subscription	There is a policy at the base of this initiative
Processes/Methodology of information sharing	Methodology of classification (confidentiality)	There is a mutual methodology to classify information
Processes/Methodology of information sharing	Exchange process	There is a defined process to share information
Modus Operandi	Tools for information exchange	mailing list, newsgroup, specific platform, web application, conference call, etc.
Modus Operandi	Physical Meetings	No meeting, sporadical meeting, periodical meeting (approximate frequency)
Modus Operandi	Online Meetings	No meeting, sporadical meeting, periodical meeting (approximate frequency)
Modus Operandi	Information flow	daily updates, weekly updates, monthly updates, sporadical, upon request, no exchange out of physical meetings

European Electronic Crime Task Force

The EU Cyber Security Strategy

– 5 –

Guidelines to shape EU Laws and Member States action plan,
published by the European Commission on February 7, 2013.



PRINCIPLES FOR CYBER SECURITY

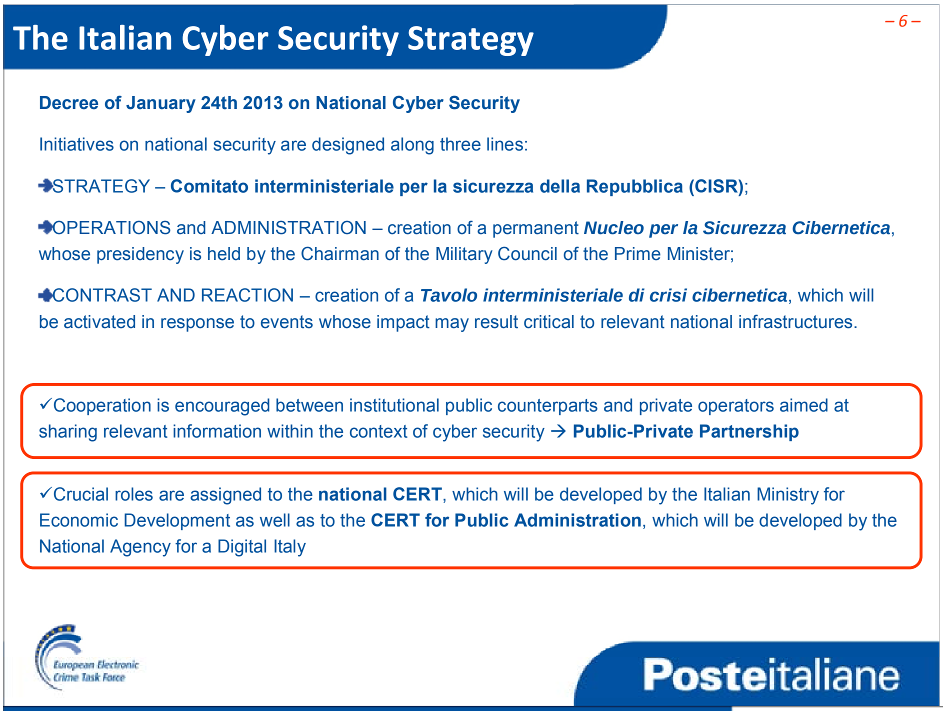
- **The EU's core values apply as much in the digital as in the physical world**
- **Protecting fundamental rights, freedom of expression, personal data and privacy**
- **Access for all**
- **Democratic and efficient multi-stakeholder governance**
- **A shared responsibility to ensure security**

PRIORITIES AND ACTIONS

- **Achieving cyber resilience**
- **Drastically reducing cybercrime**
- **Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)**
- **Develop the industrial and technological resources for cybersecurity**
- **Establish a coherent international cyberspace policy for the European Union and promote core EU values**

"Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents."

European Electronic Crime Task Force



– 6 –

The Italian Cyber Security Strategy

Decree of January 24th 2013 on National Cyber Security

Initiatives on national security are designed along three lines:

➧STRATEGY – **Comitato interministeriale per la sicurezza della Repubblica (CISR)**;

➧OPERATIONS and ADMINISTRATION – creation of a permanent ***Nucleo per la Sicurezza Cibernetica***, whose presidency is held by the Chairman of the Military Council of the Prime Minister;

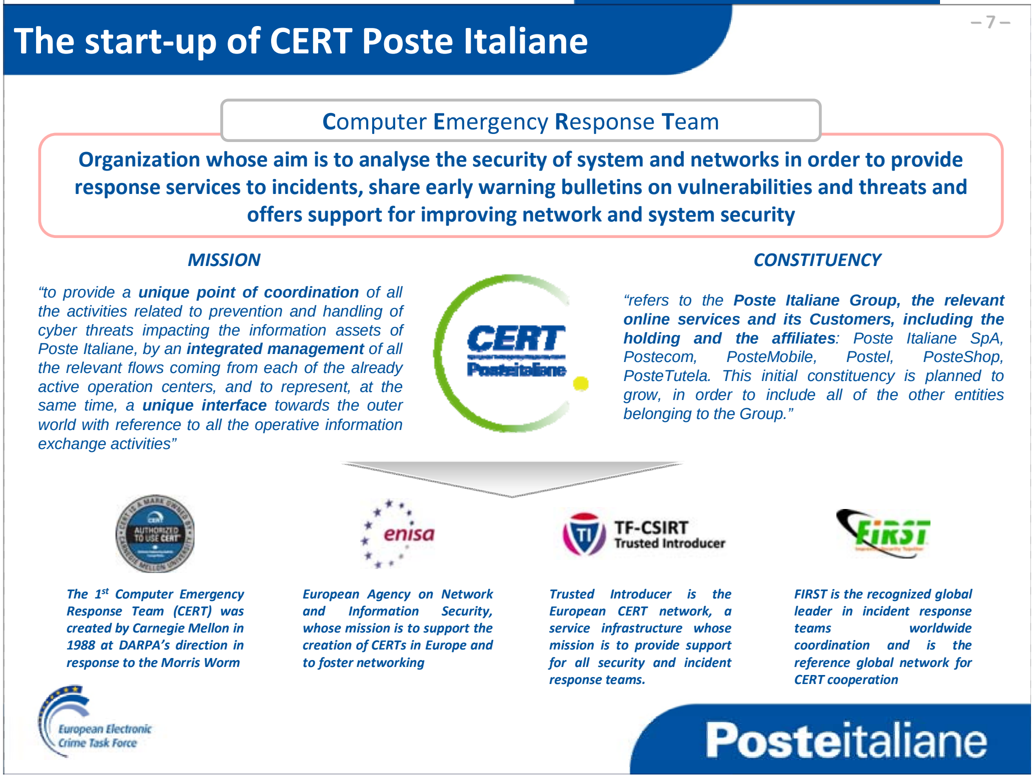
➧CONTRAST AND REACTION – creation of a ***Tavolo interministeriale di crisi cibernetica***, which will be activated in response to events whose impact may result critical to relevant national infrastructures.

✓Cooperation is encouraged between institutional public counterparts and private operators aimed at sharing relevant information within the context of cyber security → **Public-Private Partnership**

✓Crucial roles are assigned to the **national CERT**, which will be developed by the Italian Ministry for Economic Development as well as to the **CERT for Public Administration**, which will be developed by the National Agency for a Digital Italy

European Electronic Crime Task Force

Posteitaliane



– 7 –

The start-up of CERT Poste Italiane

Computer Emergency Response Team

Organization whose aim is to analyse the security of system and networks in order to provide response services to incidents, share early warning bulletins on vulnerabilities and threats and offers support for improving network and system security

MISSION

*"to provide a **unique point of coordination** of all the activities related to prevention and handling of cyber threats impacting the information assets of Poste Italiane, by an **integrated management** of all the relevant flows coming from each of the already active operation centers, and to represent, at the same time, a **unique interface** towards the outer world with reference to all the operative information exchange activities"*

CONSTITUENCY

*"refers to the **Poste Italiane Group, the relevant online services and its Customers, including the holding and the affiliates**: Poste Italiane SpA, Postecom, PosteMobile, Postel, PosteShop, PosteTutela. This initial constituency is planned to grow, in order to include all of the other entities belonging to the Group."*

The 1st Computer Emergency Response Team (CERT) was created by Carnegie Mellon in 1988 at DARPA's direction in response to the Morris Worm

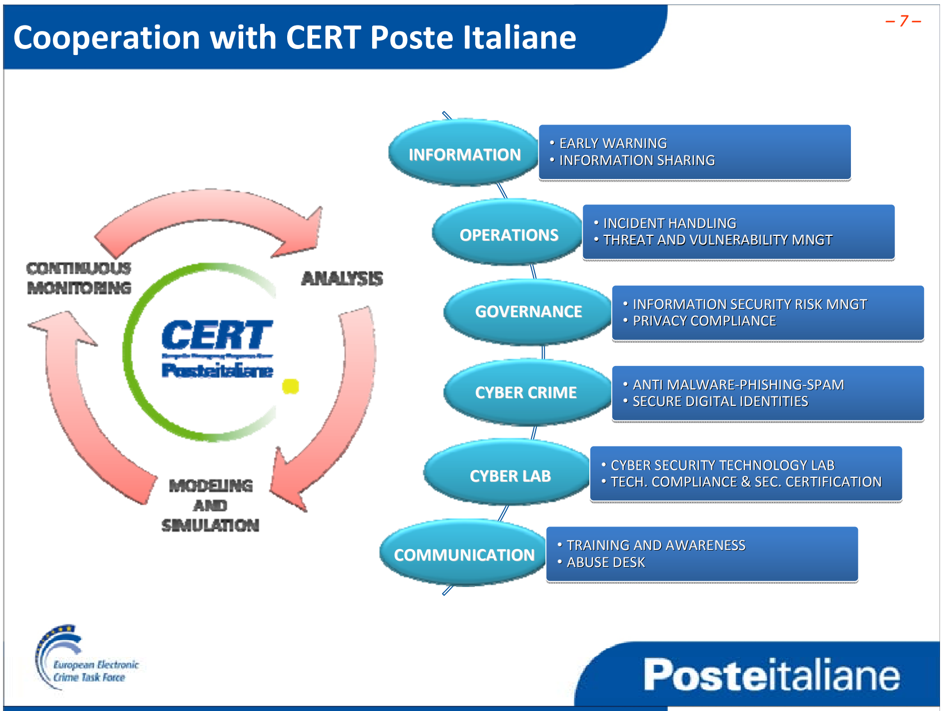
European Agency on Network and Information Security, whose mission is to support the creation of CERTs in Europe and to foster networking

Trusted Introducer is the European CERT network, a service infrastructure whose mission is to provide support for all security and incident response teams.

FIRST is the recognized global leader in incident response teams worldwide coordination and is the reference global network for CERT cooperation

European Electronic Crime Task Force

Posteitaliane



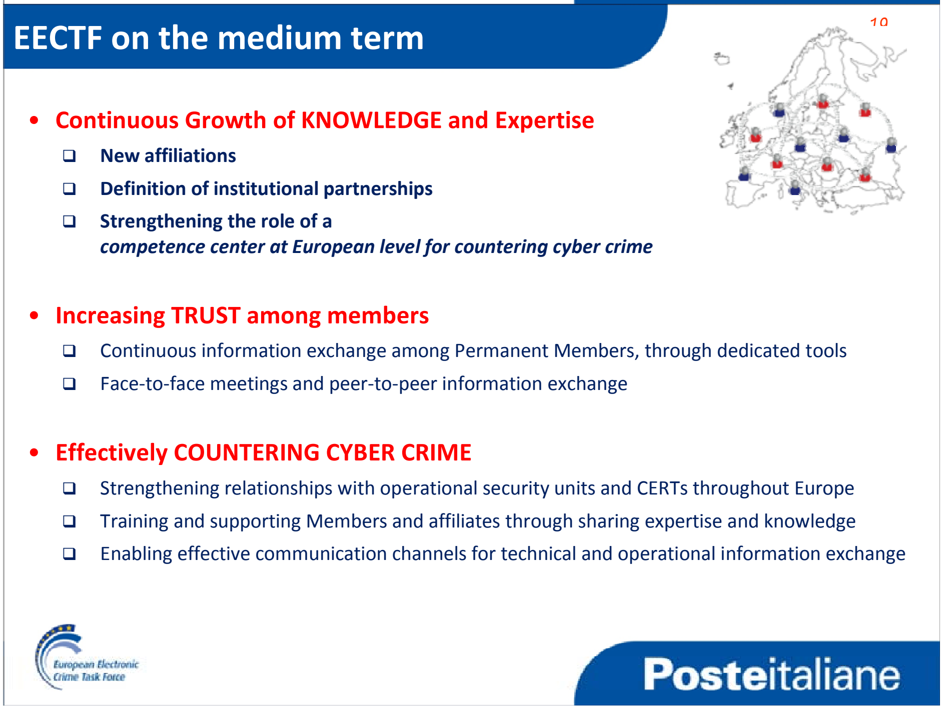
Cooperation with CERT Poste Italiane

– 7 –

- INFORMATION
  - EARLY WARNING
  - INFORMATION SHARING
- OPERATIONS
  - INCIDENT HANDLING
  - THREAT AND VULNERABILITY MNGT
- GOVERNANCE
  - INFORMATION SECURITY RISK MNGT
  - PRIVACY COMPLIANCE
- CYBER CRIME
  - ANTI MALWARE-PHISHING-SPAM
  - SECURE DIGITAL IDENTITIES
- CYBER LAB
  - CYBER SECURITY TECHNOLOGY LAB
  - TECH. COMPLIANCE & SEC. CERTIFICATION
- COMMUNICATION
  - TRAINING AND AWARENESS
  - ABUSE DESK

European Electronic Crime Task Force

Posteitaliane



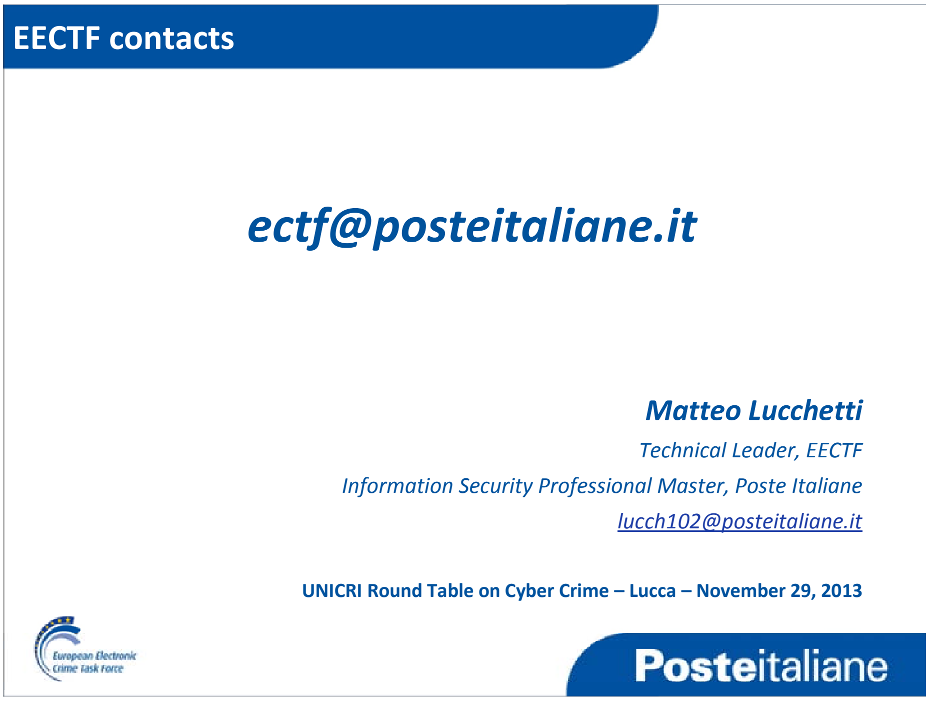
EECTF on the medium term

10

- **Continuous Growth of KNOWLEDGE and Expertise**
  - ❑ **New affiliations**
  - ❑ **Definition of institutional partnerships**
  - ❑ **Strengthening the role of a** ***competence center at European level for countering cyber crime***
- **Increasing TRUST among members**
  - ❑ Continuous information exchange among Permanent Members, through dedicated tools
  - ❑ Face-to-face meetings and peer-to-peer information exchange
- **Effectively COUNTERING CYBER CRIME**
  - ❑ Strengthening relationships with operational security units and CERTs throughout Europe
  - ❑ Training and supporting Members and affiliates through sharing expertise and knowledge
  - ❑ Enabling effective communication channels for technical and operational information exchange

European Electronic Crime Task Force

Posteitaliane



EECTF contacts

ectf@posteitaliane.it

Matteo Lucchetti

Technical Leader, EECTF

Information Security Professional Master, Poste Italiane

lucch102@posteitaliane.it

UNICRI Round Table on Cyber Crime – Lucca – November 29, 2013

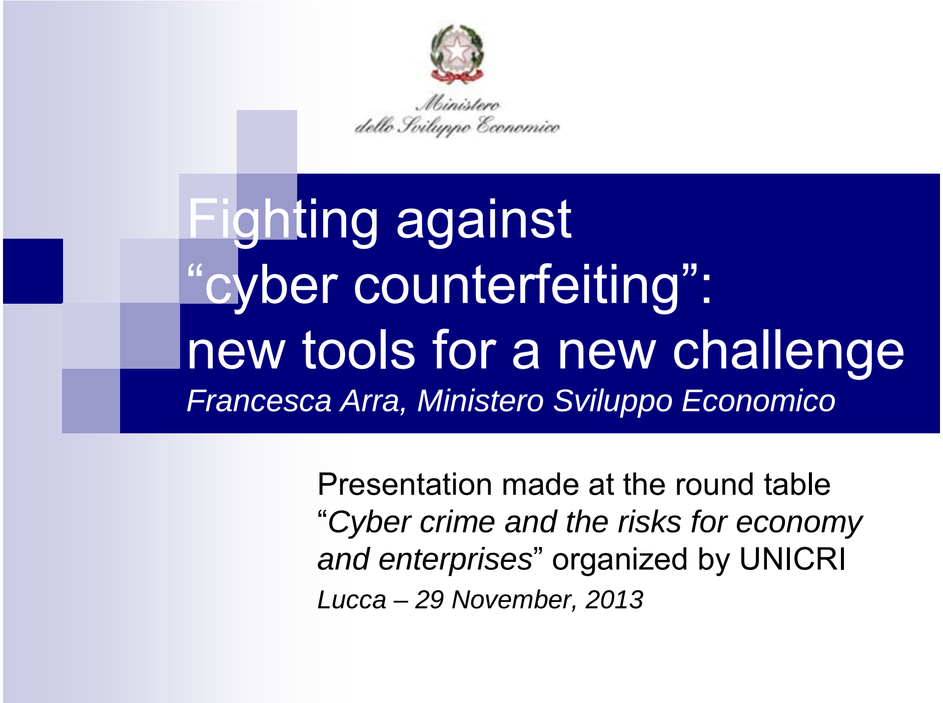
European Electronic Crime Task Force
Posteitaliane

Biography: Stefano Grassi

After more than twenty years of experience in the field of security, as Senior Officer of the Guardia di Finanza (holding the position of Commander of Regional Team of Tax Police of Lombardy with the rank of Colonel), Stefano Grassi was called in 2004 to direct the structure of Poste Italiane dedicated to the company protection. In the same year, he was appointed CEO of Poste Tutela, a Poste group society in charge of cash management and security.Graduated with honors in Law and in Science of Economic and Financial Security, he holds a Master in Corporate Tax Law from Bocconi University in Milan. He is licensed to practice law and he is the author of several publications in the field of law and in the field of security.

He is Chairman of the European Electronic Crime Task Force, an information sharing initiative born as a cooperation between Poste Italiane, United States Secret Service and Polizia Postale e delle Comunicazioni.

He is currently the President of Security Section of UNINDUSTRIA (Union of Industrialists and Enterprises) of Rome and also a member of Technical Confederal Committee “Salute e Sicurezza” of Confindustria. He attended numerous conferences as a speaker and he has held many teaching activities in the Tax field, corporate security and corporate liability, at the Tax Police School of the Guardia di Finanza, at LUMSA University in Rome, the University of Milano-Bicocca and other national and international universities.



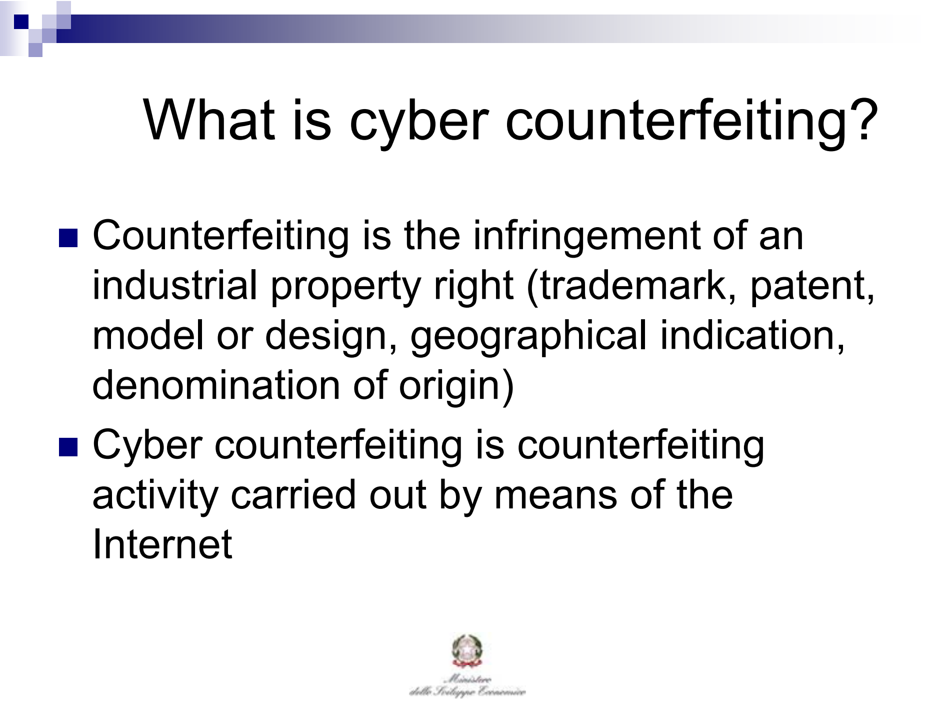
Ministero dello Sviluppo Economico

Fighting against "cyber counterfeiting": new tools for a new challenge

Francesca Arra, Ministero Sviluppo Economico

Presentation made at the round table "*Cyber crime and the risks for economy and enterprises*" organized by UNICRI

Lucca – 29 November, 2013



What is cyber counterfeiting?

- Counterfeiting is the infringement of an industrial property right (trademark, patent, model or design, geographical indication, denomination of origin)
- Cyber counterfeiting is counterfeiting activity carried out by means of the Internet

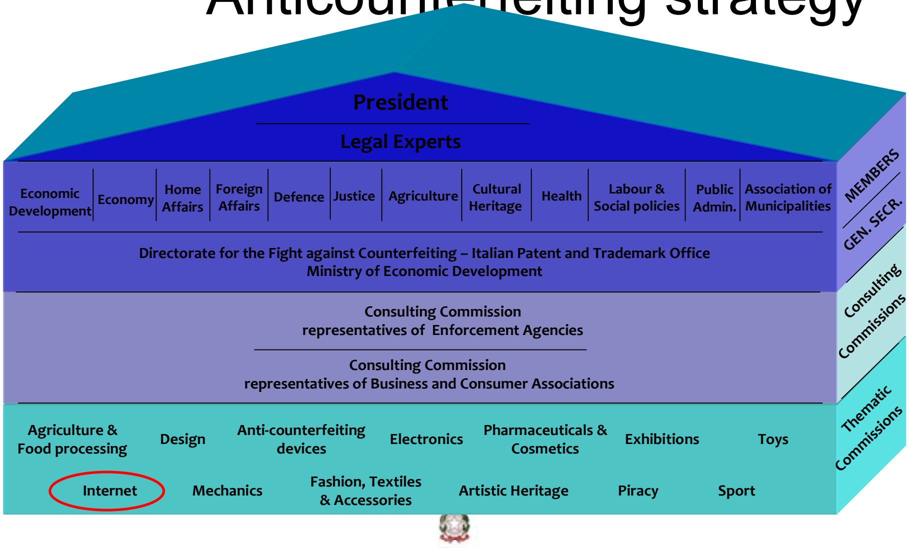
Ministero dello Sviluppo Economico

Anticounterfeiting policy and strategy

- Italian Ministry for Economic Development
  - □ DG for the fight against counterfeiting – Italian Patent and Trademark Office (DGLC-UIBM)
- National Anticounterfeiting Council (CNAC)

Ministero dello Sviluppo Economico

Anticounterfeiting strategy



President

Legal Experts

Economic Development	Economy	Home Affairs	Foreign Affairs	Defence	Justice	Agriculture	Cultural Heritage	Health	Labour & Social policies	Public Admin.	Association of Municipalities

Directorate for the Fight against Counterfeiting – Italian Patent and Trademark Office
Ministry of Economic Development

Consulting Commission
representatives of Enforcement Agencies

Consulting Commission
representatives of Business and Consumer Associations

Agriculture & Food processing — Design — Anti-counterfeiting devices — Electronics — Pharmaceuticals & Cosmetics — Exhibitions — Toys

Internet — Mechanics — Fashion, Textiles & Accessories — Artistic Heritage — Piracy — Sport

Ministero dello Sviluppo Economico

Counterfeiting affects consumers

- Health and safety risks related to fake...
  - □ Pesticides and Pharmaceuticals
  - □ Domestic appliances
  - □ Auto parts
  - □ Food and beverages
  - □ Toys
  - □ Body care products
  - □ Clothes, shoes, glasses
  - □ ……………

Ministero
dello Sviluppo Economico

Counterfeiting affects businesses

- Profit losses and decreasing margins
- Marketing investment devaluation
- Customer trust and business reputation erosion

Ministero
dello Sviluppo Economico

Counterfeiting affects economic systems

- Worldwide
  - □ US$1.7 trillion by 2015
    Estimating the global economic and social impacts of counterfeiting and piracy, ICC, 2011
    - International trade value: US$960 billion
    - Domestic production and consumption value: US$370-570 billion
    - Digitally pirated music, movies and software value: US$240 billion
    - Effects on government tax revenues, welfare spending, costs of crime on health services, FDI flows: US$125 billion
    - Employment losses in the G20 economies: 2.5 million jobs

- Italy
  - □ € 7 ca. billion turnover
    "Il fenomeno della contraffazione nel mondo e le ricadute sul mercato italiano: gli scenari e le strategie di contrasto" (Censis, 2012)
    - Tax revenue losses: € 4.6 billion
    - Job losses: 110,000 jobs

Counterfeiting affects nations

- Security risks
  - □ *Counterfeit milspec electronics easily bought online* - www.fiercegovernmentit.com, March 28, 2012
  - □ *Federal agencies launch "Operation Chain Reaction". Increased focus on counterfeit items entering the US government supply chain* - ICE news release, June 14, 2011

Again, what is cyber counterfeiting?

- **Cybersquatting**
  Registration, traffic or use of a domain name that is identical or confusingly similar to the name of another or a brand name
  - □ *Gucci Wins UDRP on 165 Domain Names* (5 June 2013)
    - all-gucci-japan.com
    - authenticguccioutletonline.net
    - bestgucciyahoo.com
    - guccihomedesign.com
    - yourmuguccihandbags.com
    - 2013freegucci-handbags.com
    - borse-gucciborse.com
    - ………………………

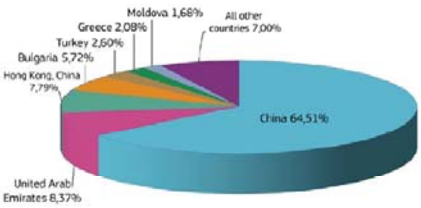
What is cyber counterfeiting?

- **Brand abuse in search engine marketing**
  Use of brand names as keywords to trigger ads diverting traffic to websites selling counterfeit goods
  - □ LVMH vs Google for violation of its trademarks related to Google AdWords system (2010)
- **SEO manipulation**
  Use of a company’s brand names, slogans or trademarks (by someone other than the legitimate owner) to affect search engine ranking
- **Selling of counterfeit goods on marketplaces**, auction sites, price comparison sites, retail store sites, independent sellers' sites

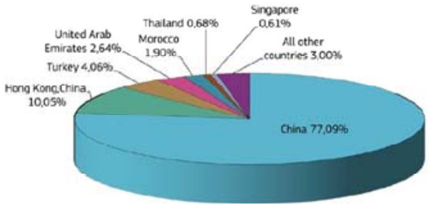
Who is to blame?

- Some countries more than others

Country of provenance by articles



Country of provenance by value



Source: *Report on EU customs enforcement of intellectual property rights. Results at EU border 2012*
European Commission, 2013

Who is to blame?

- Consumers?
- Businesses?
- Internet Service Providers!

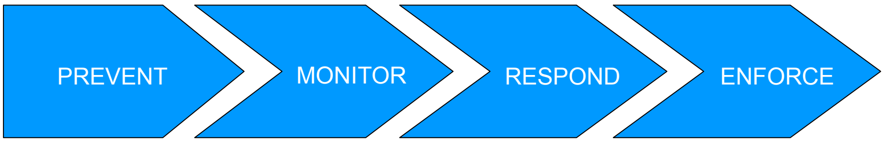
ISP liability

- E-commerce Directive (Directive 2000/31/EC)
  - ISPs are not liable for users' illegal activity providing that they have no actual knowledge of this illegal activity or, upon obtaining such knowledge, they act expeditiously to remove or to disable access information
  - No general obligation on ISPs to monitor the content which they transmit or store
  - No general obligation on ISPs to actively seek facts or circumstances indicating illegal activity

ISP liability

- Two famous cases:
  - □ LVMH vs Google
  - □ L’Oréal vs eBay
- ECJ guidelines
  - □ ISPs not liable
    - providing their role is of a mere technical, automatic and passive nature
    - under the condition that they expeditiously remove the infringing content
  - □ ISPs can be ordered to adopt measures to terminate an alleged infringement and to prevent future infringements

Business commitment



Business commitment

- Internet monitoring and enforcement strategy
  - □ **Monitoring sites**
    collects data available across different platforms: marketplaces, auction sites, price comparison sites, retail store sites, independent sellers' sites
  - □ **Processing collected data**
    based on a special algorythm, classifies results according to levels of danger of IPR infringement and for each brand and/or product allows you to know how many listings were found, in which sites they were found, in which geographical areas are servers located, ect.
  - □ **Responding**
    warning letters, C&D letters, take down notices, policy violation notices, UDRP procedures, enforcement actions, litigation)

Ministero dello Sviluppo Economico

Coming together to combat cyber counterfeiting

- EU Stakeholders' Dialogue: MoU on the sale of counterfeit goods via the Internet

BRANDS	adidas GROUP, BURBERRY, LACOSTE, LVMH, MATTEL, NIKE JUST DO IT, AMER SPORTS, GANT, LEGO, Microsoft, P&G, Unilever, RICHEMONT, NOKIA
SITES	MIH GROUP, ebay, PRICEMINISTER, amazon

Ministero dello Sviluppo Economico

Coming together to combat cyber counterfeiting

- EU Observatory Work Programme (2014-2018)
  - □ 5 Working Groups
    - Legal
    - Enforcement
    - Public Awareness
    - Statistics and Economics
    - IP in a Digital World

Ministero dello Sviluppo Economico

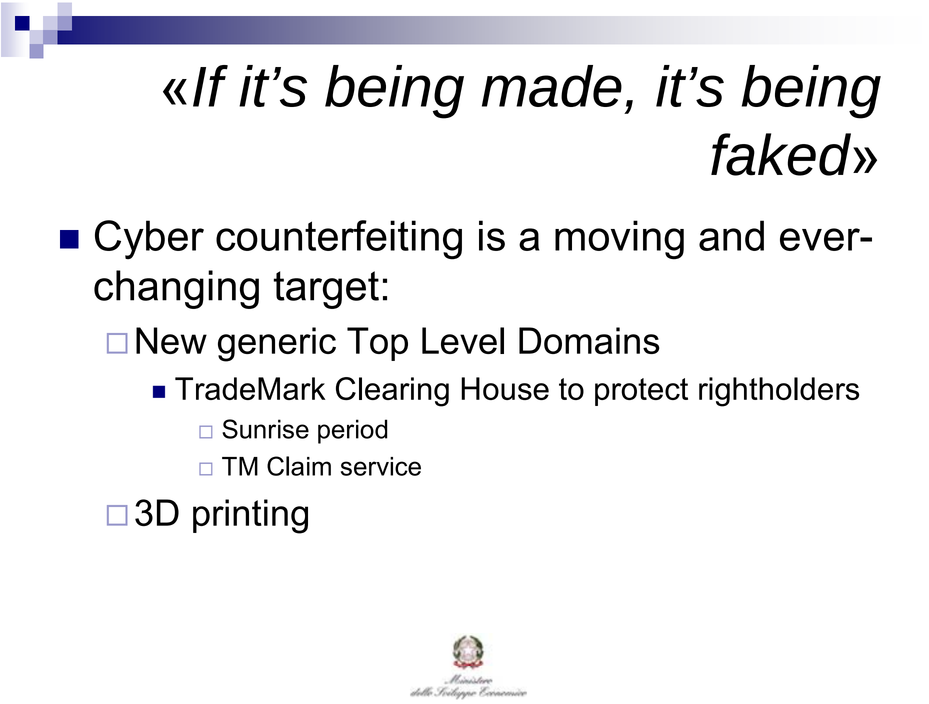
Coming together to combat cyber counterfeiting

- Italian National Anticounterfeiting strategic Plan

STATI GENERALI
Lotta alla Contraffazione
"Uniti nella lotta alla contraffazione"
Milan - November 19, 2012

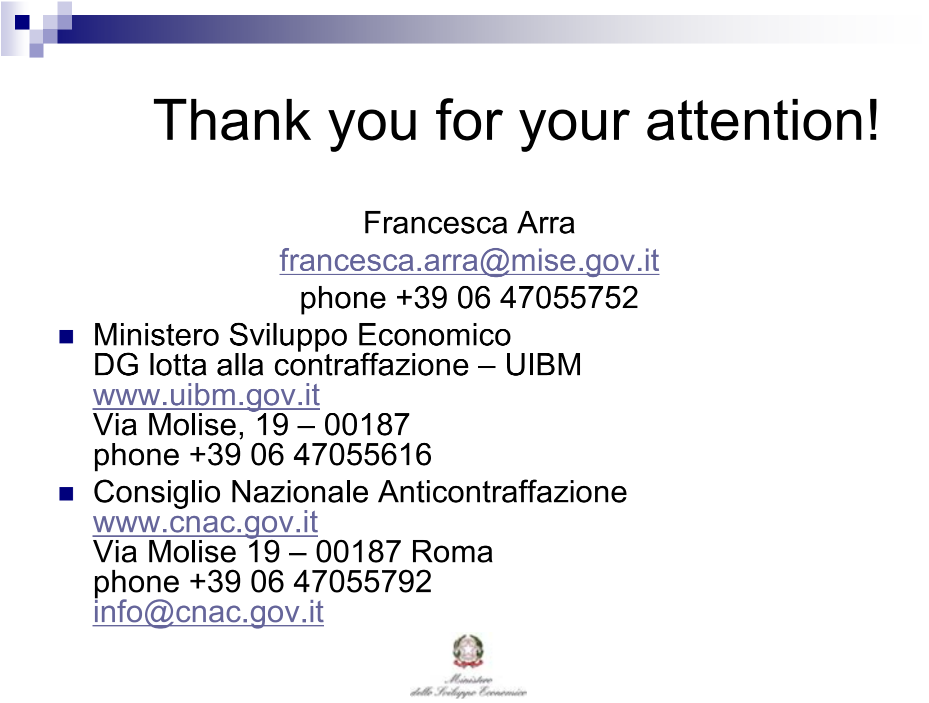
- Six macro-priorities
  - □ Encouraging communication, information and education campaigns
  - □ Preserving civil Judges' specialization and pursuing criminal Judges' specialization in IP matters
  - □ Strengthening anti-counterfeiting and IP law enforcement at local level
  - □ Fighting against online counterfeiting
  - □ Promoting training on IPR protection for enterprises
  - □ Protecting "Made in Italy" from foreign usurpation

Ministero dello Sviluppo Economico



«If it’s being made, it’s being faked»

- Cyber counterfeiting is a moving and ever-changing target:
  - □ New generic Top Level Domains
    - TradeMark Clearing House to protect rightholders
      - □ Sunrise period
      - □ TM Claim service
  - □ 3D printing



Thank you for your attention!

Francesca Arra
francesca.arra@mise.gov.it
phone +39 06 47055752

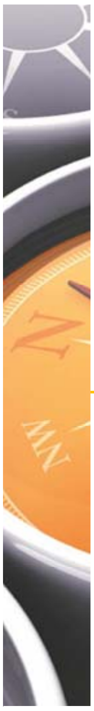
- Ministero Sviluppo Economico
  DG lotta alla contraffazione – UIBM
  www.uibm.gov.it
  Via Molise, 19 – 00187
  phone +39 06 47055616
- Consiglio Nazionale Anticontraffazione
  www.cnac.gov.it
  Via Molise 19 – 00187 Roma
  phone +39 06 47055792
  info@cnac.gov.it

Biography: Francesca Arra

Francesca Arra has been working at the Italian Ministry for Economic Development since 2010, as an officer within the DG for the fight against counterfeiting-Italian Patent and Trademark Office (www.uibm.gov.it). She is also a member of the Secretariat of the

Italian Anticounterfeiting Council (CNAC, www.cnac.gov.it), an intergovernmental body whose mission is to foster and coordinate anti-counterfeiting initiatives at national level. As a member of the CNAC Secretariat she acts as an interface between the CNAC President and the representatives and delegates of CNAC member institutions (11 Ministries, the National Association of Italian Municipalities, Anticounterfeiting law enforcement bodies, trade and consumer associations) and actively participates in the development and implementation of the National Anticounterfeiting Plan. Her areas of expertise include: IP and anticounterfeiting communication, IP financial support schemes, online counterfeiting. Before joining the Italian Ministry for Economic Development, Francesca Arra worked at IPI-Italian Institute for Industrial Promotion, at first at the Milan office (a branch of the IPI Department for Innovation and Knowledge Transfer in Rome) and then at the Rome headquarters where she was responsible for Internet and traditional media communication activities. Francesca Arra has a degree in Political Economics from Bocconi University, Milan, specialising in Monetary and Financial Economics. She works and lives in Rome, Italy.

Romano Stasi – ABI Lab



UNICRI ROUND TABLE
Lucca, November 29th 2013

Cyber security in the banking sector

The Italian FI-ISAC - Financial Institution Information Sharing & Alerting Center

Romano Stasi

Managing Director ABI Lab

SICUREZZA E FRODI INFORMATICHE IN BANCA

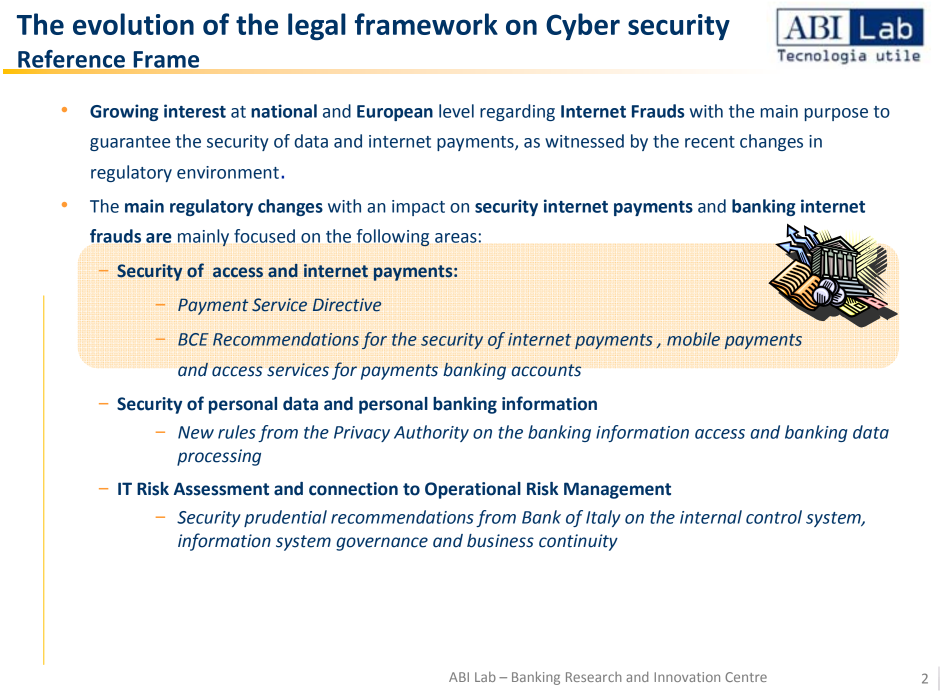
Come prevenire e contrastare le frodi su Internet e Mobile Banking

giugno 2013

ABI Lab Consortium – Banking Research and Innovation Centre

Agenda

- The evolution of the legal framework on Cyber security
- The Institutional activities on Cyber security issues
- The e-crime scenario in the Italian Banking Sector
- Actions to block and prevent Internet Frauds



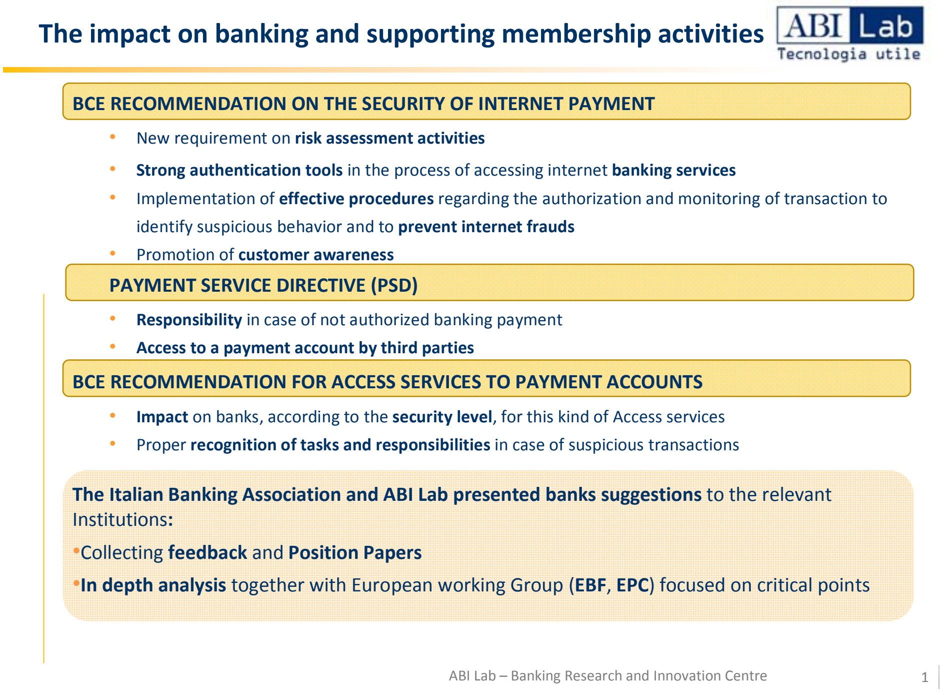
The evolution of the legal framework on Cyber security

Reference Frame

ABI Lab
Tecnologia utile

- **Growing interest** at **national** and **European** level regarding **Internet Frauds** with the main purpose to guarantee the security of data and internet payments, as witnessed by the recent changes in regulatory environment.
- The **main regulatory changes** with an impact on **security internet payments** and **banking internet frauds are** mainly focused on the following areas:
  - **Security of access and internet payments:**
    - *Payment Service Directive*
    - *BCE Recommendations for the security of internet payments , mobile payments and access services for payments banking accounts*
  - **Security of personal data and personal banking information**
    - *New rules from the Privacy Authority on the banking information access and banking data processing*
  - **IT Risk Assessment and connection to Operational Risk Management**
    - *Security prudential recommendations from Bank of Italy on the internal control system, information system governance and business continuity*

ABI Lab – Banking Research and Innovation Centre 2



The impact on banking and supporting membership activities

ABI Lab
Tecnologia utile

BCE RECOMMENDATION ON THE SECURITY OF INTERNET PAYMENT

- New requirement on **risk assessment activities**
- **Strong authentication tools** in the process of accessing internet **banking services**
- Implementation of **effective procedures** regarding the authorization and monitoring of transaction to identify suspicious behavior and to **prevent internet frauds**
- Promotion of **customer awareness**

PAYMENT SERVICE DIRECTIVE (PSD)

- **Responsibility** in case of not authorized banking payment
- **Access to a payment account by third parties**

BCE RECOMMENDATION FOR ACCESS SERVICES TO PAYMENT ACCOUNTS

- **Impact** on banks, according to the **security level**, for this kind of Access services
- Proper **recognition of tasks and responsibilities** in case of suspicious transactions

The Italian Banking Association and ABI Lab presented banks suggestions to the relevant Institutions**:**

•Collecting **feedback** and **Position Papers**

•**In depth analysis** together with European working Group (**EBF**, **EPC**) focused on critical points

ABI Lab – Banking Research and Innovation Centre 1

Agenda

- The evolution of the legal framework on Cyber security
- The Institutional activities on Cyber security issues
- The e-crime scenario in the Italian Banking Sector
- Actions to block and prevent Internet Frauds

The operational and research activities

OBSERVATORY ON COMPUTER SECURITY AND INTERNET THREATS

Continuous monitoring on security issues and banking **frauds**, with special attention to **Internet and Mobile Banking**, achieved by:

- **Research activities ➔ SURVEY & ANNUAL REPORT**
  ➔ MONTHLY BULLETIN
- **Institutional Collaboration**
- **Workshop and communication activities**

Technical meetings:
•44 banks/outsourcer
•ICT Partner
•Polizia Postale e delle Comunicazioni

COMMUNITY PRESIDIO.INTERNET

Banking Community, launched on 2009 with the aim of **information exchange and informal collaboration** with the **Law enforcement Agencies**

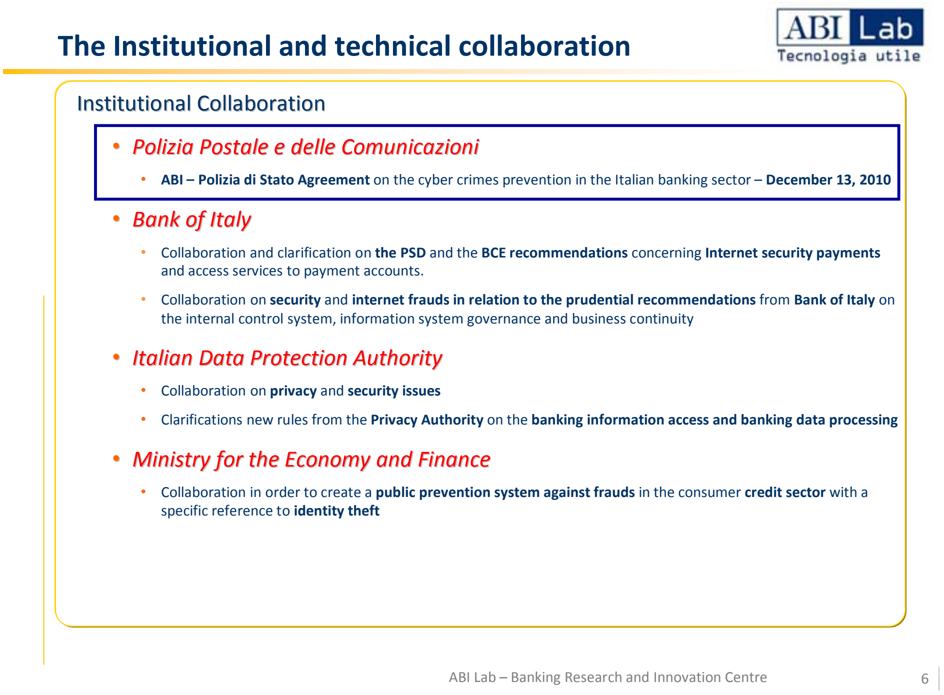
RSA
Reply
ABI Lab

Communications::
- ***1 to 1***
- ***1 to many***
- ***1 to all***

Community :
•370 experts references/outsourcer
•Polizia Postale e delle Comunicazioni
•TLC operator

INTERNATIONAL COLLABORATION

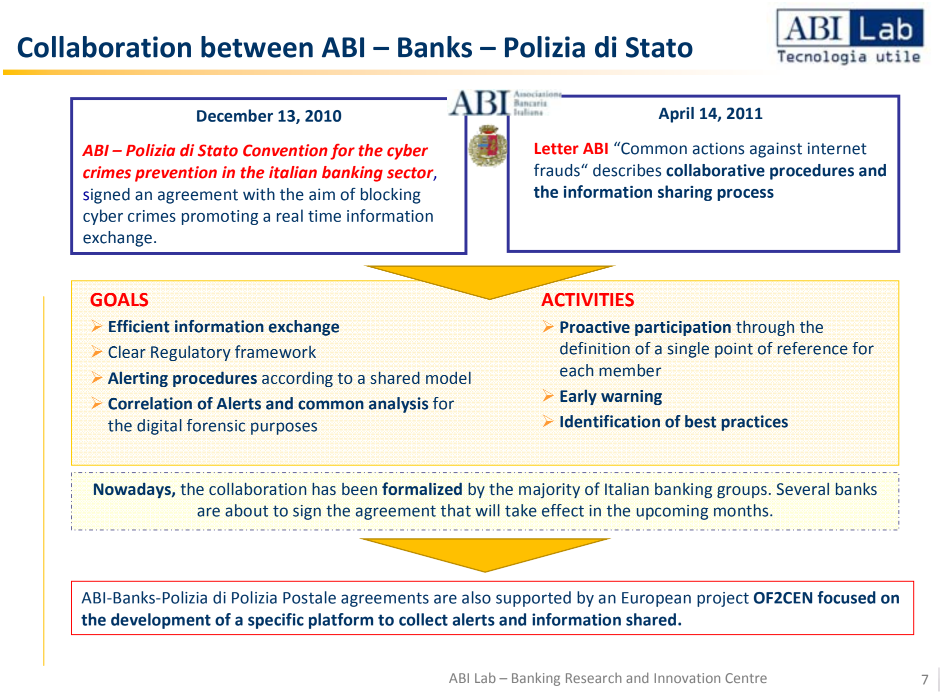
- **IT Fraud Working Group** *(European Banking Federation)*
- **ISSG/CISEG – Information Security Support Group/Cybercrime Information Sharing Expert Group** (European Payments Council)
- **European FI-ISAC – Financial Institutions Information Sharing and Analysis Centre** *(ENISA)*
- **EECTF – European Electronic Crime Task Force** *(Poste Italiane, Polizia Postale, USSS)*
- **Other network:** *- Antiphishing WG Member*
  - Joining DCC & European Project



The Institutional and technical collaboration

Institutional Collaboration

- *Polizia Postale e delle Comunicazioni*
  - **ABI – Polizia di Stato Agreement** on the cyber crimes prevention in the Italian banking sector – **December 13, 2010**
- *Bank of Italy*
  - Collaboration and clarification on **the PSD** and the **BCE recommendations** concerning **Internet security payments** and access services to payment accounts.
  - Collaboration on **security** and **internet frauds in relation to the prudential recommendations** from **Bank of Italy** on the internal control system, information system governance and business continuity
- *Italian Data Protection Authority*
  - Collaboration on **privacy** and **security issues**
  - Clarifications new rules from the **Privacy Authority** on the **banking information access and banking data processing**
- *Ministry for the Economy and Finance*
  - Collaboration in order to create a **public prevention system against frauds** in the consumer **credit sector** with a specific reference to **identity theft**



Collaboration between ABI – Banks – Polizia di Stato

December 13, 2010

ABI – Polizia di Stato Convention for the cyber crimes prevention in the italian banking sector, signed an agreement with the aim of blocking cyber crimes promoting a real time information exchange.

April 14, 2011

Letter ABI "Common actions against internet frauds" describes **collaborative procedures and the information sharing process**

GOALS

- **Efficient information exchange**
- Clear Regulatory framework
- **Alerting procedures** according to a shared model
- **Correlation of Alerts and common analysis** for the digital forensic purposes

ACTIVITIES

- **Proactive participation** through the definition of a single point of reference for each member
- **Early warning**
- **Identification of best practices**

Nowadays, the collaboration has been **formalized** by the majority of Italian banking groups. Several banks are about to sign the agreement that will take effect in the upcoming months.

ABI-Banks-Polizia di Polizia Postale agreements are also supported by an European project **OF2CEN focused on the development of a specific platform to collect alerts and information shared.**

Raising awareness
Corporate clients – recommendations

ABI Lab Consortium, with the support of CBI Consortium, is disseminating recommendations to the customers in order to guarantee a **safe use of the internet banking**.

In details:

•Actions to prevent and block internet frauds on Corporate clients using internet banking

The document contains some **useful suggestion** for banks to increase **the control activities** and to prevent frauds.

•Awareness activities for Corporate clients for a safe use of the internet banking

The document shared also with **Polizia Postale e delle Comunicazioni** is structured in 3 chapters:

- ➢Corporate policies
- ➢Guidelines for the workstation protection from which internet banking activities are carried out
- ➢Best practices and good behaviors

Raising awareness
Recommendations for Corporate clients

The recommendations are structured as following:

•Corporate policies

- ✓ Adopt a **shared policies on** cyber security
- ✓ **Identify** in advance any **employees** and PC where all transactions are processed
- ✓ Promote **regularly internal training r**egarding **cyber security**
- ✓ Promote the use of an **alternative communication channel and "strong authentication" tools** provided by the bank
- ✓ **Frequently reset passwords**

•Guidelines for the workstations protection (PC user)

- ✓ **Install and update** an efficient **anti-malware and the appropriate firewall**
- ✓ **Periodically update the operating systems**
- ✓ **Limit the web browsing** and/or **the not certified downloading**
- ✓ **Modify the users profile** depending on specific operational needs
- ✓ **If needed,** in order to guarantee the company environment, it would be helpful to develop the IB payments from a **designated workstation**

•Best practices for the IB users

- ✓ **Identify personal policies regarding data conservation**, **access codes** and **more IB information**
- ✓ **Type web addresses on the browser** not by clicking on external links

Agenda

- The evolution of the legal framework on Cyber security
- The Institutional activities on Cyber security issues
- The e-crime scenario in the Italian Banking Sector
- Actions to block and prevent Internet Frauds

ABI Lab
Activities on Information Security and Internet Frauds

ABI Lab is the Banking Research & Innovation Centre founded in 2001 on the initiative of the Italian Banking Association (ABI) with the aim of:

- **Research activities**
- **Case studies**
- **Pilot projects**
- **Lobbying to public organizations**
- **Communication**
- **KMS and community tools**

ABI Lab is a COMMUNITY with:

166 Banks & **68 ICT Partners**

4 RESEARCH AREAS

- SECURITY
- Working Group on Information Security and Internet Frauds
- Observatory on Secure Identity Management
- Observatory on Business Continuity
- Assessment on Security Governance
- IT SYSTEMS
- CHANNELS
- SUPPORT PROCESSES

To continuously **monitor threats** and **information security** issues targeting **Italian banks** and to point out **best practices to protect**, building a **community of peers for information sharing**

To support banks on **secure identity management**, with reference to both **processes** and **technologies** by **information sharing**, contribution to and clarification of **legal framework** and **pilot projects**

Methodology

- TECHNICAL FOCUS GROUP
- RELATIONSHIP WITH INSTITUTIONS
- COMMUNICATION

The Context

ABI Lab Tecnologia utile

- During last years customers have increased the use of **Internet** and **Mobile Banking :**
  - **Services provided through Mobile: +30%***
  - **Access to the Internet Banking **: +29% Retail**
    +24% Corporate

- The increased interest on using remote channels not always means an adequate knowledge of the **risks** and the **actions to prevent** and **reduce** them.
- The evolution of **Internet Frauds** causes ➔ strong and sophisticated **e-crimes attacks**

- Continuously develop and to point out **best practices and tools** to protect and prevent new and stronger e-crimes
- **Customers** education and **awareness should be reinforced** with appropriate communication on this topic.

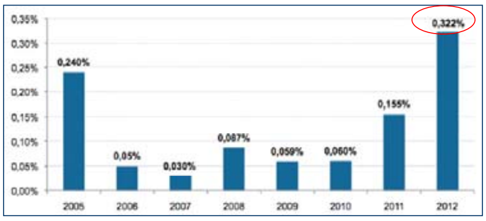
*Source: ABI Lab and School of Management – Politecnico di Milano, Observatory on Mobile Banking, Dicember 2012
**Source: ABI Lab, Observatory on Computer Security and Internet Threats, Survey on Identity Frauds, 2013, 29 respondents; processing on the average number of accesses per active user

Digital Identity Frauds on retail customers in Italy

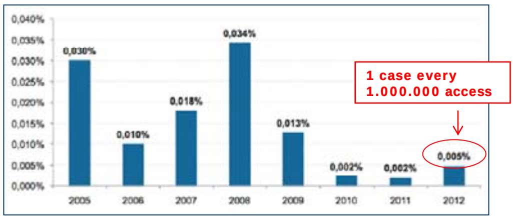
ABI Lab Tecnologia utile

- __Retail Customers – 2012:__ **740 million of** Internet Banking **login.**
- A substantial **increase** in 2012 of **lost credentials (0.322%).**
- Compared to the number of accesses, the percentage drops to a value of **0.0059%** equal to **1 lost credential every 17,000 accesses.**

Online active Retail customers who lost CREDENTIALS



Online active Retail customers who suffered an economic loss



1 case every 1.000.000 access

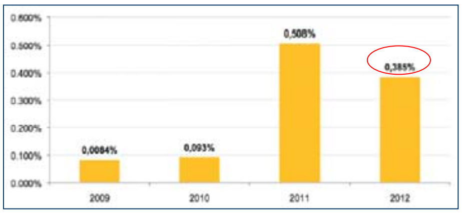
- A slight increase of retail **customers victim of frauds** and who consequently **lost money**, equal to **0.005%** of the customers.
- With regard to the estimated total number of accesses, the percentage of customers who lost money is equal to **0.0001%**, that is **1 case every 1,000,000 accesses.**

Source: ABI Lab, Observatory on Computer Security and Internet Threats, Observatory on Security Identity Management, Survey on Identity Frauds and Secure Identity Management 2013, 39 respondents

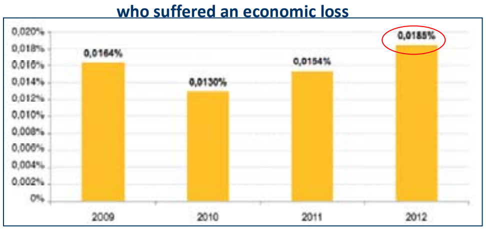
Digital Identity Frauds on Corporate customers in Italy

- Corporate customers – 2012 : over **1.6 million** active online accounts, with **300 million logins.**
- Decreased number of customers victim of Internet Banking **identity theft (0.385%).**
- Comparing to the total amount of considered logins, the percentage of identity theft is equal to **0,002%** (**1 case every 50.000 logins**).

% Online active Corporate customers who lost CREDENTIALS



% Online active Corporate customers who suffered an economic loss



- Increase number of **active corporate customers** who suffered an **economic loss (0,0185%)**
- **Comparing to the total amount of the survey sample number of accesses,** the customers who lost money is approximately close to **0,0001%** .

Source: ABI Lab, Observatory on Computer Security and Internet Threats, Survey on Identify Frauds 2013, 29 respondents

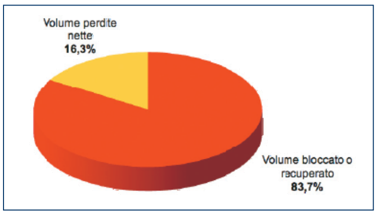
Fraudulent Transactions
Retail and Corporate Area

RETAIL CUSTOMERS

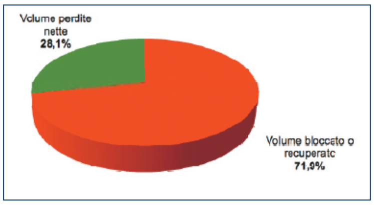
•**83,7%** of fraudulent transactions are **blocked** or **recovered**.

•**Only 0,0008% of the total number of transactions caused an economic loss.**

Fraudulent detected transactions breakdown - Retail Customers



Fraudulent detected transactions breakdown – Corporate Customers



CORPORATE CUSTOMERS

•**Only 0,0003%** of the total number of transactions **caused an economic loss.**

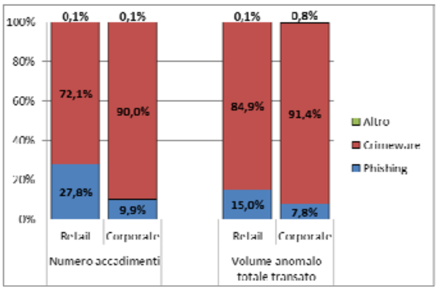
•**71,9%** of **fraudulent transactions** are **blocked** or **recovered**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Attacks

Clients segment comparison

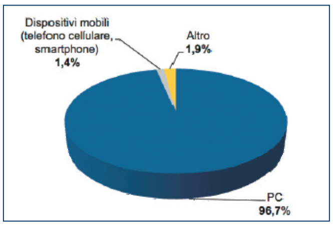
Number of attacks by type



- Compared to 2011 , crime-ware appears as the **most effective** kind of attack for **both customer segments**.
- **Customer PC** is still the **main effected** device.

- **Retail customers:** during the **2012 for the first time has been detected some mobile attacks** (1,4%)**, focused on gathering SMS to collect OTP codes** sent by the bank to authorize transactions.

Attacked Device (Retail)



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

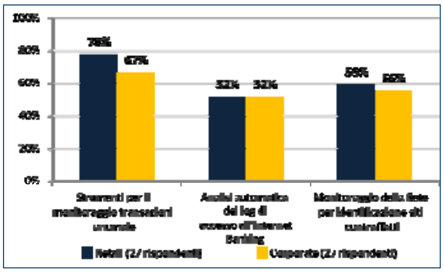
Agenda

- The evolution of the legal framework on Cyber security
- The Institutional activities on Cyber security issues
- The e-crime scenario in the Italian Banking Sector
- Actions to block and prevent Internet Frauds

Italian scenario

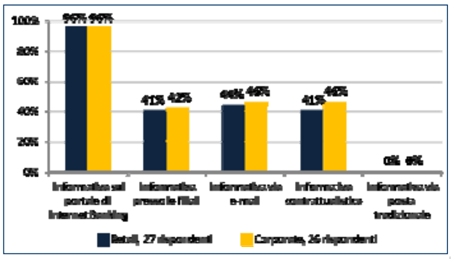
Monitoring tools and customers awareness

Monitoring activities and technological equipment



- **Increasing number of banks** that is using monitoring **tools** to identify internet banking access and anomalous transactions
- Increasing number of banks participating at **information sharing communities** and using **early warning services**.

Awareness and training activities



- **96% of banks is providing** information on cyber security trough the Internet Banking.
- **Awareness activities are raising usually focusing the following key points:**
  - **risks** and main **cyber threats**
  - **security tools** provided by the banks **together with** specific rules and user behaviors.

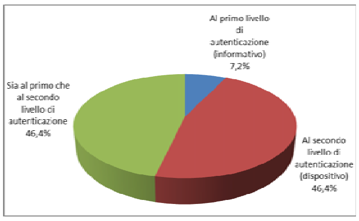
Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Italian scenario

Technological countermeasures

Retail

The Authentication factor*



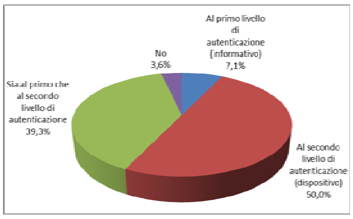
- **All the interviewed banks** are using **two level of authentication.**
- Mandatory use of strong authentication tools **in 71,4%** of banks
- The most common technologies:
  - **Token OTP** (**57,1%**),
  - **Smart grid** (35,7%),
  - **OTP via SMS** (28,6%).

* 28 rispondenti

Corporate

- **All the interviewed banks** are using **two level of authentication.**
- Mandatory use of strong authentication tools **in 63%** of banks
- The most common technologies:
  - **Token OTP** (**55,6%**),
  - **Digital certificate** (**33,3%**),
  - **Smart Grid** (29,6%).

The Authentication factor*

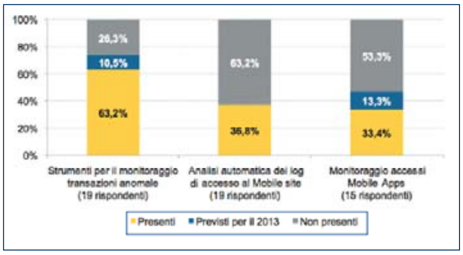


Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

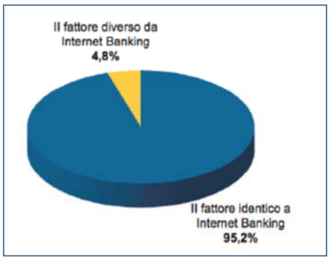
Mobile Channel security

- According to the survey, during 2012 was not identified **any fraud to specific Mobile services created by the banks** (ex. mobile apps)

Technological tools to monitor and detect attacks



Use of the second authentication factor



- **Increase of the banks** equipped with technological tools for transaction **monitoring** (**63.2%** of the sample) and **attacks detection** specific for the Mobile channel.
- In **95.2%** of the examples the strong authentication **technology for mobile banking is the same** used for accessing the **Internet Banking**.

Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2013, 29 rispondenti

Priorities in the banking sector

- Maintain the **highest protection level** that will be able **to respond to new cybercrime threats considering all the specific differences of customer segments.**
- For **Retail** segment it would be useful **to focus the attention** on the new attacks **against the mobile devices** and security solutions concerning such devices, on the other hand, for **Corporate** clients the attention should be focused on the **transactions monitoring.**
- It may be useful to set up **awareness activities** in order **to adopt** all the **security solutions provided by the bank**.
- It would be necessary to pay **attention to the evolution of the regulatory framework** in order to implement the appropriate solutions.
- Develop appropriate **procedures** for cross industry **cooperation** and **information sharing** at national and international level.

unicri United Nations Interregional Crime and Justice Research Institute

UNICRI ROUND TABLE
Lucca, November 29th 2013

ABI Lab
Tecnologia utile

THANK YOU FOR YOUR ATTENTION

Biography: Romano Stasi

Romano Stasi, born in Rome in 1968, graduated in engineering in 1993 from the University La Sapienza of Rome. He also holds an MBA from the University SDA Bocconi in Milan.

He is currently Secretary General of the ABI Lab Consortium, the Banking Research and Innovation Centre promoted by ABI. He has been a management consultant for major international companies such as Accenture and Cap Gemini Ernst & Young, developing projects in the IT domain of the financial sector.

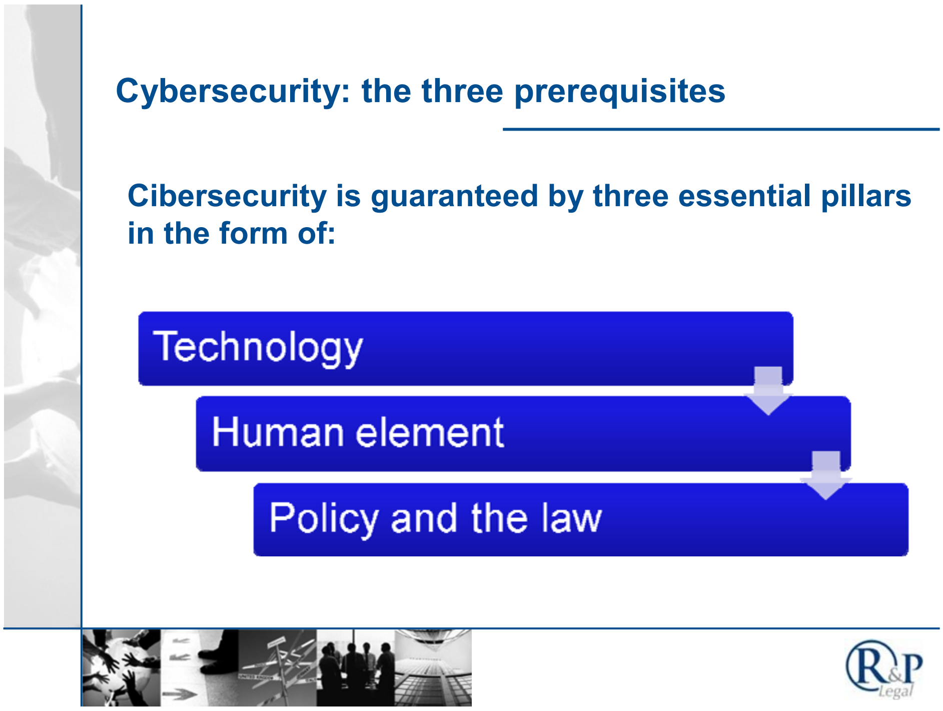
He was also a Marketing Manager and E-business leader at GE Oil & Gas where he coordinated an international project concerning the definition and implementation of a strategy for e-business.

Giuseppe Vaciago – R&P Legal

29 November– ***UNICRI***

Round Table on Cybercrime and Cybersecurity in Enterprises.

Giuseppe Vaciago

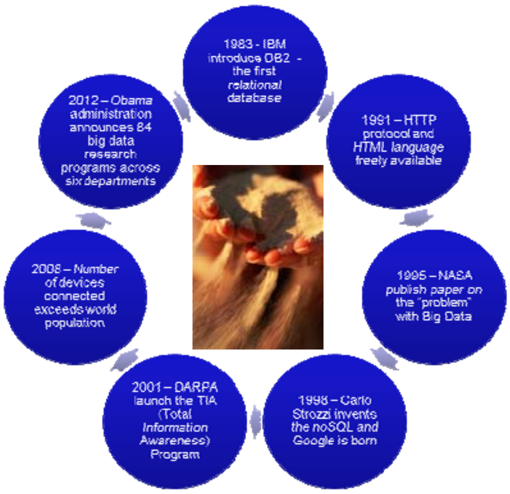


Cybersecurity: the three prerequisites

Cibersecurity is guaranteed by three essential pillars in the form of:

- Technology
- Human element
- Policy and the law

Technology: Cloud Computing and Big Data



1983 - IBM introduce DB2 - the first relational database

1991 – HTTP protocol and HTML language freely available

1995 – NASA publish paper on the "problem" with Big Data

1998 – Carlo Strozzi invents the noSQL and Google is born

2001 – DARPA launch the TIA (Total Information Awareness) Program

2008 – Number of devices connected exceeds world population

2012 – Obama administration announces 84 big data research programs across six departments

Technology: "Social Botnet"

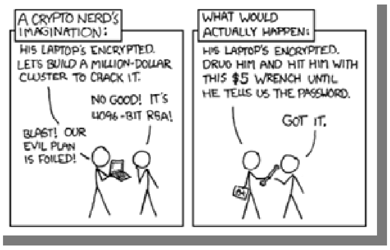
In-depth investigations by the FBI have revealed that in 2012 more than **11 million** Facebook users were affected by a particular malware capable of inflicting $**850m** worth of damage.

twitter
facebook
Source: Luma Partners, Terry Kawaja
© 2012 Buddy Media, Inc. Proprietary and Confidential

Technology: Bring Your Own Device

Loss of control over business devices
+
Increased risk of introduction of malware
=
Increased risk of losing business data

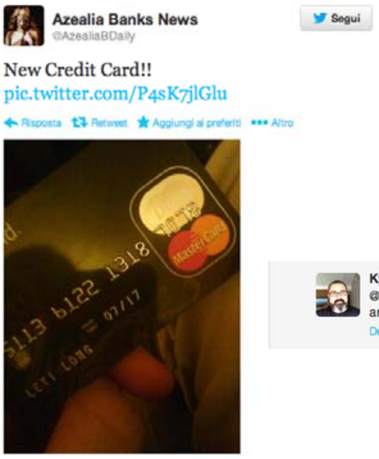
Human Element: encryption


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Snowden may have persuaded 20 to 25 NSA colleagues to give up their passwords

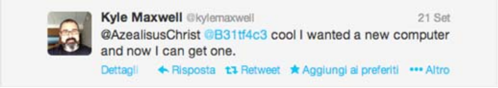
Reuters says those borrowed creds helped Snowden get access to docs he later leaked.

Human Element: @NeedADebitCard



Azealia Banks News @AzealiaBDaily

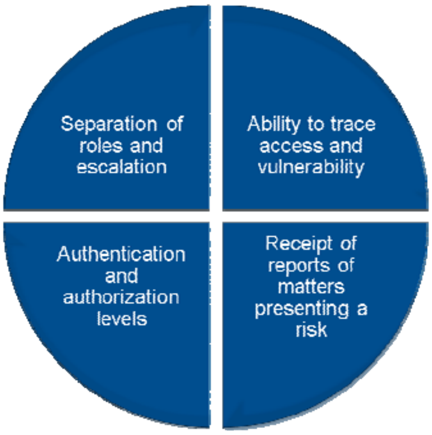
New Credit Card!!
pic.twitter.com/P4sK7jlGlu



Kyle Maxwell @kylemaxwell 21 Set

@AzealisusChrist @B31tf4c3 cool I wanted a new computer and now I can get one.

Policy: Cybersecurity management system

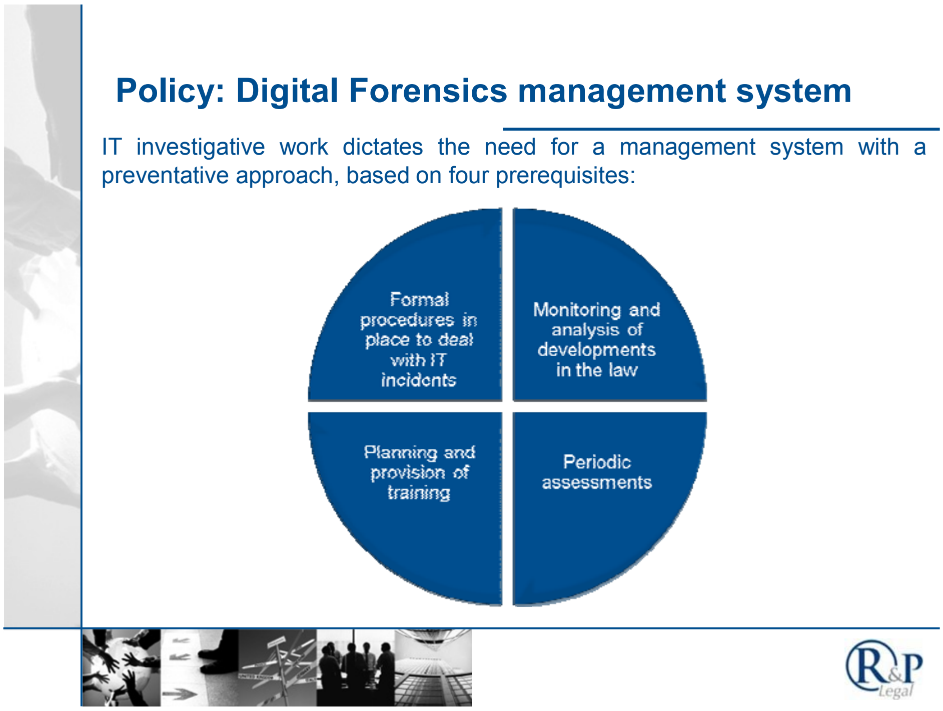


Separation of roles and escalation

Ability to trace access and vulnerability

Authentication and authorization levels

Receipt of reports of matters presenting a risk



Policy: Digital Forensics management system

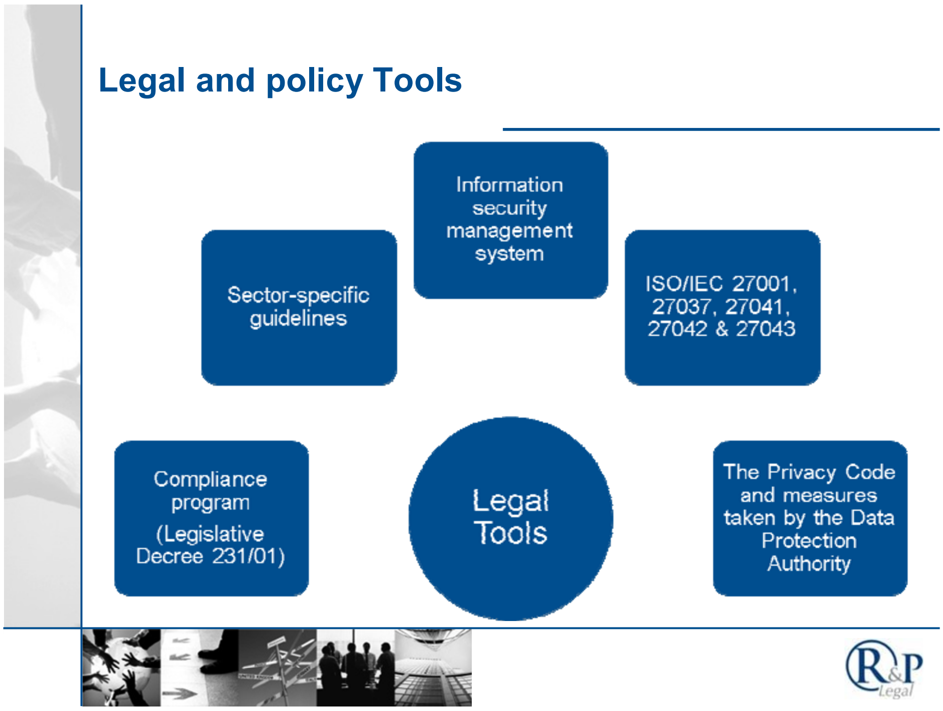
IT investigative work dictates the need for a management system with a preventative approach, based on four prerequisites:

Formal procedures in place to deal with IT incidents

Monitoring and analysis of developments in the law

Planning and provision of training

Periodic assessments



Legal and policy Tools

Information security management system

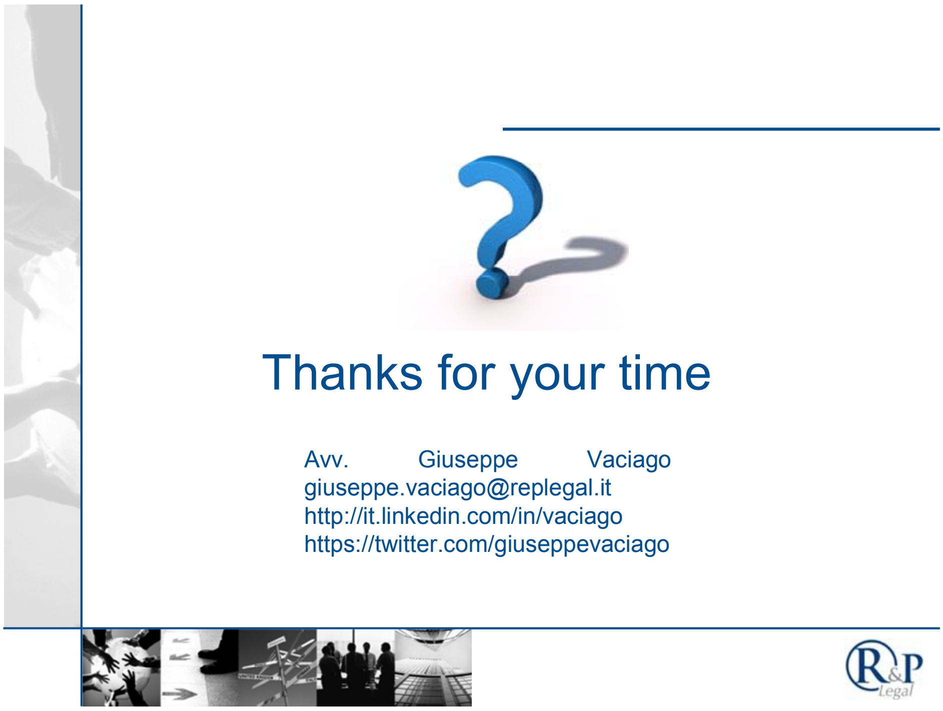
Sector-specific guidelines

ISO/IEC 27001, 27037, 27041, 27042 & 27043

Compliance program (Legislative Decree 231/01)

Legal Tools

The Privacy Code and measures taken by the Data Protection Authority



Thanks for your time

Avv. Giuseppe Vaciago
giuseppe.vaciago@replegal.it
http://it.linkedin.com/in/vaciago
https://twitter.com/giuseppevaciago

Biography: Giuseppe Vaciago

He is specialized on criminal law relating to new technology, and corporate criminal law as well as advising on the drafting of compliance program on corporate liability; he acts for a number of leading national and international companies in the IT sector. He has a PhD in Digital Forensics from the University of Milan-Bicocca and lectures in IT law at the University of Insubria. A Visiting Scholar at Standford Law School and Fordham Law School in New York, he has also been invited to speak on a number of occasions by the most prestigious Italian universities as well as universities abroad. He is a fellow at the Nexa Center of Turin, Cybercrime Institute of Köln and he is the founder of Tech and Law Center of Milan. Giuseppe is the author of a number of Italian university textbooks including “Computer Crimes” (jointly with the Milan Tax Police), "Digital Evidence" and “Organization, Management and Compliance Models pursuant to Law 231/01″.

Andrea Moretti - Ebay

UNICRI - Cyber security in enterprises: legal aspects and good practices

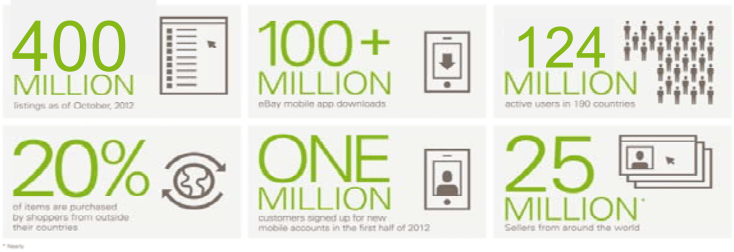
ANDREA MORETTI | HEAD OF LEGAL ITALY – 29 NOVEMBER 2013

CONNECTED COMMERCE:
CREATING MORE OPPORTUNITY
TOGETHER

EBAY– OVERVIEW

Founded in 1995, eBay is the world's largest online marketplace.

- Built around online auctions, it is used today more for **new items** at **fixed price** from **professional sellers** and businesses.
- eBay does not own or sell the items listed on this site eBay: connects a community of businesses, **buyers** and **sellers**.
- With presence in **39 countries**, in 2012, the value of items sold on eBay has been **$67,8M** and active users over **124M**.



CONSUMERS’ EXPECTATIONS ARE CHANGING

HOW TO SHOP

SERVICE LEVELS

EBAY'S MARKETPLACE IS CHANGING TOO

FROM UNIQUE ITEMS, USED, IN AUCTION → TO A SELECTION OF NEW ITEMS AND IMMEDIATELY AVAILABLE

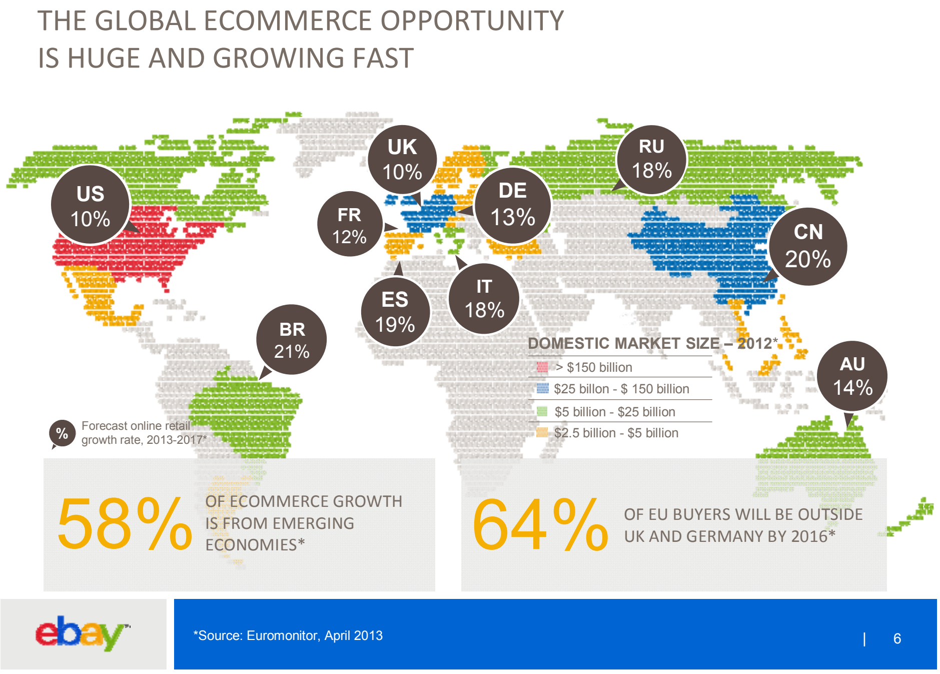
FROM THE SEARCH OF A SPECIFIC ITEM → TO AN INSPIRATIONAL SEARCH EXPERIENCE

FROM FEW SINGLE MARKETS → TO A GLOBAL MARKETPLACE WITHOUT BORDERS

FROM A DESKTOP BASED EXPERIENCE → TO A MULTI DEVICE PERFECTLY INTEGRATED EXPERIENCE

ebay

| 5



THE GLOBAL ECOMMERCE OPPORTUNITY IS HUGE AND GROWING FAST

US 10%

UK 10%

FR 12%

DE 13%

ES 19%

IT 18%

RU 18%

CN 20%

BR 21%

AU 14%

% Forecast online retail growth rate, 2013-2017*

DOMESTIC MARKET SIZE – 2012*

- 🟥 > $150 billion
- 🟦 $25 billon - $ 150 billion
- 🟩 $5 billion - $25 billion
- 🟨 $2.5 billion - $5 billion

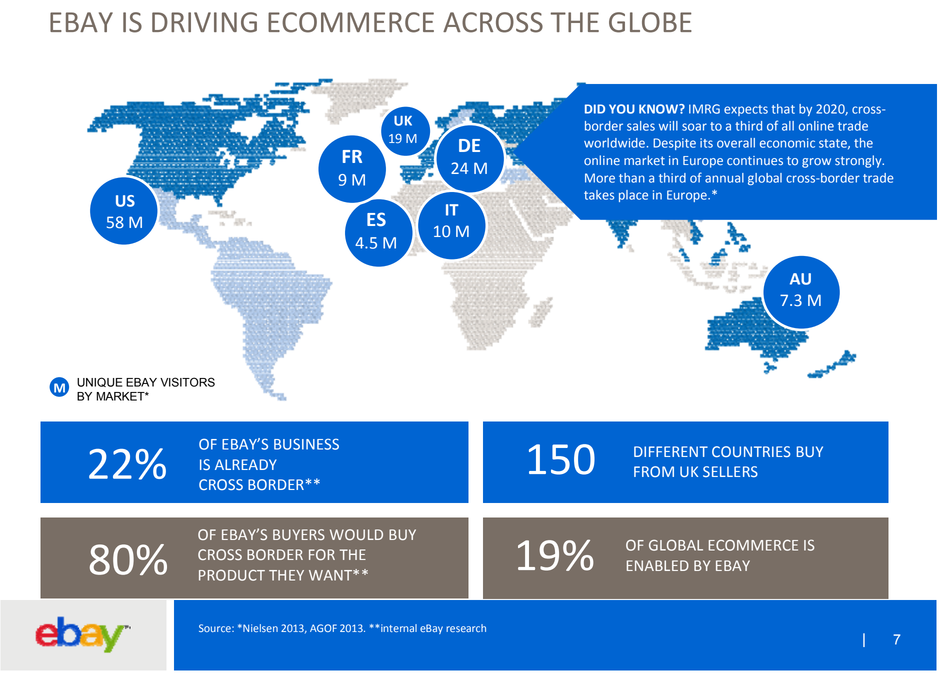
58% OF ECOMMERCE GROWTH IS FROM EMERGING ECONOMIES*

64% OF EU BUYERS WILL BE OUTSIDE UK AND GERMANY BY 2016*

ebay

*Source: Euromonitor, April 2013

| 6



EBAY IS DRIVING ECOMMERCE ACROSS THE GLOBE

US
58 M
UK
19 M
FR
9 M
DE
24 M
ES
4.5 M
IT
10 M
AU
7.3 M

DID YOU KNOW? IMRG expects that by 2020, cross-border sales will soar to a third of all online trade worldwide. Despite its overall economic state, the online market in Europe continues to grow strongly. More than a third of annual global cross-border trade takes place in Europe.*

M UNIQUE EBAY VISITORS BY MARKET*

22% OF EBAY'S BUSINESS IS ALREADY CROSS BORDER**

150 DIFFERENT COUNTRIES BUY FROM UK SELLERS

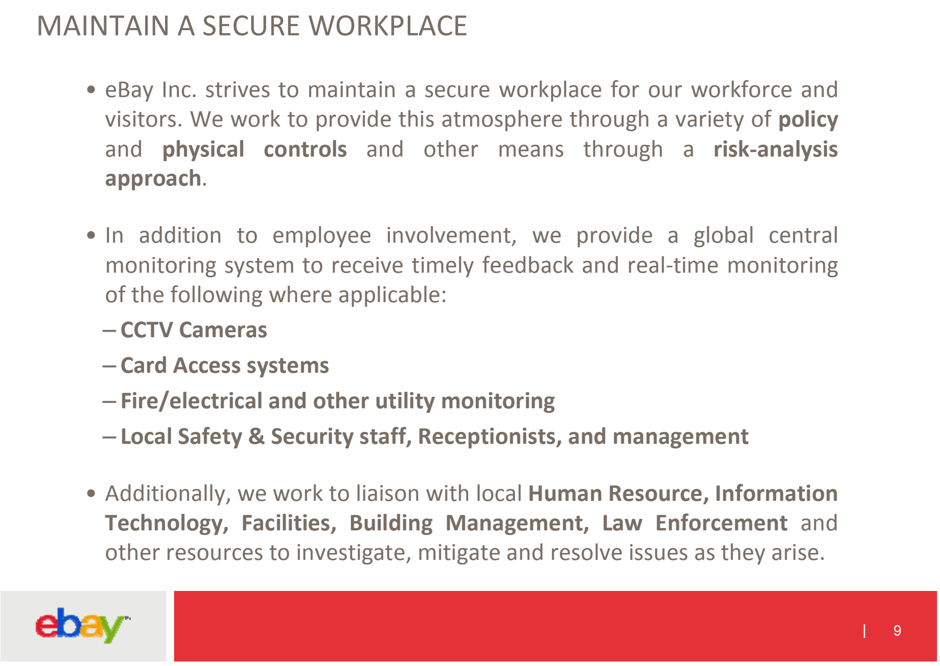
80% OF EBAY'S BUYERS WOULD BUY CROSS BORDER FOR THE PRODUCT THEY WANT**

19% OF GLOBAL ECOMMERCE IS ENABLED BY EBAY

Source: *Nielsen 2013, AGOF 2013. **internal eBay research

| 7

SAFETY AND SECURITY: PROTECTING THE ASSETS

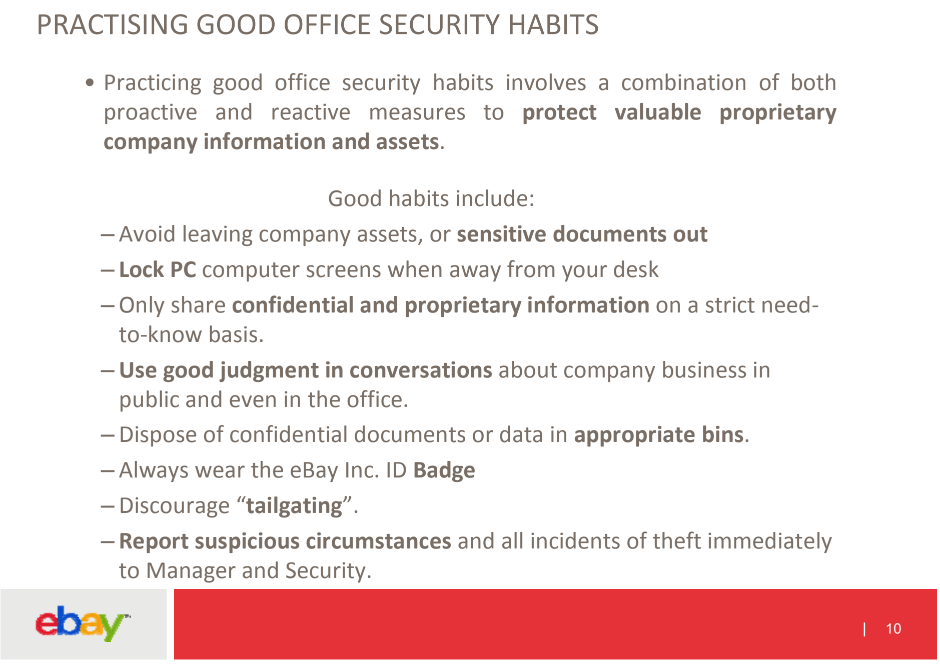


MAINTAIN A SECURE WORKPLACE

- eBay Inc. strives to maintain a secure workplace for our workforce and visitors. We work to provide this atmosphere through a variety of **policy** and **physical controls** and other means through a **risk-analysis approach**.

- In addition to employee involvement, we provide a global central monitoring system to receive timely feedback and real-time monitoring of the following where applicable:
  - **CCTV Cameras**
  - **Card Access systems**
  - **Fire/electrical and other utility monitoring**
  - **Local Safety & Security staff, Receptionists, and management**

- Additionally, we work to liaison with local **Human Resource, Information Technology, Facilities, Building Management, Law Enforcement** and other resources to investigate, mitigate and resolve issues as they arise.

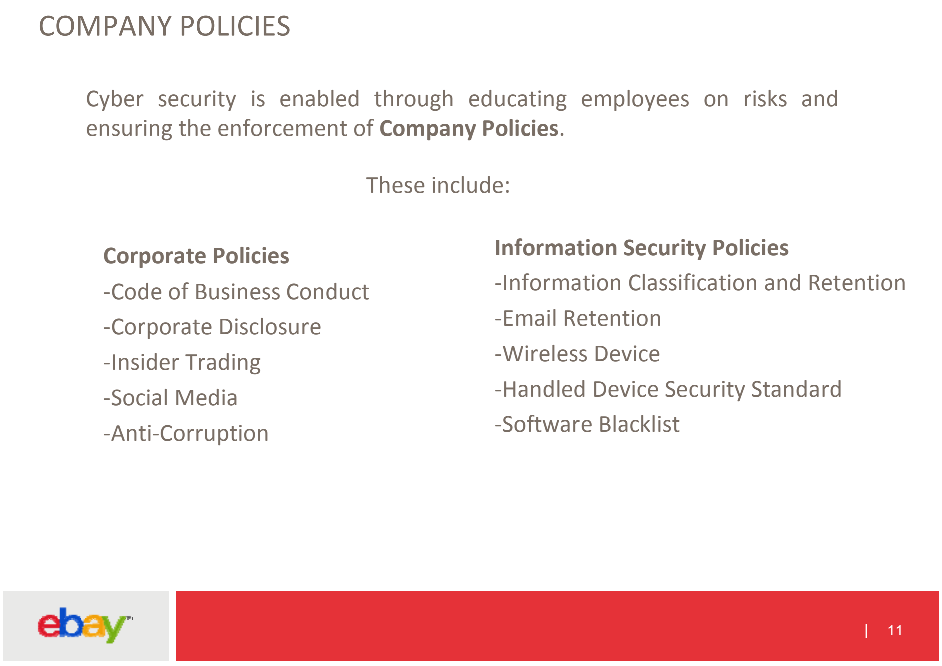


PRACTISING GOOD OFFICE SECURITY HABITS

- Practicing good office security habits involves a combination of both proactive and reactive measures to **protect valuable proprietary company information and assets**.

Good habits include:

- Avoid leaving company assets, or **sensitive documents out**
- **Lock PC** computer screens when away from your desk
- Only share **confidential and proprietary information** on a strict need-to-know basis.
- **Use good judgment in conversations** about company business in public and even in the office.
- Dispose of confidential documents or data in **appropriate bins**.
- Always wear the eBay Inc. ID **Badge**
- Discourage “**tailgating**”.
- **Report suspicious circumstances** and all incidents of theft immediately to Manager and Security.



COMPANY POLICIES

Cyber security is enabled through educating employees on risks and ensuring the enforcement of **Company Policies**.

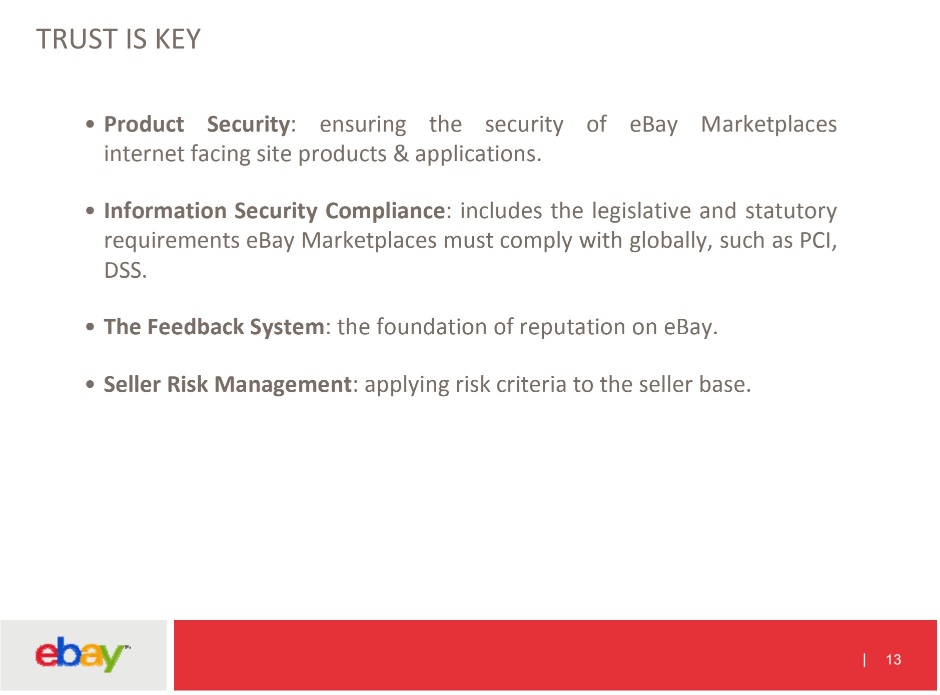
These include:

Corporate Policies
-Code of Business Conduct
-Corporate Disclosure
-Insider Trading
-Social Media
-Anti-Corruption

Information Security Policies
-Information Classification and Retention
-Email Retention
-Wireless Device
-Handled Device Security Standard
-Software Blacklist

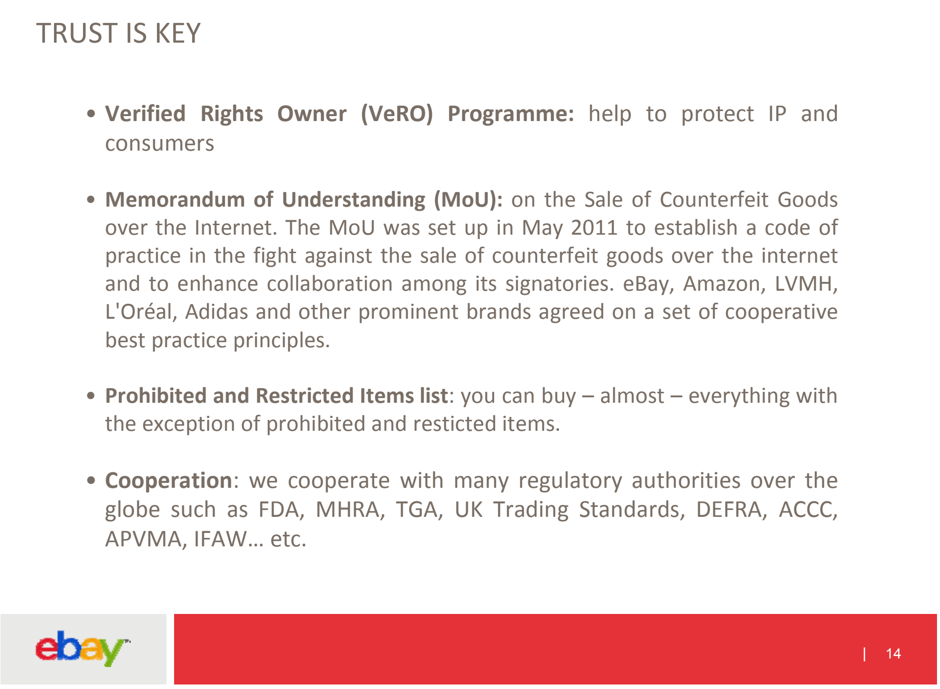
| 11

A SAFE PLACE TO TRADE



TRUST IS KEY

- **Product Security**: ensuring the security of eBay Marketplaces internet facing site products & applications.
- **Information Security Compliance**: includes the legislative and statutory requirements eBay Marketplaces must comply with globally, such as PCI, DSS.
- **The Feedback System**: the foundation of reputation on eBay.
- **Seller Risk Management**: applying risk criteria to the seller base.



TRUST IS KEY

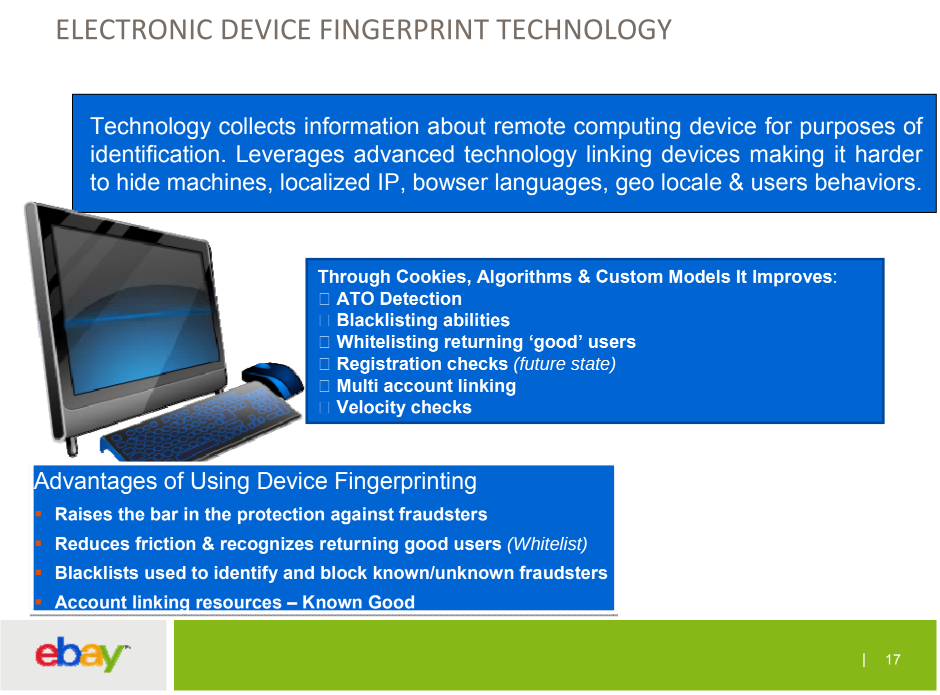
- **Verified Rights Owner (VeRO) Programme:** help to protect IP and consumers
- **Memorandum of Understanding (MoU):** on the Sale of Counterfeit Goods over the Internet. The MoU was set up in May 2011 to establish a code of practice in the fight against the sale of counterfeit goods over the internet and to enhance collaboration among its signatories. eBay, Amazon, LVMH, L'Oréal, Adidas and other prominent brands agreed on a set of cooperative best practice principles.
- **Prohibited and Restricted Items list**: you can buy – almost – everything with the exception of prohibited and resticted items.
- **Cooperation**: we cooperate with many regulatory authorities over the globe such as FDA, MHRA, TGA, UK Trading Standards, DEFRA, ACCC, APVMA, IFAW… etc.

GLOBAL ASSET PROTECTION

GLOBAL ASSET PROTECTION

Support eBay INC commerce communities by developing systems & procedures to protect our users and global assets, address risk through **prevention** & **reduction of criminal activity**, foster **strategic relationships** w/internal business partners, **law enforcement & government agencies**.

- Response to **requests for information** and proactive referrals of **criminal** matters
- Increase effectiveness of **proactive investigations** by promptly responding to and identifying significant incidents protecting users & brand, mitigate future risk, minimize financial losses and recover assets
- Actively engage and develop mutually beneficial **partnerships with retail industry** regarding both **stolen goods** and level of trust supporting merchant development
- Leverage **technology** to full scale improving efficiency of data disclosure processes



ELECTRONIC DEVICE FINGERPRINT TECHNOLOGY

Technology collects information about remote computing device for purposes of identification. Leverages advanced technology linking devices making it harder to hide machines, localized IP, bowser languages, geo locale & users behaviors.

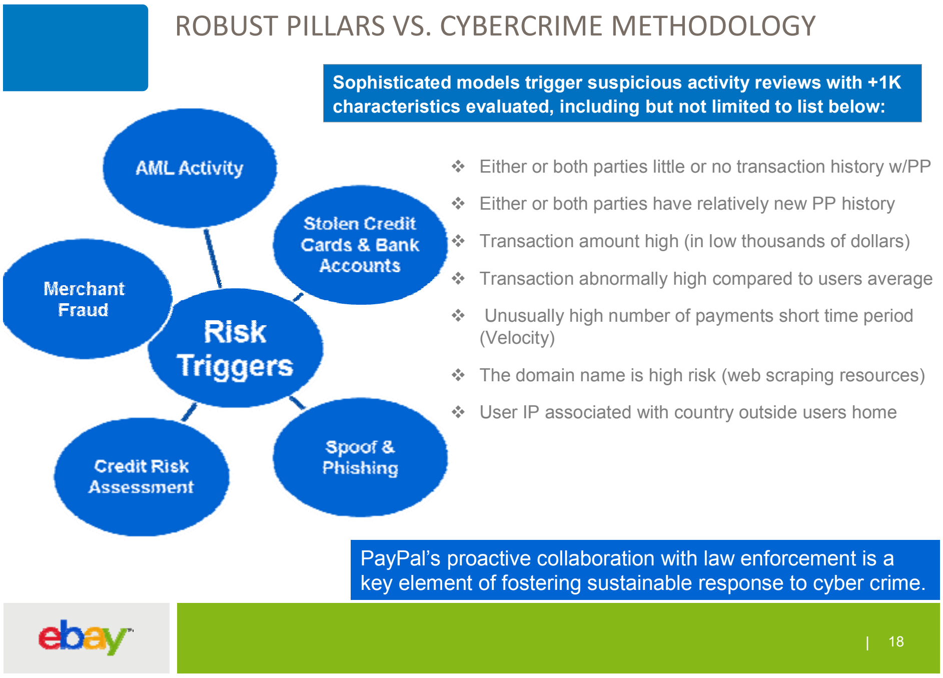
Through Cookies, Algorithms & Custom Models It Improves:

- □ **ATO Detection**
- □ **Blacklisting abilities**
- □ **Whitelisting returning ‘good’ users**
- □ **Registration checks** *(future state)*
- □ **Multi account linking**
- □ **Velocity checks**

Advantages of Using Device Fingerprinting

- **Raises the bar in the protection against fraudsters**
- **Reduces friction & recognizes returning good users** *(Whitelist)*
- **Blacklists used to identify and block known/unknown fraudsters**
- **Account linking resources – Known Good**

ebay | 17



ROBUST PILLARS VS. CYBERCRIME METHODOLOGY

Sophisticated models trigger suspicious activity reviews with +1K characteristics evaluated, including but not limited to list below:

Risk Triggers

AML Activity

Stolen Credit Cards & Bank Accounts

Merchant Fraud

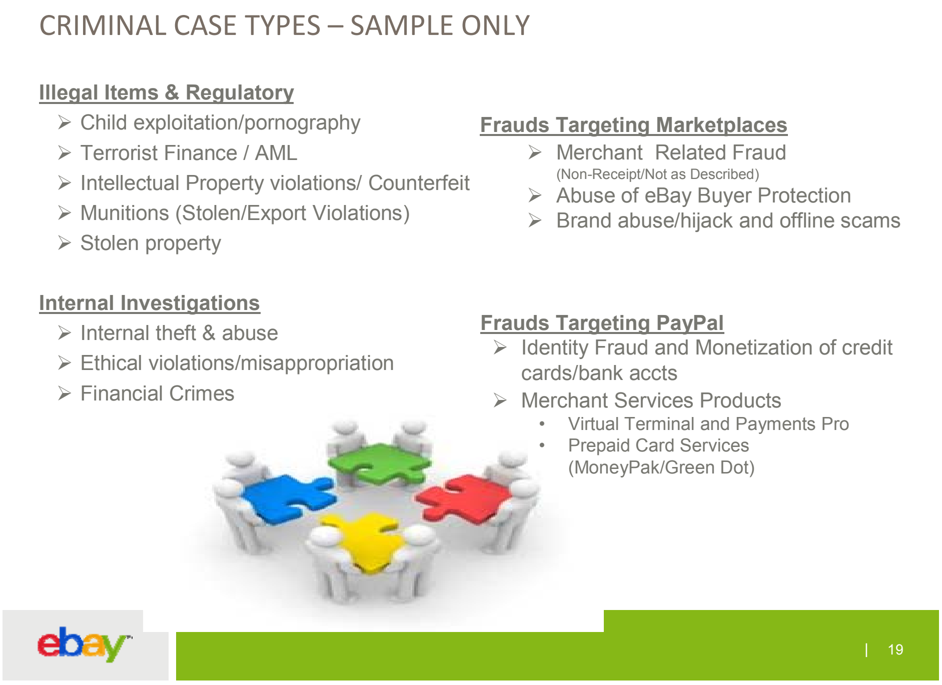
Credit Risk Assessment

Spoof & Phishing

- ❖ Either or both parties little or no transaction history w/PP
- ❖ Either or both parties have relatively new PP history
- ❖ Transaction amount high (in low thousands of dollars)
- ❖ Transaction abnormally high compared to users average
- ❖ Unusually high number of payments short time period (Velocity)
- ❖ The domain name is high risk (web scraping resources)
- ❖ User IP associated with country outside users home

PayPal’s proactive collaboration with law enforcement is a key element of fostering sustainable response to cyber crime.

ebay | 18



CRIMINAL CASE TYPES – SAMPLE ONLY

Illegal Items & Regulatory

- ➢ Child exploitation/pornography
- ➢ Terrorist Finance / AML
- ➢ Intellectual Property violations/ Counterfeit
- ➢ Munitions (Stolen/Export Violations)
- ➢ Stolen property

Internal Investigations

- ➢ Internal theft & abuse
- ➢ Ethical violations/misappropriation
- ➢ Financial Crimes

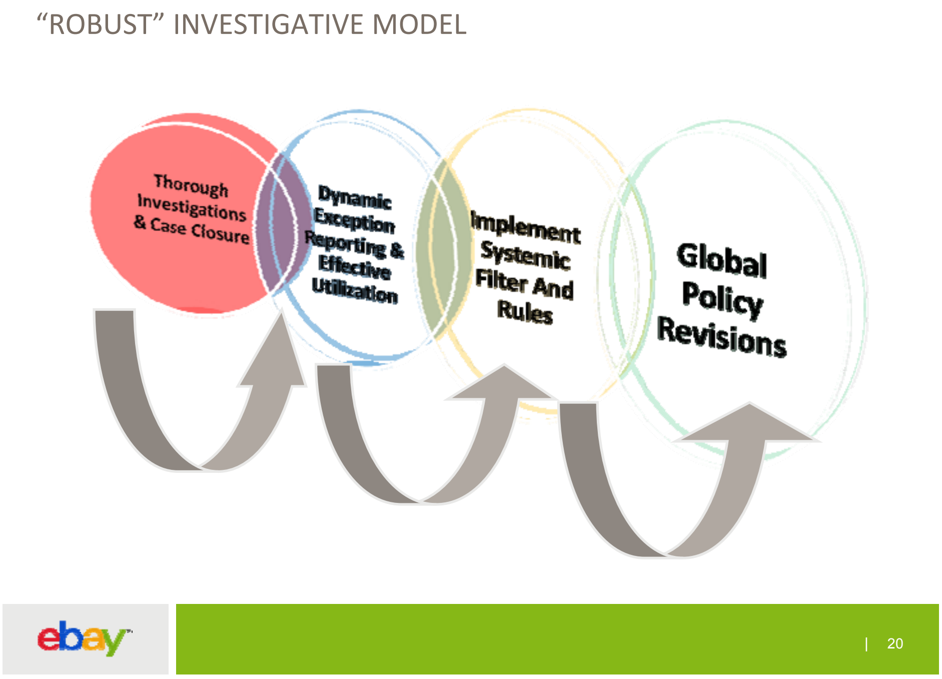
Frauds Targeting Marketplaces

- ➢ Merchant Related Fraud (Non-Receipt/Not as Described)
- ➢ Abuse of eBay Buyer Protection
- ➢ Brand abuse/hijack and offline scams

Frauds Targeting PayPal

- ➢ Identity Fraud and Monetization of credit cards/bank accts
- ➢ Merchant Services Products
  - Virtual Terminal and Payments Pro
  - Prepaid Card Services (MoneyPak/Green Dot)

ebay | 19



"ROBUST" INVESTIGATIVE MODEL

Thorough Investigations & Case Closure
Dynamic Exception Reporting & Effective Utilization
Implement Systemic Filter And Rules
Global Policy Revisions

ebay | 20

GLOBAL LAW ENFORCEMENT AGENCY PARTNERSHIPS

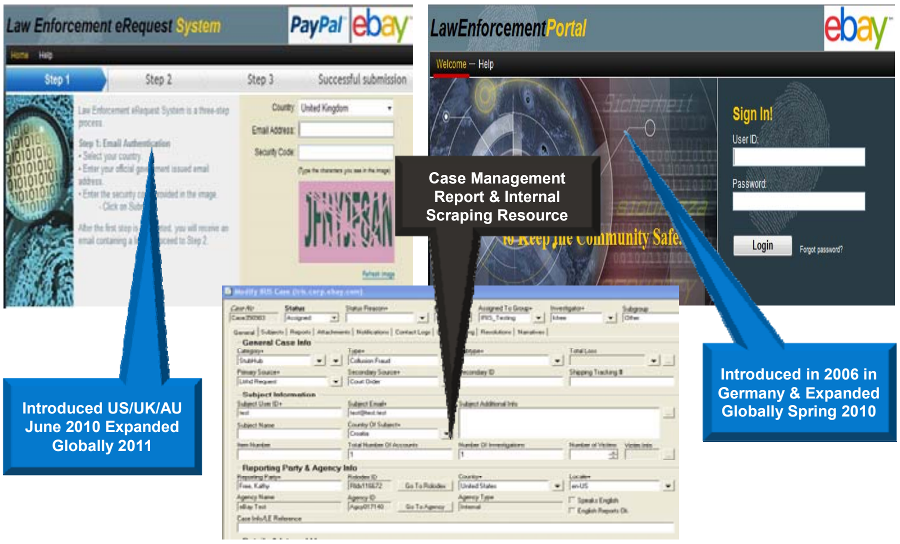
FDA
U.S. Immigration and Customs Enforcement
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
An Garda Síochána Ireland's National Police Service
ActionFraud Report Fraud & Internet Crime
Politie Polite
METROPOLITAN POLICE
CITY OF LONDON POLICE
POLICIA
Bundeskriminalamt BKA
POLIZEI
CARABINIERI
Polisen
POLICJA
AFP
INTERPOL
EUROPOL
FATF-GAFI Financial Action Task Force Groupe d'action financière

Global Crime Intelligence Organizations

European Union

United Nations

Global Law Enforcement Tools



Law Enforcement eRequest System is a three-step process.

Step 1: Email Authentication
- Select your country.
- Enter your official government issued email address.
- Enter the security code provided in the image.
  - Click on Submit

After the first step is completed, you will receive an email containing a link to proceed to Step 2.

Country: United Kingdom

Email Address:

Security Code:

(Type the characters you see in the image)

User ID:

Password:

Case Nr: Case250083
Status: Assigned
Status Reason:
Assigned To Group: IRIS_Testing
Investigator:
Subgroup: Other

General | Subjects | Reports | Attachments | Notifications | Contact Logs | Revolutions | Narratives

General Case Info
Category: StubHub
Type: Collusion Fraud
Subtype:
Total Loss:
Primary Source: Lnfrd Request
Secondary Source: Court Order
Secondary ID:
Shipping Tracking #

Subject Information
Subject User ID: test
Subject Email:
Subject Additional Info
Subject Name:
Country Of Subject: Croatia
Item Number:
Total Number Of Accounts: 1
Number Of Investigations: 1
Number of Victims:

Reporting Party & Agency Info
Reporting Party:
Agency Name: eBay Test
Country: United States
Locale: en-US
Agency Type: Internal
☐ Speaks English
☐ English Reports Ok
Case Info/LE Reference

Introduced US/UK/AU June 2010 Expanded Globally 2011

Case Management Report & Internal Scraping Resource

Introduced in 2006 in Germany & Expanded Globally Spring 2010

CASE STUDY

ANONYMOUS-K41 – LANCIANO (CH), ITALY

Situation

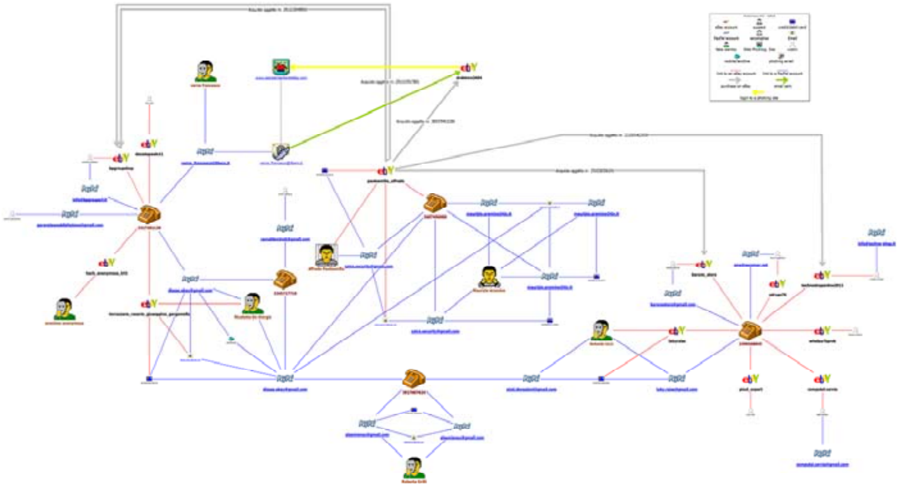
Jul 2012 *a person, using the nickname of "Anonymous-k41" attacks several eBay sellers' accounts.*

We investigate further and find that he is using a combination of **phishing**, **malwares** and **social engineering** in order to take over eBay and PayPal accounts.

At the time when the investigation started the suspect was mainly causing service **disruptions** to and bullying eBay users.

Following the links through different accounts we discovered that the suspect was also responsible for several "traditional" eBay frauds: **INR, SNAD**. Calculated profits: **+€750.000,00** over 2 years.

ANONYMOUS-K41 – LANCIANO (CH), ITALY



ANONYMOUS-K41 – LANCIANO (CH), ITALY

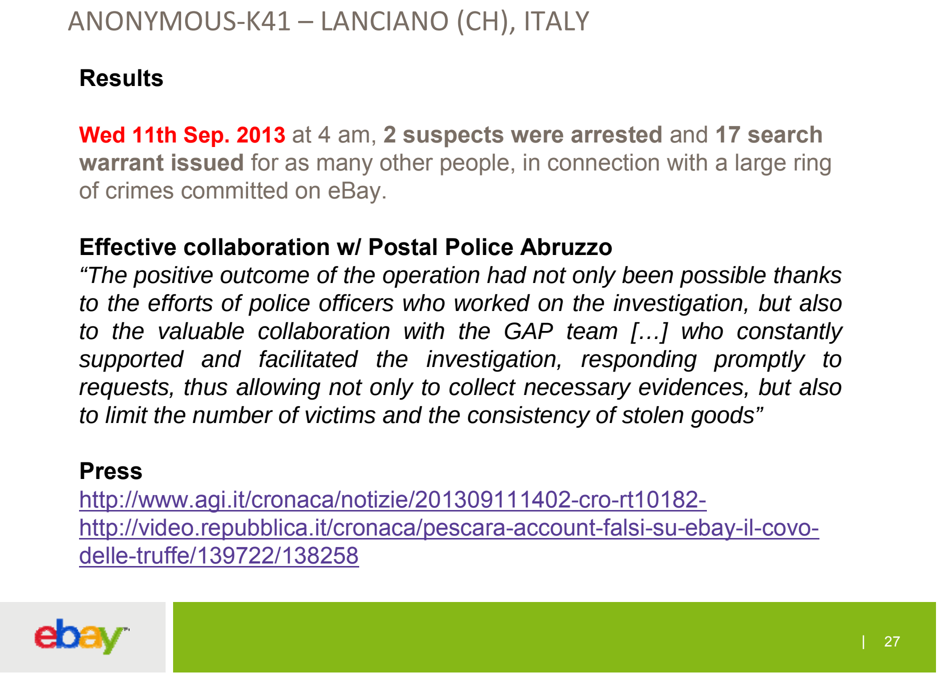
Action

•**Built extensive reports**

•**Assisted** and interviewed the **victims** involved

•**Fed** our findings **back** to the business, helping the improvement of our security measures

•**Identified** and **worked** closely with the local **Law Enforcement agency**, supporting their investigation throughout the last year and half



ANONYMOUS-K41 – LANCIANO (CH), ITALY

Results

Wed 11th Sep. 2013 at 4 am, **2 suspects were arrested** and **17 search warrant issued** for as many other people, in connection with a large ring of crimes committed on eBay.

Effective collaboration w/ Postal Police Abruzzo
"The positive outcome of the operation had not only been possible thanks to the efforts of police officers who worked on the investigation, but also to the valuable collaboration with the GAP team […] who constantly supported and facilitated the investigation, responding promptly to requests, thus allowing not only to collect necessary evidences, but also to limit the number of victims and the consistency of stolen goods"

Press
http://www.agi.it/cronaca/notizie/201309111402-cro-rt10182-
http://video.repubblica.it/cronaca/pescara-account-falsi-su-ebay-il-covo-delle-truffe/139722/138258

| 27

THANK YOU

Biography: Andrea Moretti

Andrea Moretti is eBay Head of Legal Italy, heading up the Legal function for the Italian Marketplace eBay.it and the Classifieds properties eBayAnnunci.it and Kijiji.it.

Mr. Moretti is an Italian qualified lawyer with experience on Corporate, IP, Litigation, Privacy, Regulatory matters and strategic commercial agreements. He graduated and specialized in Information Technology Law.

Before his current role, Mr. Moretti spent previous five years at eBay's HQ in London (UK) advising company's European Business unit on regional compliance and international deals including the expansion of the operations into Russia, Greece, Portugal, Sweden, Czech Republic, Norway and Denmark.

Giancarlo Grasso - Anitec

ANITEC
ASSOCIAZIONE NAZIONALE
INDUSTRIE INFORMATICA, TELECOMUNICAZIONI
ED ELETTRONICA DI CONSUMO

CONFINDUSTRIA

UNICRI - Lucca 29.11.2013

Giancarlo Grasso

FINMECCANICA

CONFINDUSTRIA DIGITALE

MISSION AND VISION

MISSION

Anitec represents companies with operations in Italy that provide ICT services and technologies in the Italian economic, industrial, technological and training environment

VISION

Contribute to the growth and development of our country by promoting the use and application of the most innovative digital technologies

ANITEC GOALS

Promote the development of the ICT sector as generator of growth, competitiveness and sustainability

Foster the development of the digital culture and sustain the implementation of the Digital Agenda.

Cooperate with the Italian institutions as advisor on the strategic choices on ICT strategies and technologies.

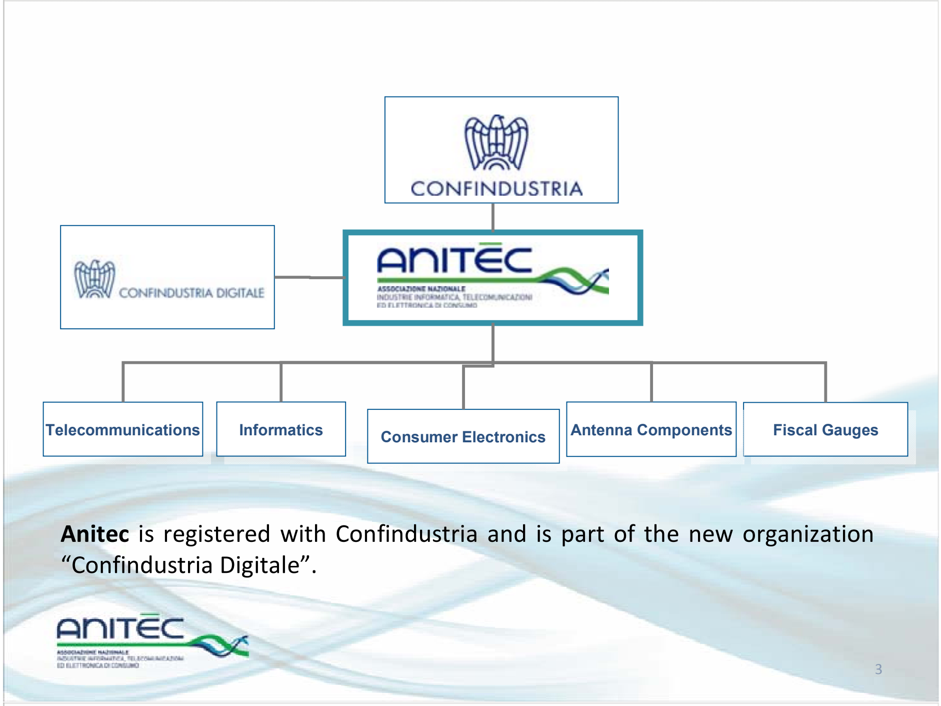
Contribute to the definition of sector specific laws in Italy and in the European Institutions

Promote Italian excellences and its know-how in the global market

Foster the maintenance and the growth in Italy of the entire value chain of the ICT sector.

ANITEC
ASSOCIAZIONE NAZIONALE
INDUSTRIE INFORMATICA, TELECOMUNICAZIONI
ED ELETTRONICA DI CONSUMO

2



CONFINDUSTRIA

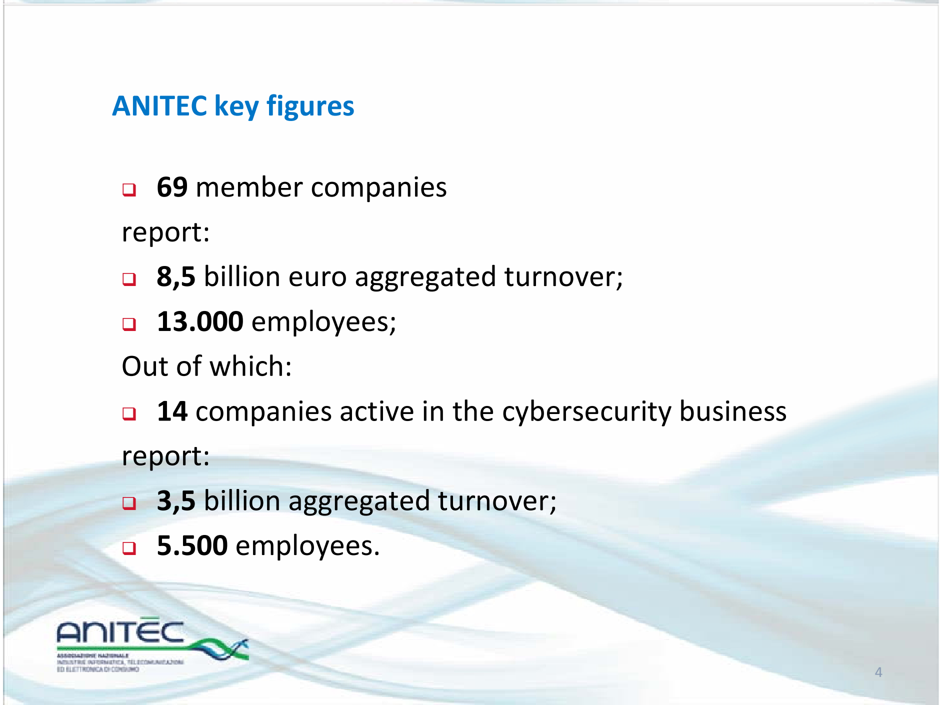
CONFINDUSTRIA DIGITALE

ANITEC
ASSOCIAZIONE NAZIONALE
INDUSTRIE INFORMATICA, TELECOMUNICAZIONI
ED ELETTRONICA DI CONSUMO

Telecommunications | Informatics | Consumer Electronics | Antenna Components | Fiscal Gauges

Anitec is registered with Confindustria and is part of the new organization "Confindustria Digitale".

3



ANITEC key figures

- **69** member companies

report:

- **8,5** billion euro aggregated turnover;
- **13.000** employees;

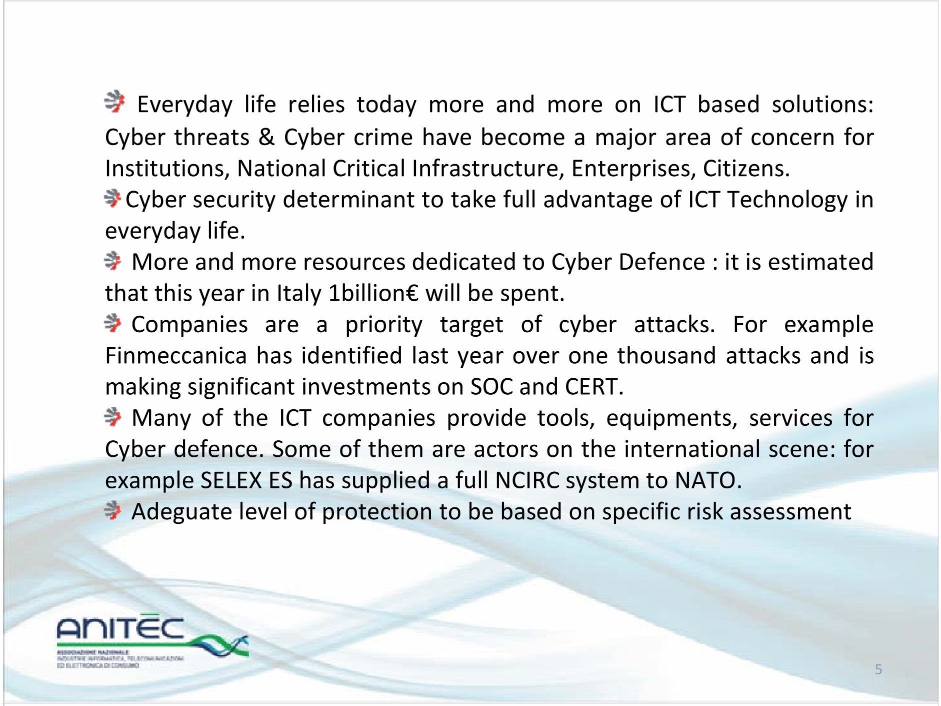
Out of which:

- **14** companies active in the cybersecurity business

report:

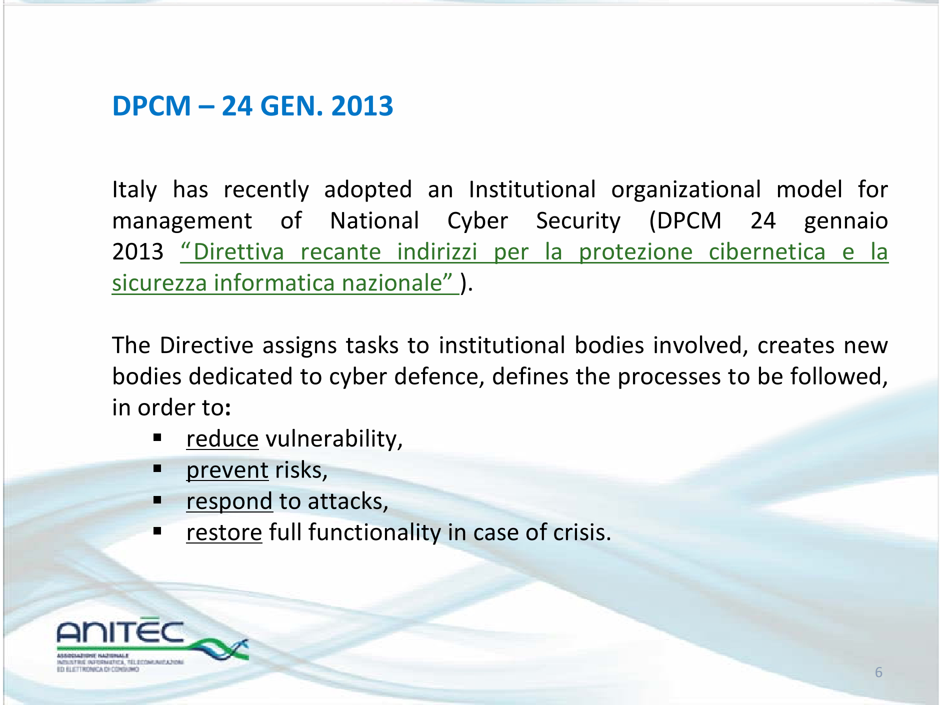
- **3,5** billion aggregated turnover;
- **5.500** employees.

4



- Everyday life relies today more and more on ICT based solutions: Cyber threats & Cyber crime have become a major area of concern for Institutions, National Critical Infrastructure, Enterprises, Citizens.
- Cyber security determinant to take full advantage of ICT Technology in everyday life.
- More and more resources dedicated to Cyber Defence : it is estimated that this year in Italy 1billion€ will be spent.
- Companies are a priority target of cyber attacks. For example Finmeccanica has identified last year over one thousand attacks and is making significant investments on SOC and CERT.
- Many of the ICT companies provide tools, equipments, services for Cyber defence. Some of them are actors on the international scene: for example SELEX ES has supplied a full NCIRC system to NATO.
- Adeguate level of protection to be based on specific risk assessment

5



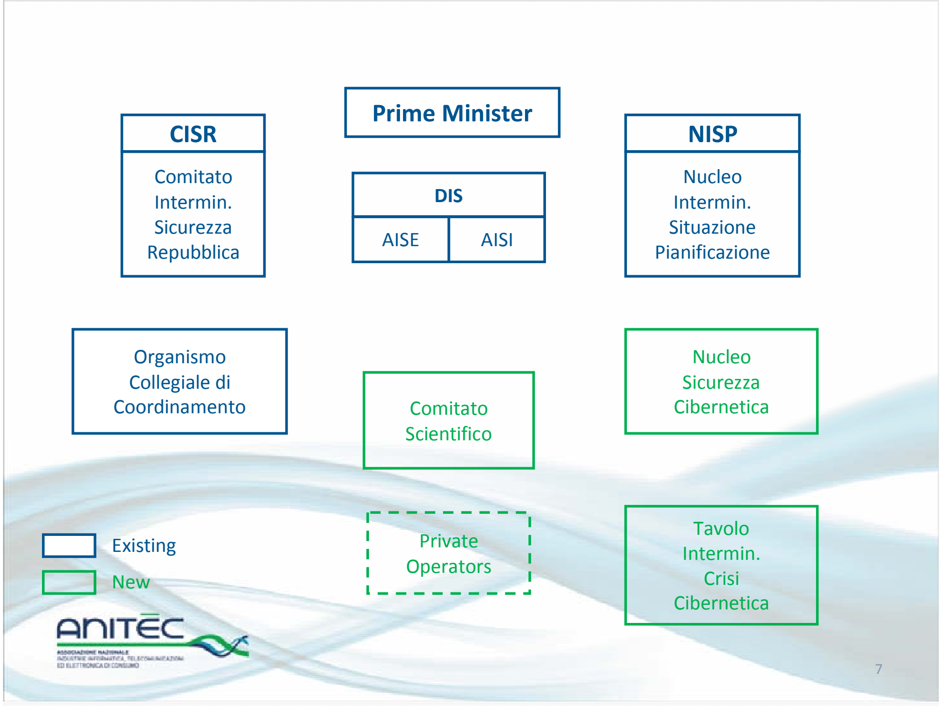
DPCM – 24 GEN. 2013

Italy has recently adopted an Institutional organizational model for management of National Cyber Security (DPCM 24 gennaio 2013 “Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale”).

The Directive assigns tasks to institutional bodies involved, creates new bodies dedicated to cyber defence, defines the processes to be followed, in order to:

- reduce vulnerability,
- prevent risks,
- respond to attacks,
- restore full functionality in case of crisis.

6



Prime Minister

CISR

Comitato Intermin. Sicurezza Repubblica

DIS

AISE

AISI

NISP

Nucleo Intermin. Situazione Pianificazione

Organismo Collegiale di Coordinamento

Comitato Scientifico

Nucleo Sicurezza Cibernetica

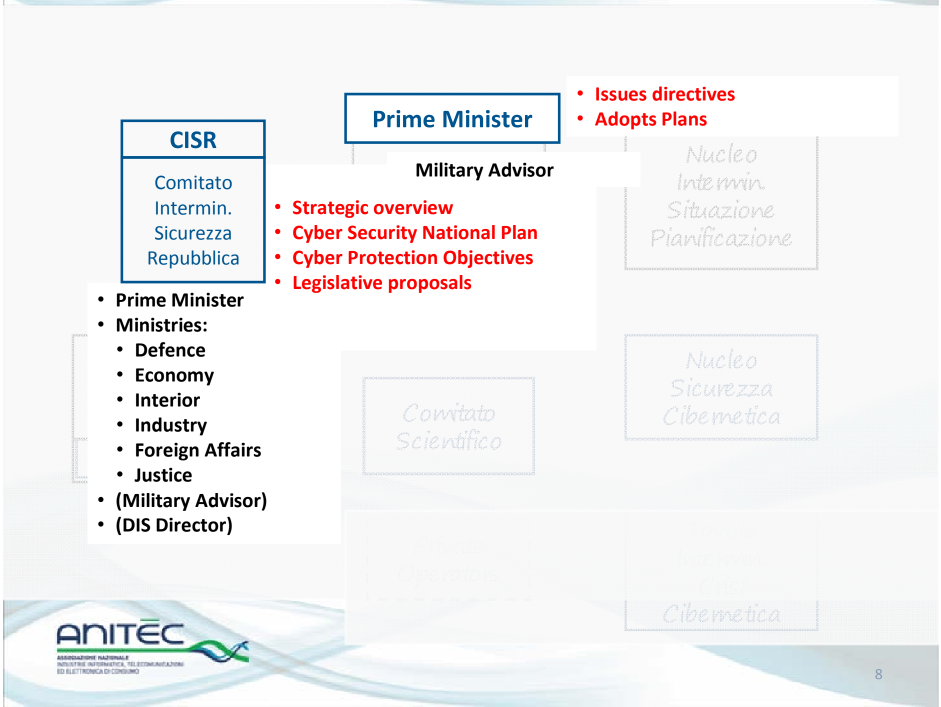
Private Operators

Tavolo Intermin. Crisi Cibernetica

□ Existing

□ New

7



Prime Minister

- Issues directives
- Adopts Plans

CISR

Comitato Intermin. Sicurezza Repubblica

Military Advisor

- Strategic overview
- Cyber Security National Plan
- Cyber Protection Objectives
- Legislative proposals

- Prime Minister
- Ministries:
  - Defence
  - Economy
  - Interior
  - Industry
  - Foreign Affairs
  - Justice
- (Military Advisor)
- (DIS Director)

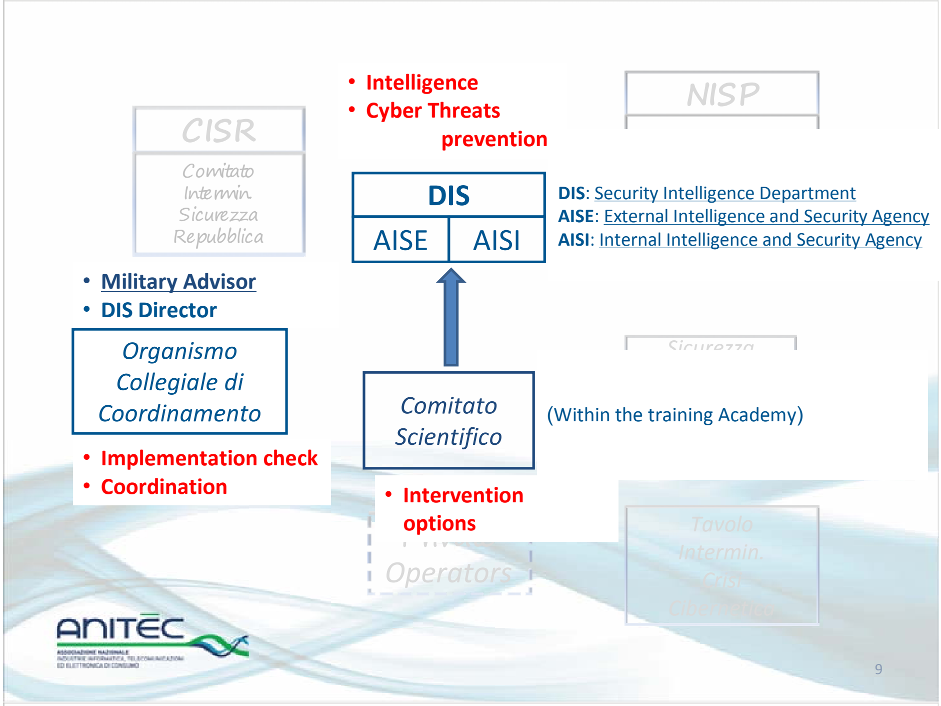
Nucleo Intermin. Situazione Pianificazione

Comitato Scientifico

Nucleo Sicurezza Cibernetica

Cibernetica

8



CISR

Comitato Intermin. Sicurezza Repubblica

- Intelligence
- Cyber Threats prevention

NISP

DIS

AISE | AISI

DIS: Security Intelligence Department
AISE: External Intelligence and Security Agency
AISI: Internal Intelligence and Security Agency

- Military Advisor
- DIS Director

Organismo Collegiale di Coordinamento

- Implementation check
- Coordination

Sicurezza

Comitato Scientifico

(Within the training Academy)

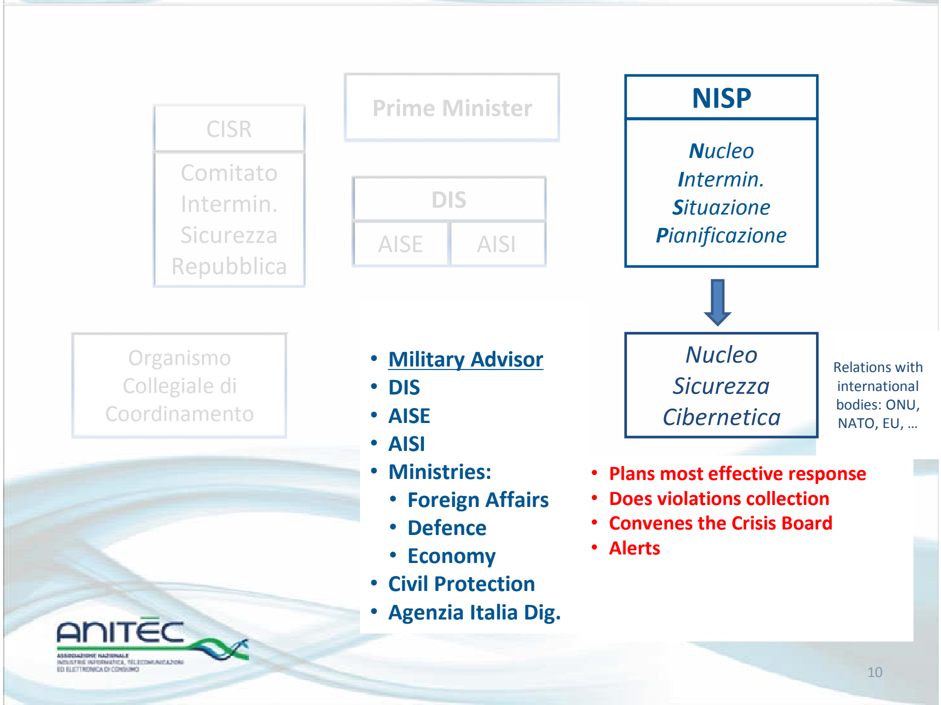
- Intervention options

Operators

Tavolo Intermin. Crisi Cibernetica

ANITEC

9



CISR

Comitato Intermin. Sicurezza Repubblica

Prime Minister

DIS

AISE | AISI

NISP

***N**ucleo **I**ntermin. **S**ituazione **P**ianificazione*

Organismo Collegiale di Coordinamento

- Military Advisor
- DIS
- AISE
- AISI
- Ministries:
  - Foreign Affairs
  - Defence
  - Economy
- Civil Protection
- Agenzia Italia Dig.

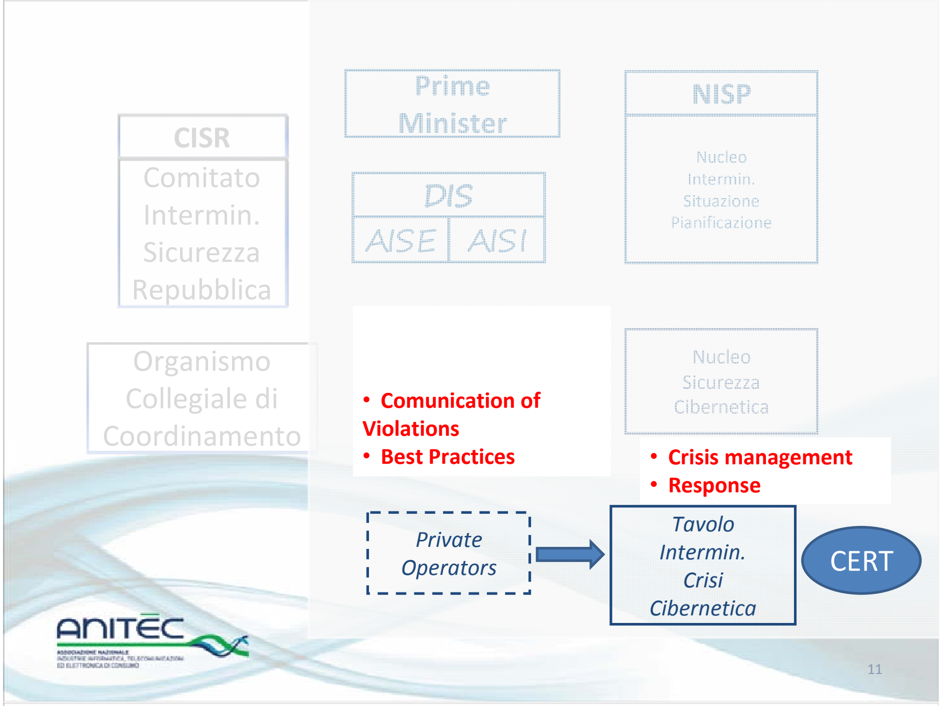
Nucleo Sicurezza Cibernetica

Relations with international bodies: ONU, NATO, EU, …

- Plans most effective response
- Does violations collection
- Convenes the Crisis Board
- Alerts

ANITEC

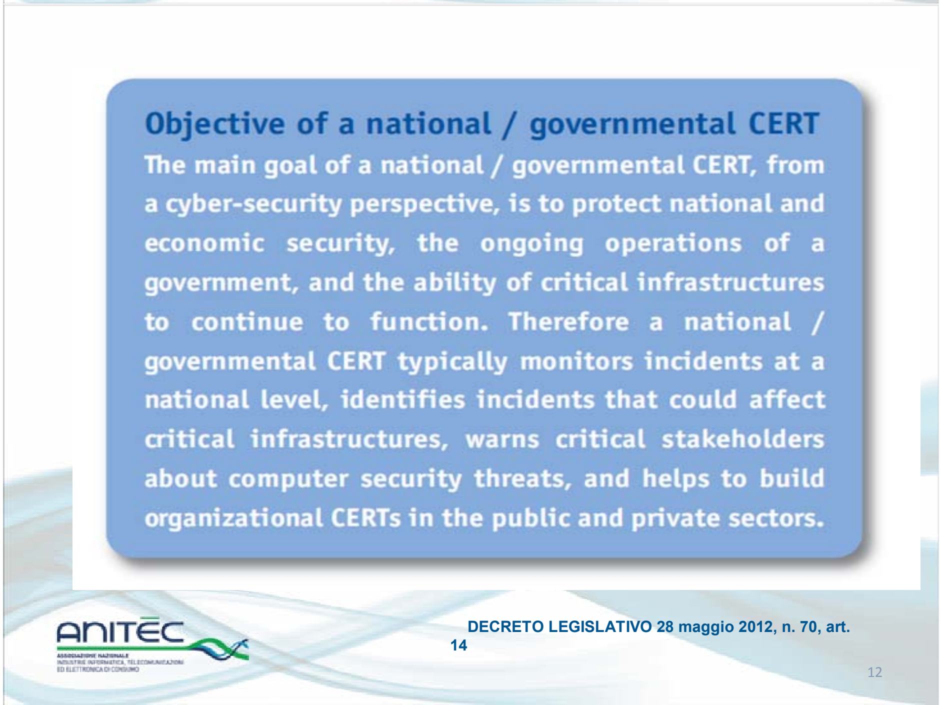
10


CISR
Comitato Intermin. Sicurezza Repubblica
Prime Minister
DIS
AISE
AISI
NISP
Nucleo Intermin. Situazione Pianificazione
Organismo Collegiale di Coordinamento
Nucleo Sicurezza Cibernetica
Private Operators
Tavolo Intermin. Crisi Cibernetica
CERT
ANITEC

- **Comunication of Violations**
- **Best Practices**

- **Crisis management**
- **Response**

11

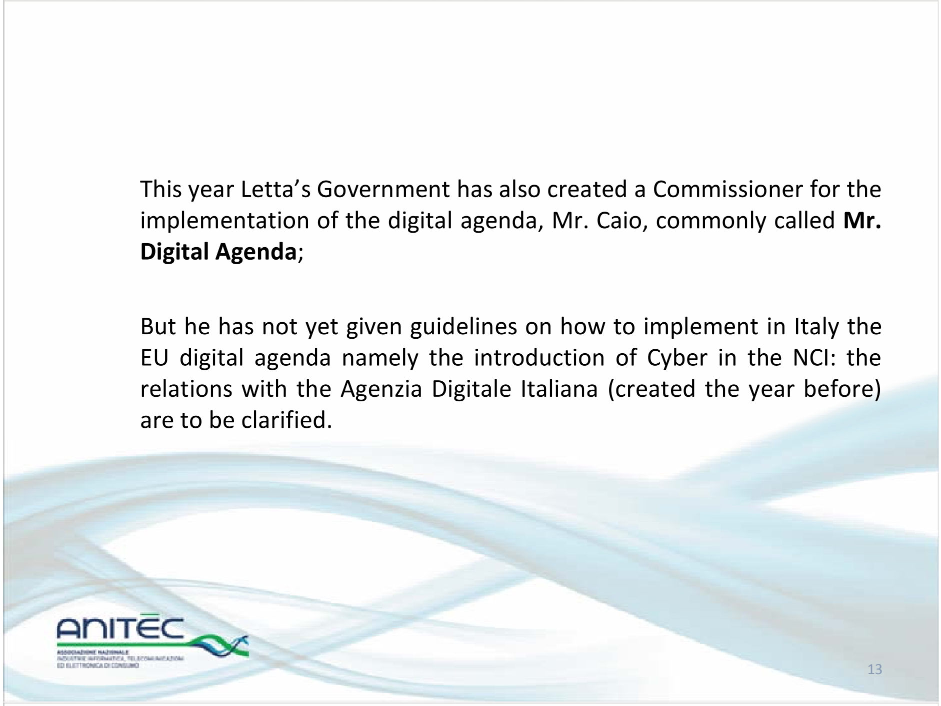


Objective of a national / governmental CERT

The main goal of a national / governmental CERT, from a cyber-security perspective, is to protect national and economic security, the ongoing operations of a government, and the ability of critical infrastructures to continue to function. Therefore a national / governmental CERT typically monitors incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, and helps to build organizational CERTs in the public and private sectors.

DECRETO LEGISLATIVO 28 maggio 2012, n. 70, art. 14

12

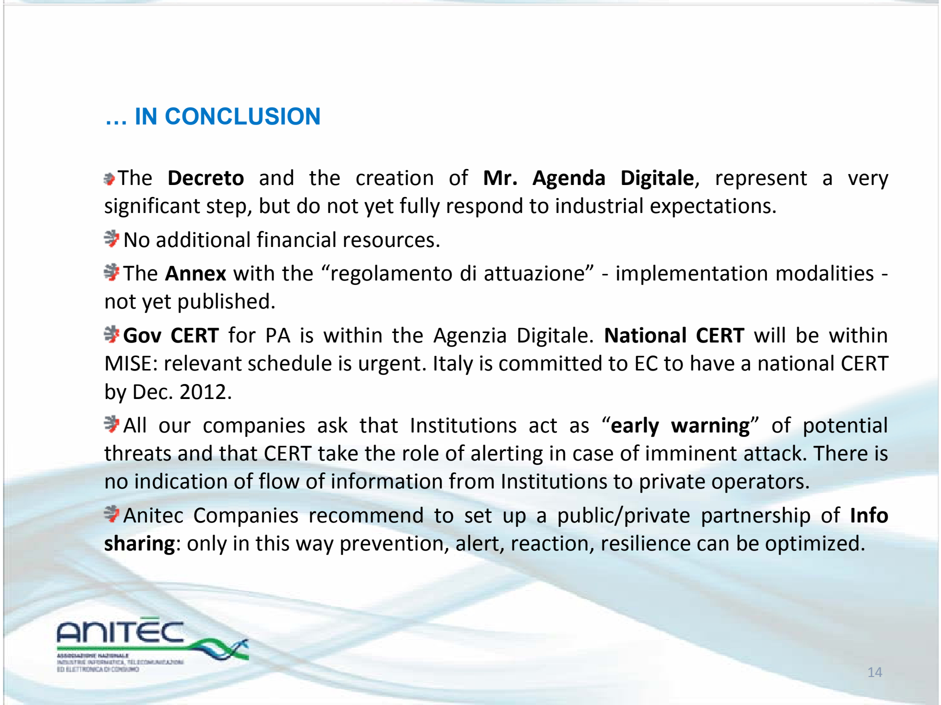


This year Letta's Government has also created a Commissioner for the implementation of the digital agenda, Mr. Caio, commonly called **Mr. Digital Agenda**;

But he has not yet given guidelines on how to implement in Italy the EU digital agenda namely the introduction of Cyber in the NCI: the relations with the Agenzia Digitale Italiana (created the year before) are to be clarified.

ANITEC
ASSOCIAZIONE NAZIONALE
INDUSTRIE INFORMATICA, TELECOMUNICAZIONI
ED ELETTRONICA DI CONSUMO

13



… IN CONCLUSION

- The **Decreto** and the creation of **Mr. Agenda Digitale**, represent a very significant step, but do not yet fully respond to industrial expectations.
- No additional financial resources.
- The **Annex** with the "regolamento di attuazione" - implementation modalities - not yet published.
- **Gov CERT** for PA is within the Agenzia Digitale. **National CERT** will be within MISE: relevant schedule is urgent. Italy is committed to EC to have a national CERT by Dec. 2012.
- All our companies ask that Institutions act as "**early warning**" of potential threats and that CERT take the role of alerting in case of imminent attack. There is no indication of flow of information from Institutions to private operators.
- Anitec Companies recommend to set up a public/private partnership of **Info sharing**: only in this way prevention, alert, reaction, resilience can be optimized.

ANITEC
ASSOCIAZIONE NAZIONALE
INDUSTRIE INFORMATICA, TELECOMUNICAZIONI
ED ELETTRONICA DI CONSUMO

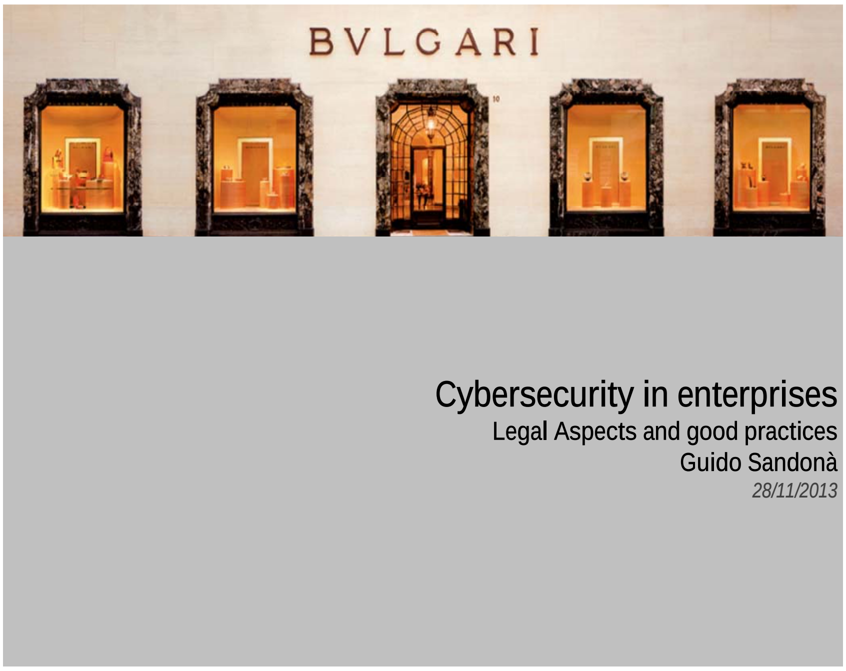
14

Biography: Giancarlo Grasso

Mr. Giancarlo Grasso served as the Chief Technical Officer and Senior Vice President of Product Policy at Finmeccanica SpA. Mr. Grasso serves as a Senior Advisor to the Chairman of Finmeccanica. He served as the Chief Executive Officer of SELEX Galileo S.p.A (formerly Galileo Avionica SpA) of Finmeccanica SpA. He served as the Chief Executive Officer at Finmeccanica SpA and ALENIA SPAZIO S p A since February 6,

2009. He served as the Chief Executive Officer of Selex Communications S.p.A (alternately SELEX Elsag S.p.A.) since February 2009 and Selex Communications, Inc., U.S.A. He serves as the Chairman of the Board at SELEX Galileo S.p.A. and OTO MELARA S.p.A. of Finmeccanica SpA. He serves as a Deputy Chairman of Ansaldo STS SpA. He has been a Director of Eurotech SpA since April 28, 2011.

Guido Sandonà – Bulgari

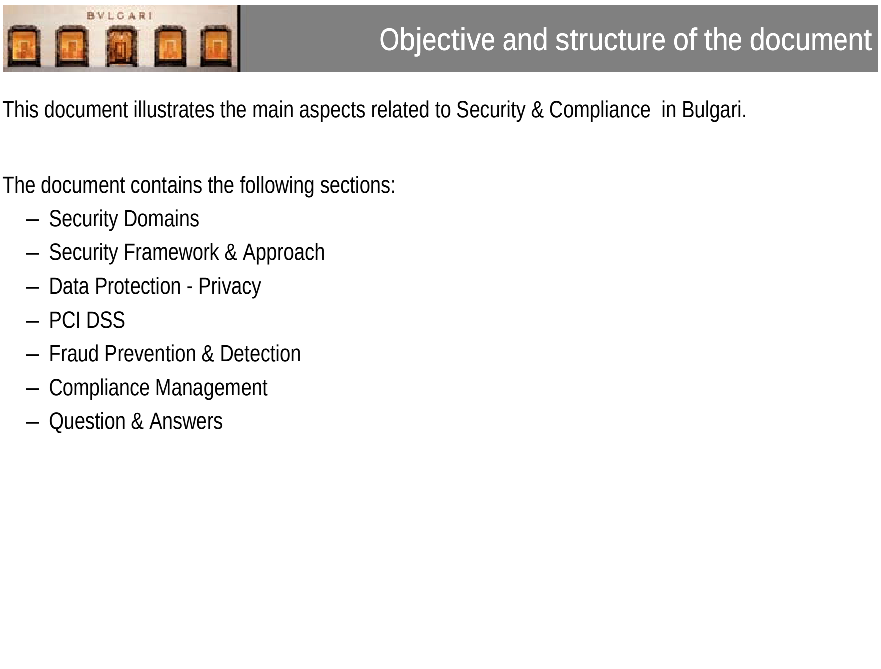


Cybersecurity in enterprises

Legal Aspects and good practices

Guido Sandonà

28/11/2013



Objective and structure of the document

This document illustrates the main aspects related to Security & Compliance in Bulgari.

The document contains the following sections:

- Security Domains
- Security Framework & Approach
- Data Protection - Privacy
- PCI DSS
- Fraud Prevention & Detection
- Compliance Management
- Question & Answers

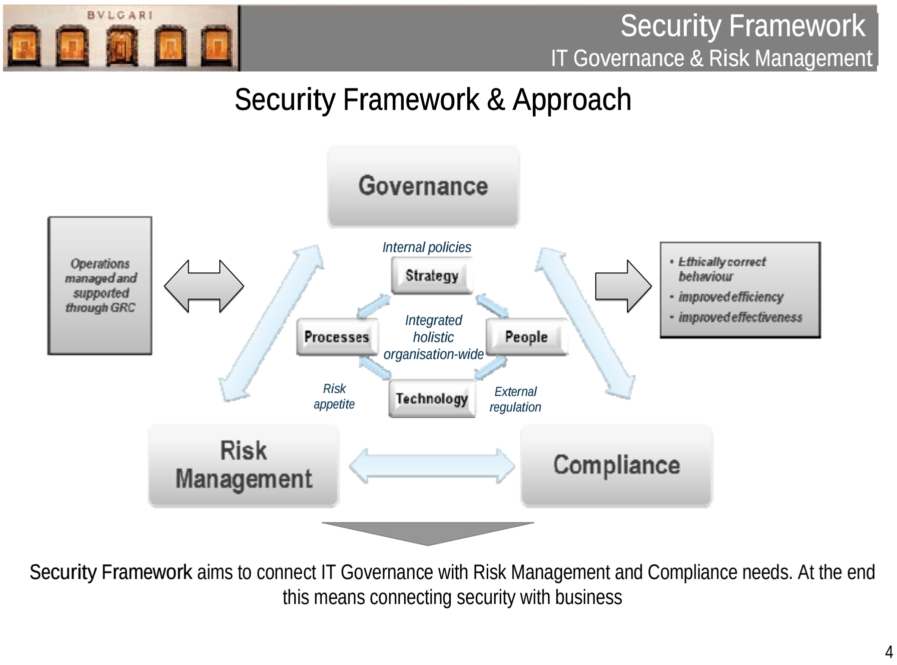
2

BVLGARI

IT Security domains

- Data Protection - Privacy
- PCI -DSS
- Fraud Detection & Pevention
- Segregation od Duties
- Perimeter Security

3



BVLGARI

Security Framework

IT Governance & Risk Management

Security Framework & Approach

Security Framework aims to connect IT Governance with Risk Management and Compliance needs. At the end this means connecting security with business

4

DATA PROTECTION - PRIVACY

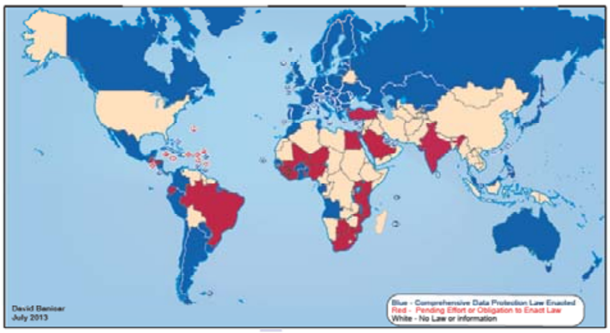
Customer Data Protection

CRM Activities

International Data Protection Laws

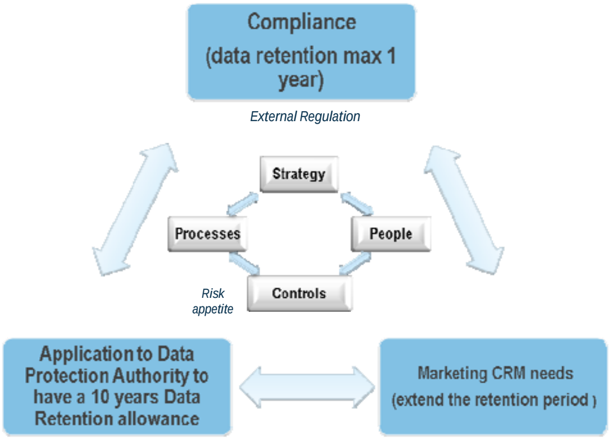
World Wide Data Protection Mapping

National Comprehensive Data Protection/Privacy Laws and Bills 2013


David Banisar
July 2013
Blue - Comprehensive Data Protection Law Enacted
Red - Pending Effort or Obligation to Enact Law
White - No Law or information

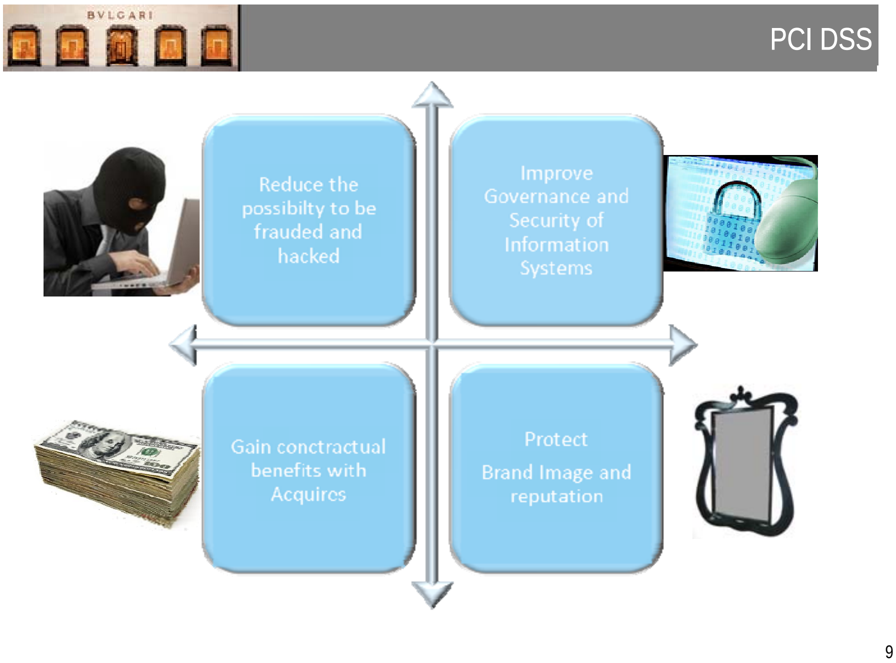
Customer Data Retention

Customer Data Retention


Compliance
(data retention max 1 year)
External Regulation
Strategy
Processes
People
Controls
Risk appetite
Application to Data Protection Authority to have a 10 years Data Retention allowance
Marketing CRM needs
(extend the retention period)

PCI DSS

PCI-DSS
Payment Card Industry – Data Security Standard



BVLGARI

PCI DSS

Reduce the possibilty to be frauded and hacked

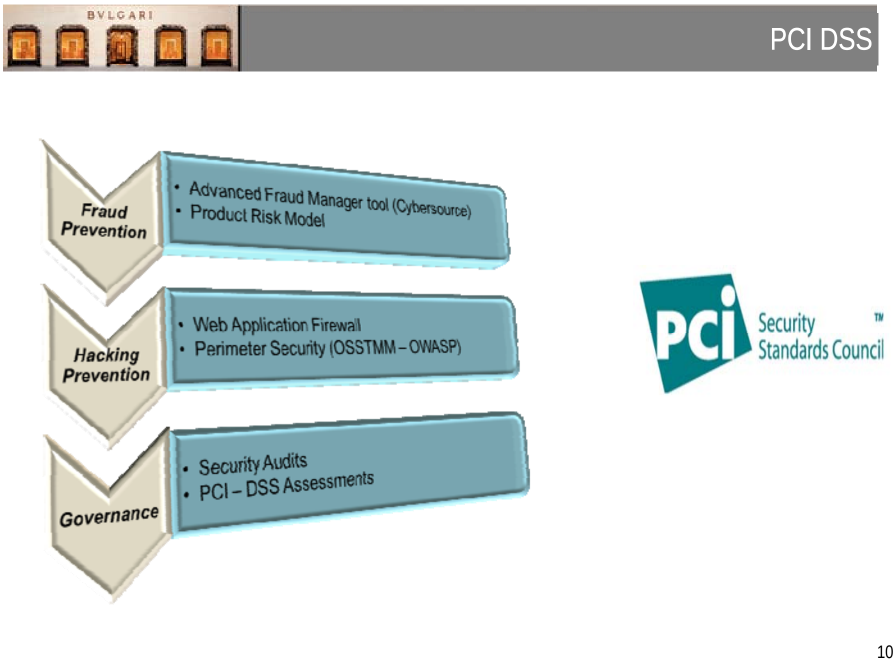
Improve Governance and Security of Information Systems

Gain conctractual benefits with Acquires

Protect

Brand Image and reputation

9



BVLGARI

PCI DSS

Fraud Prevention

- Advanced Fraud Manager tool (Cybersource)
- Product Risk Model

Hacking Prevention

- Web Application Firewall
- Perimeter Security (OSSTMM – OWASP)

Governance

- Security Audits
- PCI – DSS Assessments

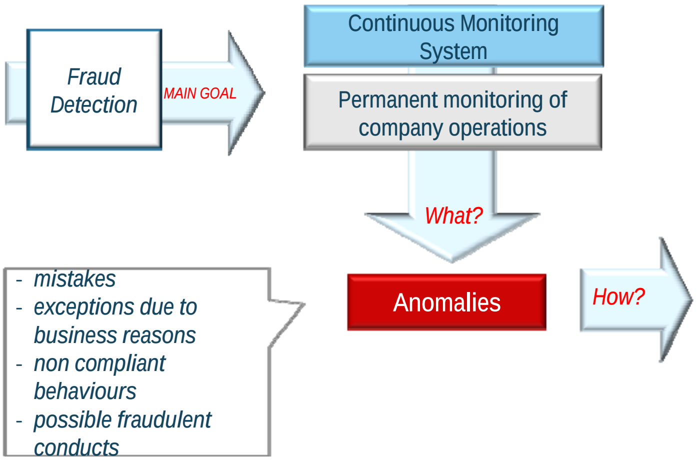
PCI Security Standards Council™

10

FRAUD PREVENTION & DETECTION

FRAUD PREVENTION & DETECTION

Internal Fraud Prevention & Detection



Fraud Detection

MAIN GOAL

Continuous Monitoring System

Permanent monitoring of company operations

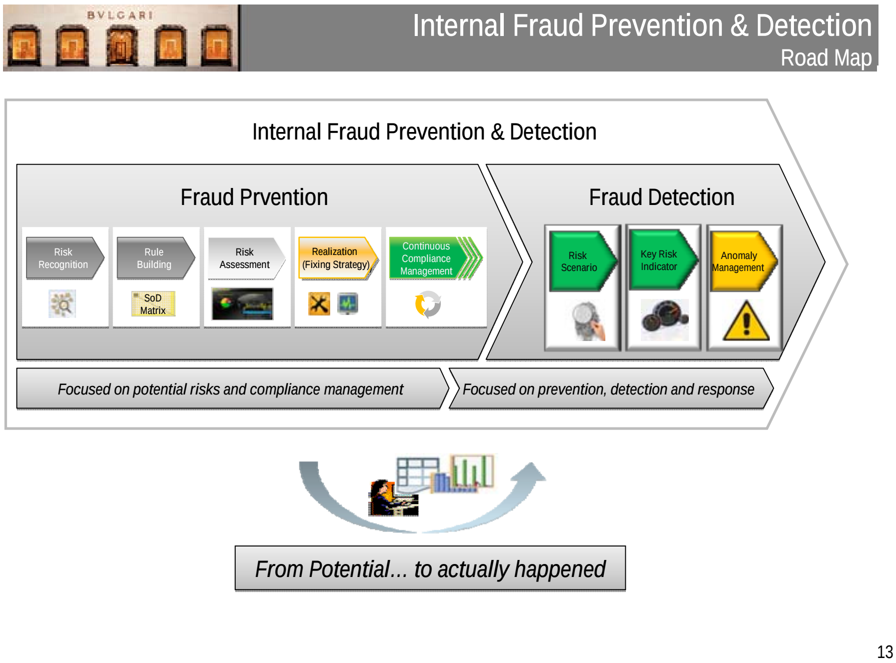
What?

Anomalies

- mistakes
- exceptions due to business reasons
- non compliant behaviours
- possible fraudulent conducts

How?

- Automatic and real time controls
- Controls based on Key Risk Indicators (KRIs):
- Cross-checks of different data
- 100% relevant transactions



BVLGARI

Internal Fraud Prevention & Detection

Road Map

Internal Fraud Prevention & Detection

Fraud Prvention

Risk Recognition

Rule Building

SoD Matrix

Risk Assessment

Realization (Fixing Strategy)

Continuous Compliance Management

Fraud Detection

Risk Scenario

Key Risk Indicator

Anomaly Management

Focused on potential risks and compliance management

Focused on prevention, detection and response

From Potential… to actually happened

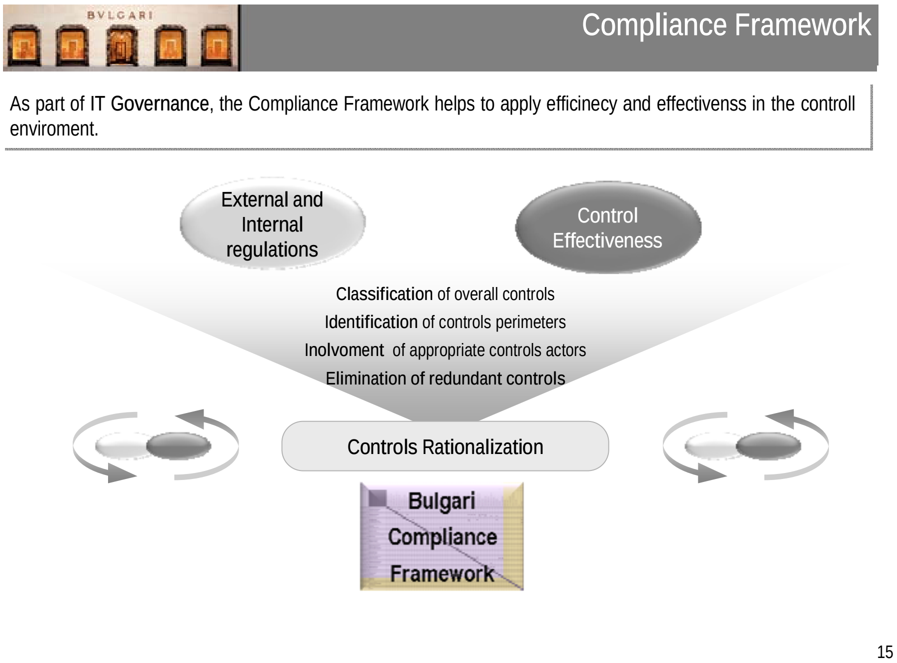
13

BVLGARI

COMPLIANCE MANAGEMENT

Compliance Management

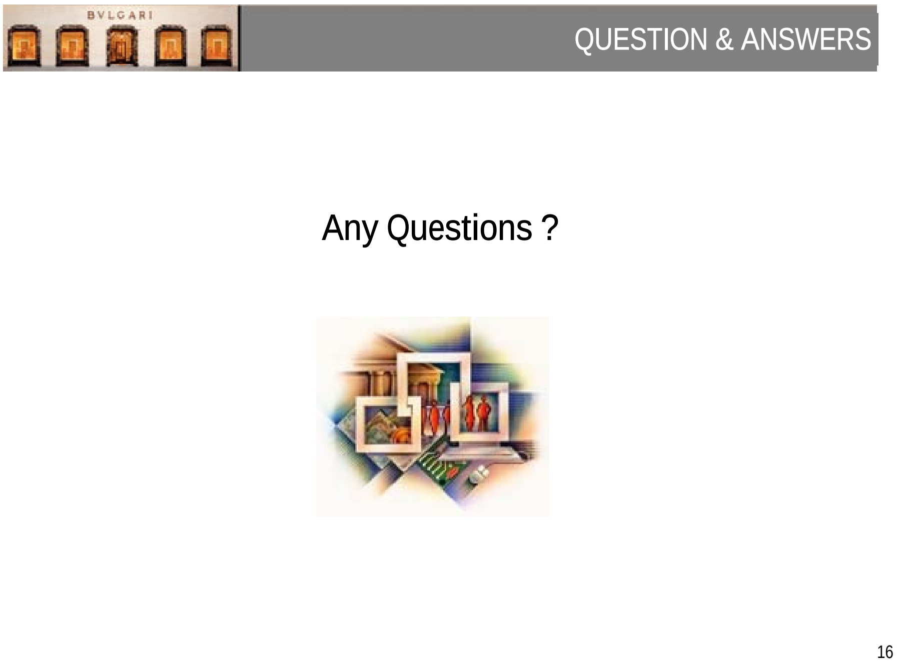
14



Compliance Framework

As part of IT Governance, the Compliance Framework helps to apply efficinecy and effectivenss in the controll enviroment.

External and Internal regulations
Control Effectiveness
Classification of overall controls
Identification of controls perimeters
Inolvoment of appropriate controls actors
Elimination of redundant controls
Controls Rationalization
Bulgari Compliance Framework



QUESTION & ANSWERS

Any Questions ?

Biography: Guido Sandonà

Guido Sandonà is currently the Chief Information Security Officer at Bulgari.

The Road Ahead

UNICRI’s roundtable at Lucca brought together a broad spectrum of actors from the cyber security and business communities to tackle an emerging threat that has no chance of going away anytime soon. Combating cybercrime, therefore, will involve a multidisciplinary approach, involving policy makers, international organizations, various LEAs, cybercrime experts, and representatives from across the private sector, ranging from large corporations to SMEs.

Being aware of the risks associated with cybercrime is key for businesses looking to develop a comprehensive cyber security strategy and to create a culture of security:

Some main points and topics that were highlighted during the various presentations at Lucca are summarized here below:

- Importance of Security-by-Design and Privacy-by-Design
- Need for a commonly agreed methodology for collecting data on cyber crime to understand its size and typologies
- Need for a set of common standard policies and procedures to protect enterprises
- Enhancing enterprises’ knowledge and awareness on security investment
- Increasing consumer awareness of cyber crime
- Ad hoc policies on BYOD (Bring Your Own Device)
- The capacity to understand and evaluate cyber risks
- Understanding the nature and extent of criminal networks online
- Tracking money flows online
- The need to create trust between the private sector and the law enforcement
- Need for regulatory measures for Public Private Partnerships
- The creation of guidelines/platforms for information sharing in Public Private Partnerships
- Respecting data protection and human rights while investigating cyber crime
- for the importance of multidisciplinary training for all actors involved in fighting cyber crime and enhancing cyber security
- Need for multilevel awareness raising initiatives

Work on the awareness raising strategy promoted at Lucca will continue throughout the year. A study on the topic of cybercrime, as it pertains to risks for the economy and enterprises, will be completed in the fall of 2014, with a presentation conference planned for the end of the year.