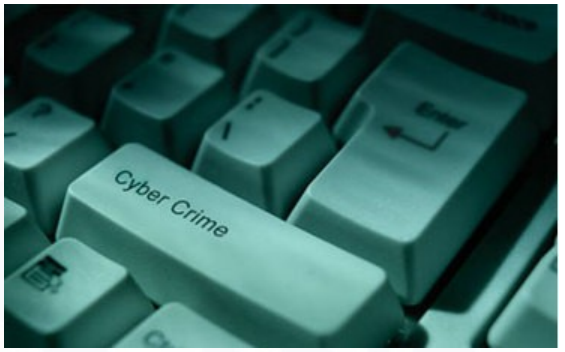
UNICRI and the Assessment of Crime in Cyberspace

25-29 May 2015

WSIS Forum

Francesca Bosco

Project Officer, UNICRI



Presentation Overview:

- Introducing UNICRI
- UNICRI's Cyber Projects
- In focus: SMEs and Cyber Risk
- UNICRI role in "Combating Cybercrime - Tools and Capacity Building for Emerging Economies"
- Conclusions

unicri
United Nations
Interregional Crime and Justice
Research Institute

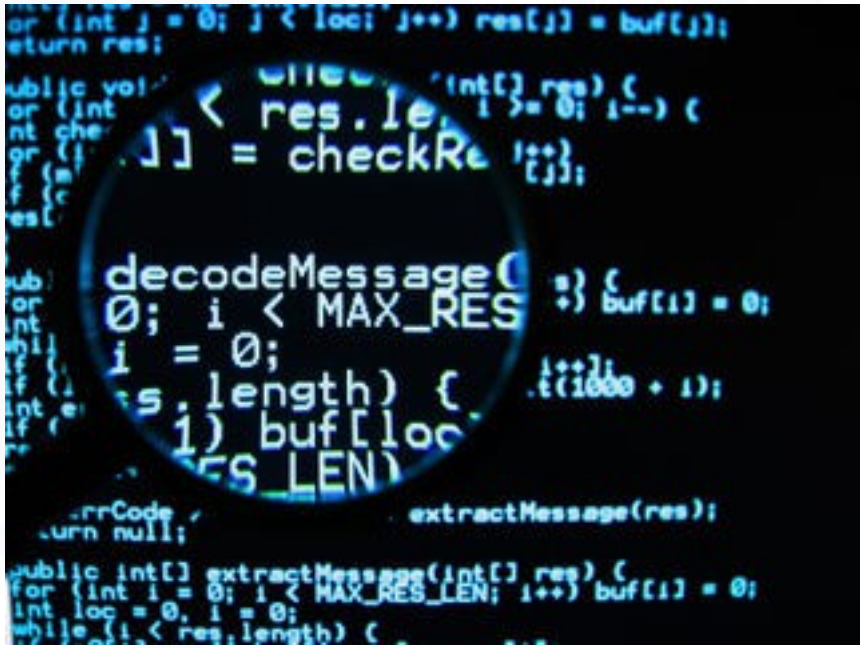
UNICRI's Main Goals

- Advancing an understanding of crime-related issues.
- Fostering just and efficient criminal justice systems.
- Supporting respect for international instruments and other standards.
- Facilitating international law enforcement cooperation and judicial assistance.

UNICRI Emerging Crimes Unit activities

UNICRI's Emerging Crimes Unit tackles organized crime involvement in both established and emerging forms of crime and implements programs for the protection of vulnerable people. In particular, the Institute deals with:

- **Cybercrime**
- Counterfeiting
- Trafficking in persons
- Environmental crimes
- Corruption
- Victim assistance



Why UNICRI is strongly committed to fight cybercrime:

"I urge you to be more innovative when it comes to emerging threats such as cyber-crime, environmental crime and counterfeiting, we must stay one step ahead of the criminals. We must also be more effective in stopping the money flows enabled by corruption and money-laundering"

Ban Ki-moon, 2010

UNICRI's Misuse of Technology Strategy

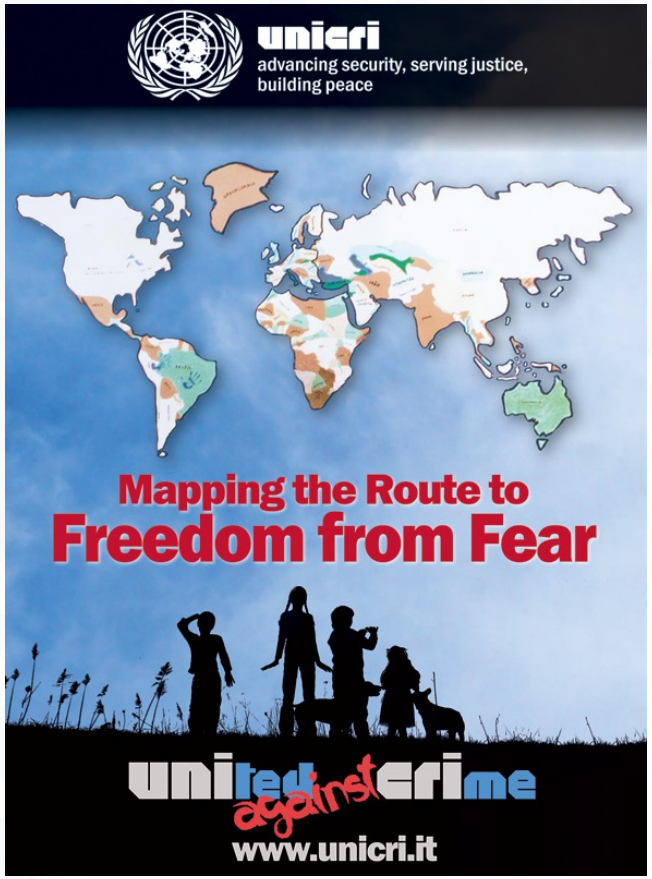
Technology is seen both as a tool to fight crime and protect human rights, while also being a means for criminal activity, whose misuse must be addressed.

The institute employs a holistic approach to its strategy, incorporating multidisciplinary and transnational aspects through the involvement of different actors in its projects, from governments and the private sector to civil society.

UNICRI: What we do…

he activities of the Emerging Crimes Unit regarding fighting and preventing cyber threats concentrate on

- Profiling hackers and cybercriminals
- Evolution of the criminal business model: organized crime links
- Analysis of cybercriminals' modus operandi
- Comprehensive evaluation of case studies
- Specific focus: terrorists' use of the internet, cyberwar and cyberterrorism
- Evolution of cybersecurity



The Hackers' Profiling Project

COURAGE-Cybercrime and cyberterrOrism (E)Uropean Research AGEnda

The COuRAGE consortium is delivering a measured, comprehensive, relevant research agenda for Cyber Crime and Cyber Terrorism (CC/CT) guided by the knowledge of the highly experienced and qualified consortium (17 partners,12 countries) and Advisory Board members (14 organisations including EUROPOL, JRC and ERA).

The purpose of COuRAGE is to improve the security of citizens and critical infrastructures and support crime investigators.

This Research addresses the major challenges and research gaps, and identifies practical approaches and strategies to address these issues.

SECURED-Security at the Network Edge

The SECURED project proposes an innovative architecture to achieve protection from Internet threats by offloading execution of security applications into a programmable device at the edge of the network (such as a home gateway or an enterprise router).

This approach reduces the load onto the mobile devices, guaranteeing enforcement of user-specific and device-independent security policies, and uniform protection across different devices and networks.

The project targets citizens, network providers, and companies. The latter will be able to enforce a company-wide security policy not only when the employee is connected to the corporate network but also when he/she is on the move (e.g. home network, 3G connection, airport WiFi).

Focus: Information Sharing Project

- In collaboration with the the European Electronic Crime Task Force.
- Explores existing modes of cyber-security information sharing between public and private institutions.
- Provides a list of viable suggestion for the creation of public private partnerships and for legislation in the field.

unicri
United Nations
Interregional Crime and Justice
Research Institute

Focus: Small and Medium Enterprises (SMEs) and the threat of Cyber Crime

theguardian
Winner of the Pulitzer prize

all opinion culture economy lifestyle fashion environment tech money travel

Protect your small business from cybercrime

Hackers today are no longer teenage thrill seekers. Many work with organised gangs and are a real threat to your business

FINANCIAL TIMES

Home World Companies Markets Global Economy Lex
Video Interactive Blogs News feed Alphaville beyondbrics Portfolio Special Reports

November 2, 2012 6:06 pm

Cyber criminals target small businesses

By Hugo Greenhalgh

Small and medium-sized businesses are vulnerable to cyber attacks as, unlike larger companies, they have yet to implement efficient security systems, leading IT experts have warned.

The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Women
Companies | Comment | Personal Finance | ISAs | Economy | Markets | Property | Festival o
People | Money | Sales | Technology | Gloombusters | Business Club Video | Your Business

HOME » FINANCE » BUSINESS CLUB

SMEs: How to arm your business against cyber crime

Ten tips for entrepreneurs in the fight against cyber crime

8 73 0 28 109 Email

The New Zealand Herald

Search keywords...

National Opinion Business Technology World Sport Entertainment

Business Your Business Around NZ Economy Industries Property Your Money

Pat Pilcher: 30 per cent of SMEs vulnerable to cybercrime

2:15 PM Wednesday Jun 18, 2014

Add a co

SMEs and Cyber Risk

- Cybercrime is indiscriminate in its approach, not only targeting multinational corporations and companies in the IT sector, but also SMEs, which are seen as easy targets.

- The losses deriving from cybercrime are currently estimated at between US$375 and US$575 billion per year. However, Interpol has estimated that in Europe alone, the cost of cybercrime has reached €750 billion annually.

- Cybercrime's impact on national economies is huge and SMEs are increasingly affected by cybercrime attacks. SMEs represent a pillar of the European economic and social structure, as well as 99.9% of Italian enterprises.

- This trend prompted UNICRI to commission a research study concerning the impact of cybercrime on Italian SMEs.

- **A**vailable in both English and Italian, the study aims to provide a framework to assess the impact of cybercrime on the economy and evaluate the vulnerabilities of Small and Medium Enterprises (SMEs) to cyber-attacks.

- Addresses the impact of cybercrime at the international, national (Italian) and local level.

- Targeted interviews and case study analysis were conducted to provide an overview of the tools currently used by criminals, the most common reasons that lead to these criminal acts, and the major risks and vulnerabilities for businesses.

- Interviews with institutional players and companies have helped to clarify key problems and suggest a need for a coherent strategy for SMEs to defend themselves against cybercrime.

UNICRI Strategy

The information collected in the research study allowed UNICRI to design and create a strategy based on the development of two complementary projects.

1. Aims to increase companies' knowledge and information exchange networks through the development of seminars, workshops and training courses tailored to non-technical decision makers, i.e. board of directors and business owners, and also to IT staff.

2. The organization of periodic roundtables among different actors, such as SME representatives, LEAs, business associations, academic institutions, and advocacy and legal experts. This will facilitate information sharing and the creation of a cross-sectoral community in the fight against cybercrime.

The implementation of these two projects will allow for the creation of networks of experts to promote a culture of security, with the advantage of never becoming obsolete, adapting themselves according to the evolution of cybercrime.

Other Projects

- Research on identity theft_project WebProID
- Child Online Protection (ITU)
- European Certificate on Cybercrime and Electronic Evidence
- ICT Security Training Program

Pipelines:

- Youth and Cybercrime
- Data protection and human rights protection in criminal investigations
- The Extent and Impact of Organized Crime in Cyberspace
- The Role of Technology in Human Trafficking and Violence against Women

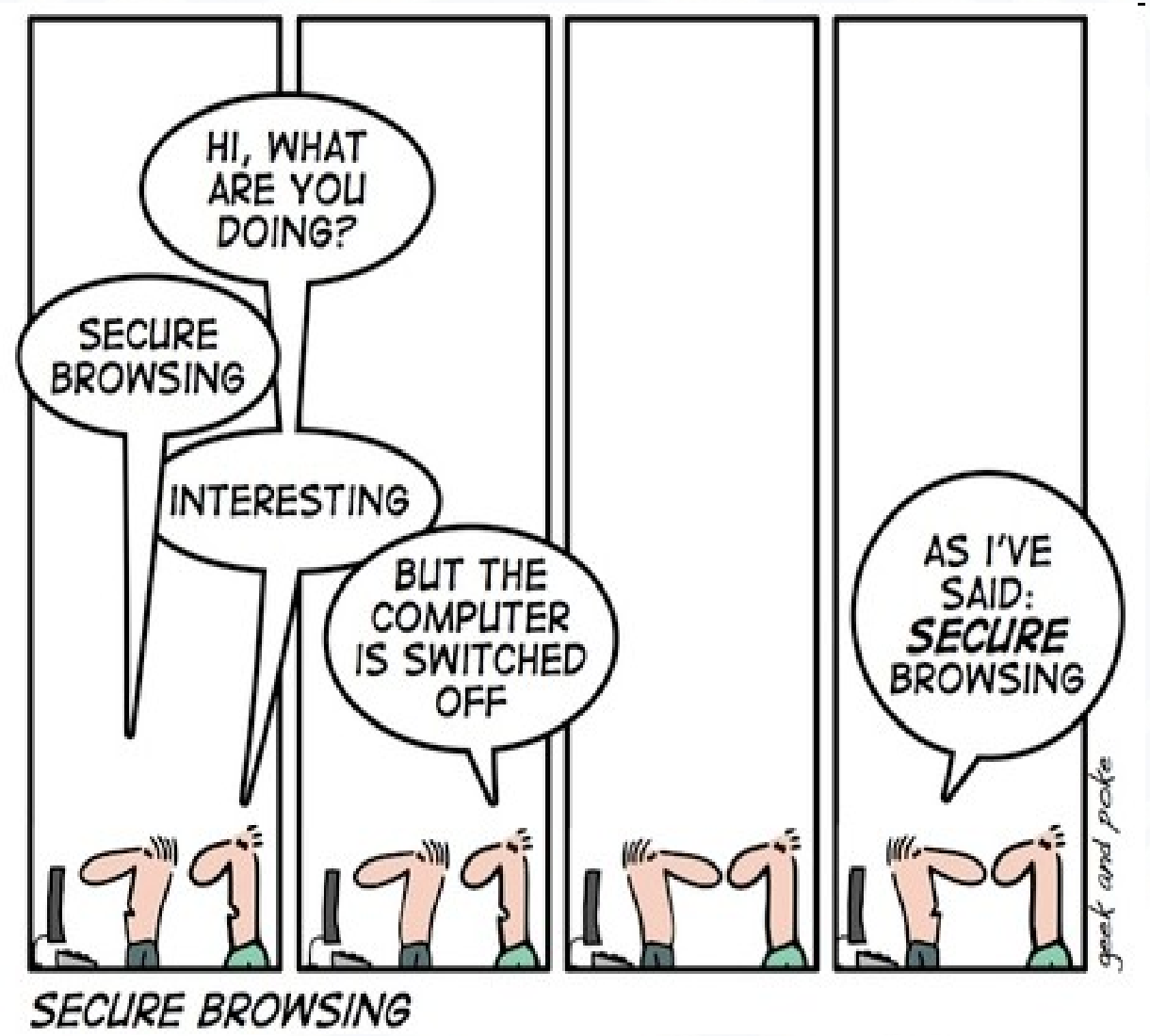
UNICRI's role within "Combating Cybercrime - Tools and Capacity Building for Emerging Economies"

UNICRI is taking an active role in 5 specific chapters of the project:

- Introductory Section
- Best Practices: Legal Enabling Environment
- Capacity Building
- The In-Country Assessment Tool
- Analysis and Conclusion

Working in conjunction with project partners, UNICRI's role will focus heavily on the aspect of capacity building. Drawing upon the expertise procured through its previous projects, UNCRI will assist in the training of LEAs, judges, and prosecutors, provide education for consumers and end users, and cooperate with the private sector and technical community on issues of resilience and security.

Questions?


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

Thank You!

Francesca Bosco

Project Officer

bosco@unicri.it

@francibosco

UNICRI:

http://unicri.it/special_topics/securing_cyberspace/