Organized Crime, Cybercrime and Counterfeiting

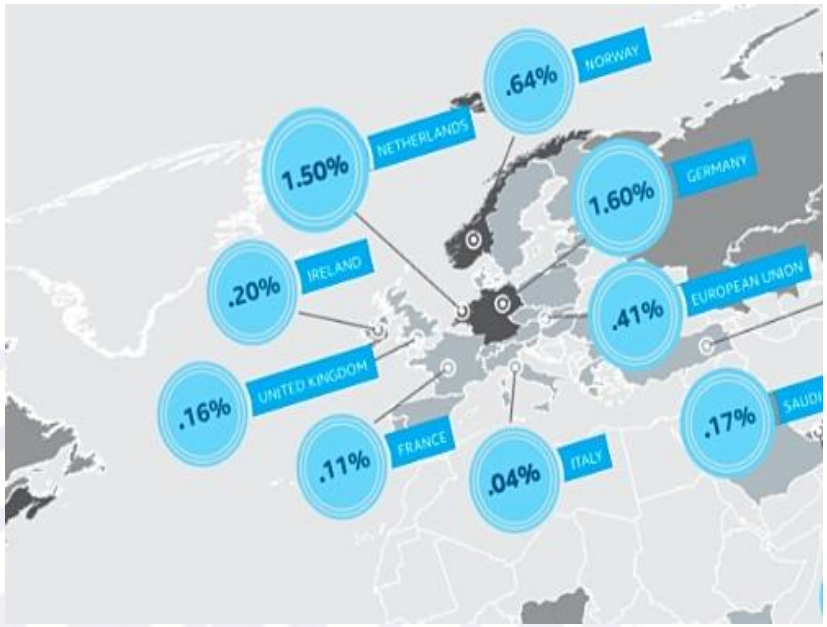
Francesca Bosco

UNICRI Project Officer

The Dark Side of E-Commerce, Zurich, 31 August 2016

The phenomenon is difficult to estimate

In general **cybercrime is increasing in scale and impact**; while there is a lack of reliable figures, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage.



Source: CSIS

Issues:

- Low percentage of incident reporting
- Lack of accurate statistics
- Anonymity

Consequence:

Difficulties to understand the problem and its consequences (damages/costs)

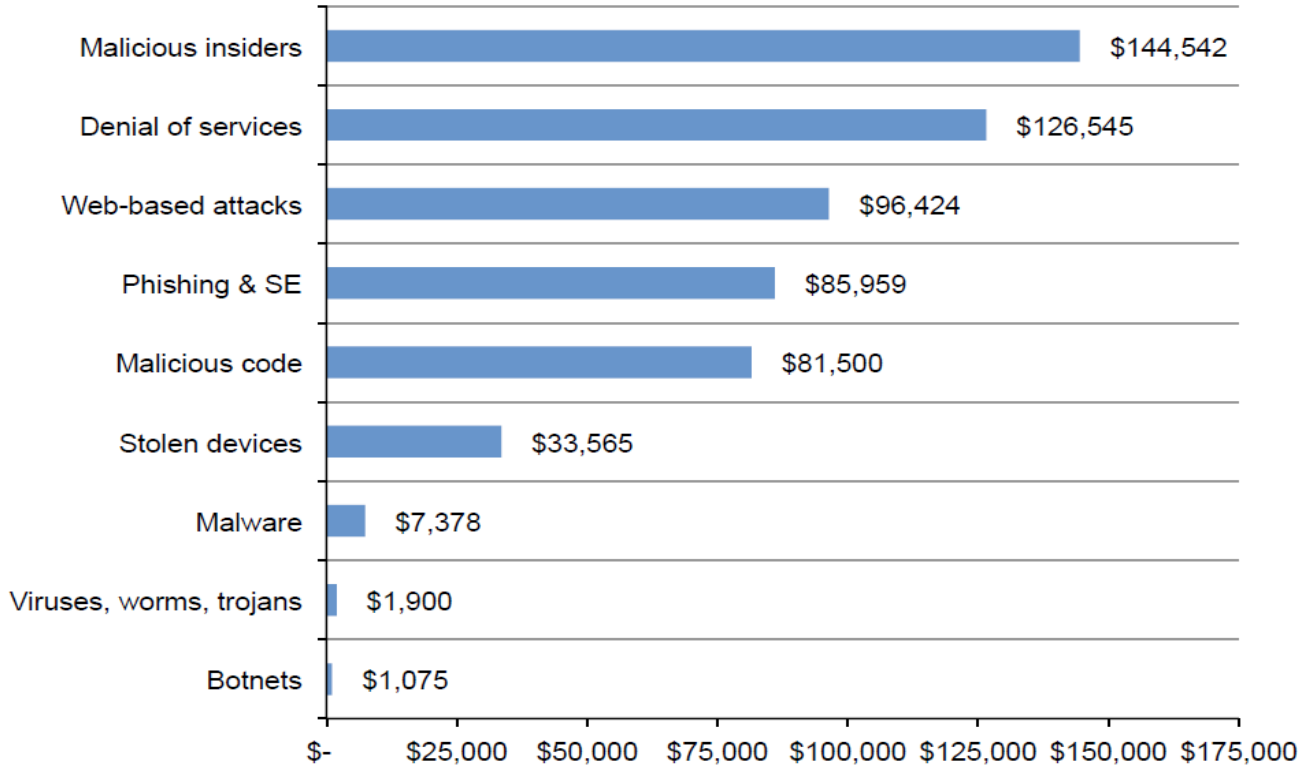
Estimating global loss from incomplete data

Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. If estimates are right, cybercrime extracts between 15% and 20% of the value created by the Internet.

McKinsey & Company estimates that cyber attacks will slow the pace of technology and business innovation over the next few years and cost the economy as much as $3 trillion annually.

In perspective: approximating the Enormous Cost of Cybercrime

Figure 11. Average annualized cyber crime cost weighted by attack frequency
Consolidated view, n = 252 separate companies

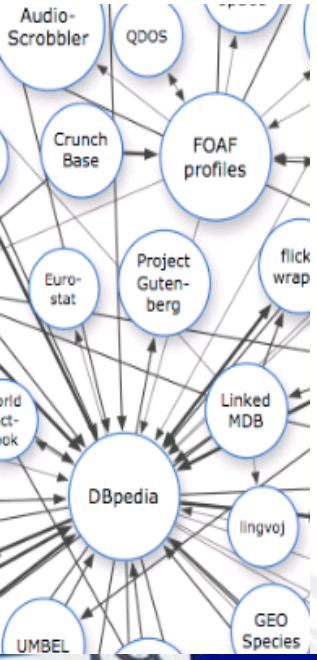


Source: Ponemon Institute, Annual Cost of Cybercrime 2015

Different threats

- Fraud
- Sensitive data and intellectual property theft
- Extortion
- Demonstrative attacks
- Identity theft
- Espionage
- Sabotage

What are cybercriminals interested in?



Data: is more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money or for further leverage.
(payment data, authentication,medical records, classified info)

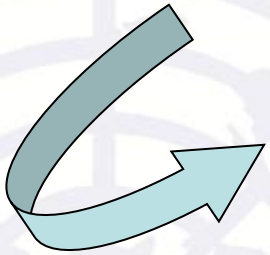
Intellectual property: keep in mind

- a database of credit cards = easy to monetize
- a database of IP = monetizing stolen IP is much harder BUT also much more lucrative if done correctly.

Cyber criminals' attraction for IP

It is difficult to overstate the importance of intellectual property to economic prosperity and difficult to gauge the full extent of the damage done by IP theft.

Stolen IP is a subsidy to foreign suppliers that do not have to bear the costs of developing or licensing it.



Stolen blueprints and notes from corporate meetings cause a competitive advantage to criminal firms who copy and fabricate products using the original firms' copyrighted information.

Different types of attackers

- Organized crime groups
- Insiders
- Industrial spies
- Hacktivist
- Wannabe lamer, script kiddie

Cyber criminals' attraction for IP

Intruders in corporate computer networks:

The "opportunistic hacker"

Uses the Internet to run probing attacks against many networks and intrudes wherever he finds vulnerability

The "targeted hacker"

seeks to take specific proprietary information in a specific network belonging to a specific government agency or private company

Some target entities for individual reasons, others are sponsored by a government agency, often for direct military aims or to damage military networks. Other targeted hackers seek to intrude on behalf of a foreign corporate competitor, often to take specific information to gain a business advantage.

The Evolving links between Cybercrime and Organized Crime

unicri
United Nations Interregional Crime and Justice Research Institute

The Dark Side of E-Commerce, Zurich, 31 August 2016

The New Face of Organized Crime

Hackers are no longer lone wolves. They're now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

80%

of cyber-attacks are driven by **organized crime rings**, in which data, tools, and expertise are widely shared.[1]

Source: SecurityIntelligence, April 2015

The winner is…
Transnational organized crime + Cybercrime

Main elements of success:

- Profit oriented
- Enterprise driven
- Strategic alliances
- Multi-ethnic
- Multi-jurisdictional
- Corruption
- Hyper- connectivity=growing field with guaranteed opportunities
- Hacking Prêt-à-porter

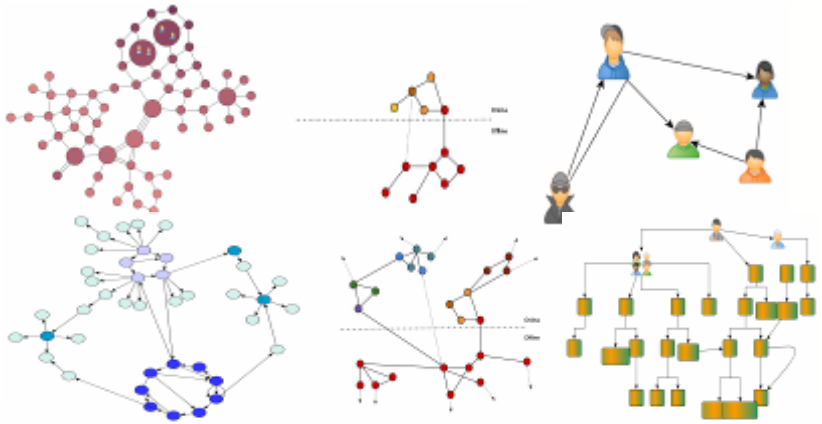
Organized crime typologies in cyberspace

Activities:

- **Type A:** activities directed towards the digital environment
- **Type B:** activities that switch between and across online and offline contexts
- **Type C:** activities predominantly centered on offline criminal projects, but which increasingly intersect with digital environments.

Organization:

- **Type A:** Swarms
- **Type B:** Clustered Hybrids
- **Type C:** Aggregates
- **Type D:** Hubs
- **Type E:** Extended Hybrids
- **Type F:** Hierarchies



Case example: The Big Circle Boys

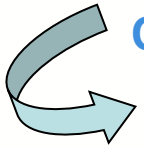
The Canadian government's Criminal Intelligence Service reports that Asian based organized-crime groups, such as the Big Circle Boys, in the lower mainland of British Columbia are involved in large-scale importing and distribution of counterfeit tobacco and consumer goods, as well as in cyber-crimes (identity theft, reproduction of fraudulent credit cards, phone cards, and hotel card keys).

The Big Circle Boys, born of the Red Guards and specializing in loan sharking and drugs, are among many Asian organized-crime groups dealing in counterfeit goods, including pirated films.

It is reported that the Big Circle Boys have cells throughout North America.

Service-Based Industry

- Traditional organized crime groups (including those with a mafia-style structure) use the service based nature of the cybercrime market to carry out more sophisticated crimes, buying access to the technical skills they require.



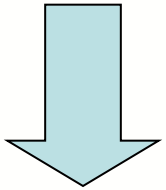
Cybercrime trend -> more transactional and less structured models for future crime?

- Underground forums provide cyber-criminals with a hub for networking, creating an organized set of criminal relationships from an otherwise disparate population.

- Anonymisation, encryption and virtual currencies exploited by cybercriminals – challenges for law enforcement.

- Malware is becoming increasingly sophisticated, intelligent, versatile, available, and is affecting a broader range of targets and devices.

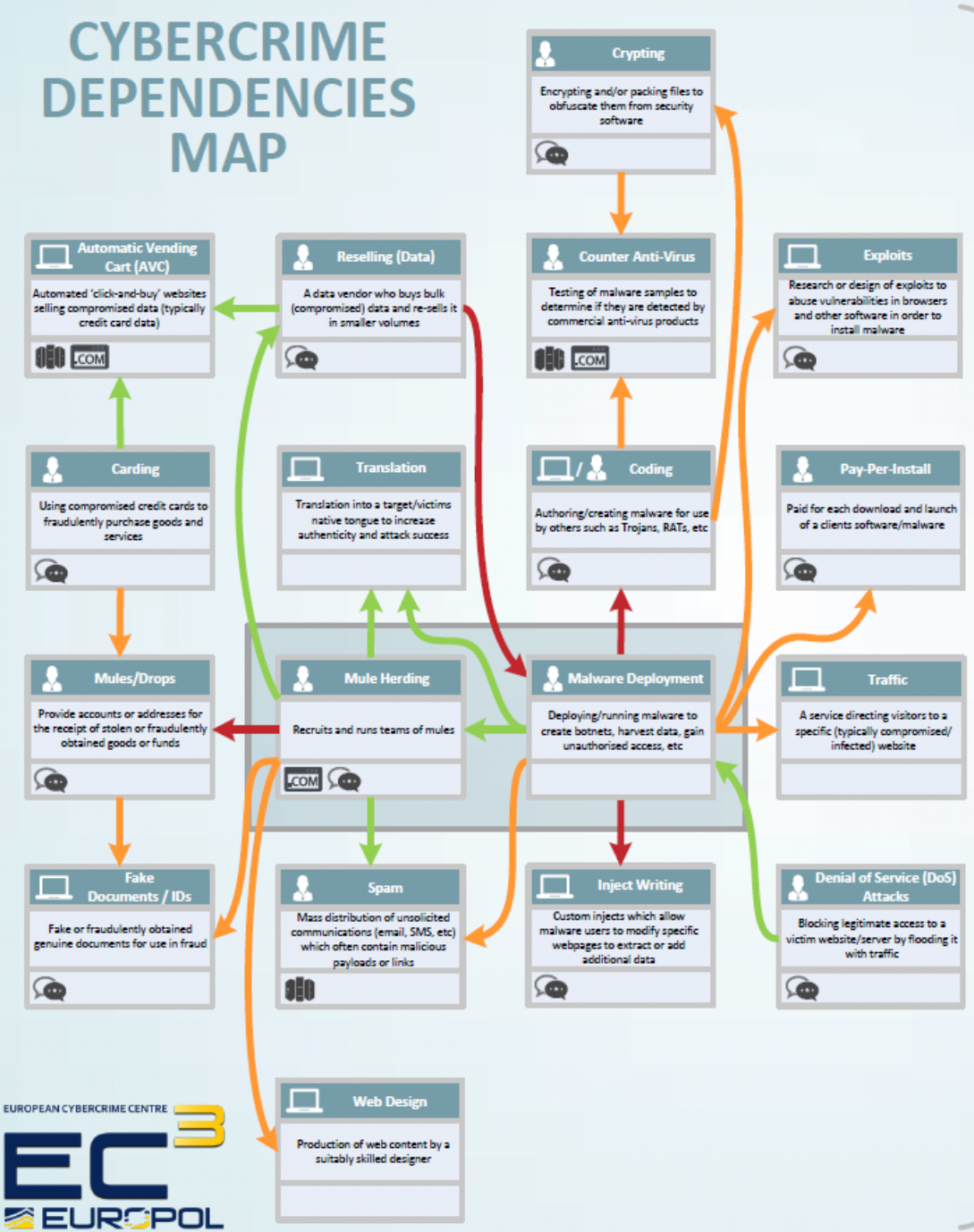
It’s a business - we need to think in business terms



Growth, evolution, processes of specialization and componentization are part of it.

Specialization has allowed hacking “corporations” to grow, taking advantage of the same compartmentalization of any major business. As members of the team grow into their roles they become increasingly skilled at narrow sets of an operation, whether it’s moving stolen merchandise, identifying targets or coding the necessary malware.

CYBERCRIME DEPENDENCIES MAP



Cross-Crime Factors

Hosting (Bulletproof)
Dedicated/shared/virtual hosting which may be non-compliant to law enforcement requests

Forums
Online bulletin boards used as meeting places and markets by cybercriminals to sell products/ services

Domain Services
Provision of generic and countrycode Top Level Domains (gTLDs and ccTLDs)

VPN / Proxy Services
Anonymising services which masks a user's original IP address and can encrypt their internet traffic

Currency Exchange
Exchange between virtual and other (virtual or fiat) currencies

Mixer / Tumbler
A money-laundering service which hides a virtual currency financial trail by pooling and redistributing clients funds

Secure Communications
Secure (e.g. encrypted, un-logged) email and/or instant messaging

The **Cybercrime Dependencies Map** is designed to outline the key products and services within the digital underground and to highlight how and to what degree these products and services are *DEPENDENT* on each other to operate. For example, **Mule Herding** has a *HIGH DEPENDENCY* on the availability of **Mules**.

Several products or services are commonly required by many other services in order for them to operate. These have been collected under **Cross-Crime Factors**. Where one of these **Cross-Crime Factors** has been assessed as being of *HIGH* or *MEDIUM* importance to some of the key products/services it has been allocated an icon in order to annotate the appropriate product/ service.

Mouse over the arrows to see the level of dependency between products and/or services.

LEGEND

Highly dependent on - Cannot do without

Key product/service but not essential

'Optional' service

Product/Service
Product/Service Description
Cross-Crime Factors upon which this service has a High/Medium dependence

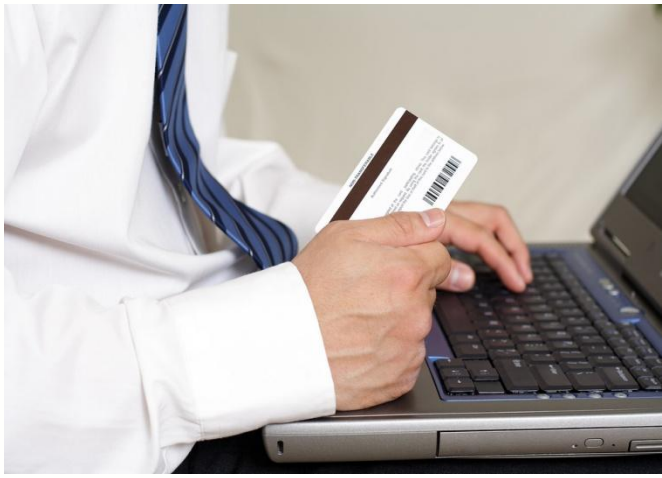
Product
Where the customer is required to do everything themselves after purchase

Service
Where a product involves on-going interaction or is run and maintained by someone else

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Europol Public Information

E-Commerce



E-commerce related fraud has increased in line with the growing number of online payments, affecting major industries such as airlines and hotels.

Key factors:

- Large-scale data breaches supplying compromised card data to underground forums
- Generalized lack of implementation of preventive measures by merchants and the financial industry

Conclusions from the study

- Many online business models infringing IPRs are based on generally applicable legal online business models; revenue sources also appear to be the same whether they are direct sources such as sales revenue or indirect revenue such as pay-per click fees or income from providing advertising space.

- Customers' deception appears to be the marking spot of online business models infranging IPR. In some instances, the infringement of the IPR is carried out openly, but the business model is still deceptive towards the customers due to dissemination of malware.

- Specific online business models benefit from infringement of IPRs (revenue from phishing e-mails, dissemination of ransomware or other fraudulent activities)

- Vendors often either conceal their identities by using privacy shield services for the registration of their domain names, or they provide false contact details on the website – challenge for law enforcement

Shift of IPR-infringing services to the Darknet

- An increasing number of providers of IPR-infringing goods and services are moving their businesses to the Darknet or are offering their services on both the open and the hidden part of the internet

Providers are more anonymous and cannot be easily identified

- Customers' deception appears to be the marking spot of online business models infranging IPR. In some instances, the infringement of the IPR is carried out openly, but the business model is still deceptive towards the customers due to dissemination of malware.

- Specific online business models benefit from infringement of IPRs (revenue from phishing e-mails, dissemination of ransomware or other fraudulent activities)

IP theft case: Stolen trade secrets by Chinese wind turbine firm

- In 2013, the U.S. Department of Justice has charged the Chinese wind turbine firm “Sinovel”, one of the largest in the country, and two of its employees, alleging the group stole trade secrets from an American supplier in an act of "attempted corporate homicide”.

- Sinovel used the technology stolen from computers of US company AMSC in four turbines that were sold to customers in Massachusetts and installed not far from AMSC's headquarters.

- Sometimes such acts of IP theft can destroy most or all of the value of individual companies. A case in point noted by the IP Commission is American Superconductor: When it “had its wind-energy software code stolen by a major customer in China, it lost not only that customer, but also 90% of its stock value.”

Conclusions

- IP rights are essential drives to foster innovation, creativity and economic growth. Protecting Intellectual Property Rights is fundamental to achieve progress in any field. On the other hand, IP-right violations, including counterfeiting and piracy, negatively affect the economy, society, its citizens and its consumers.

- Counterfeiting and piracy are increasingly widespread and no longer limited to luxury items: it affects all types of goods (books, shoes,DVDs, games, medicines, electrical equipment, chemicals, tools, mobile phone batteries, and so on…)

- The globalization of economies and the more widespread use of the Internet have benefited not only legitimate business but also the expansion of IP crime.

Conclusions

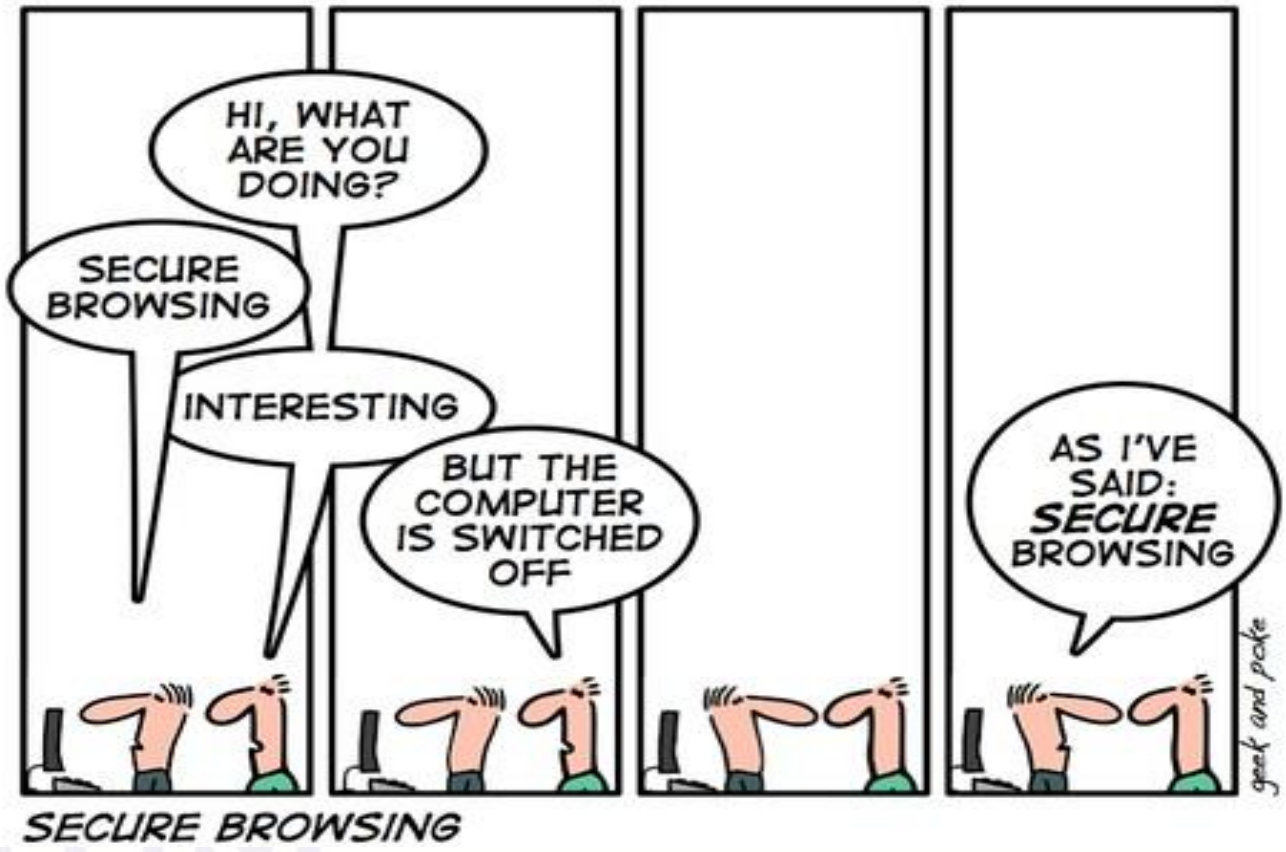
- Data, personal information and patents can be an incredibly lucrative business for criminals and organized crime and the Internet allows for facilitating conditions to commit IP theft and cybercrimes, in lack of adequate and uptodate security measures.

- Gangs and organized crime are known to be in this business – examples of counterfeit DVDs, medicines, luxury items... Links are incresingly being found between common crimes and cybercrime.

- It is pivotal to protect all kinds of data against unlicensed use, especially considering the new possibilities given by the Internet.

unicri
United Nations Interregional Crime and Justice Research Institute

QUESTIONS?


HI, WHAT ARE YOU DOING?
SECURE BROWSING
INTERESTING
BUT THE COMPUTER IS SWITCHED OFF
AS I'VE SAID: SECURE BROWSING
geek and poke
SECURE BROWSING

Contacts

Francesca Bosco: bosco@unicri.it

Project Officer

UNICRI:

http://unicri.it/special_topics/cyber_threats