United Nations
Interregional Crime and Justice
Research Institute

Cybersecurity in SMEs: Evaluating the Risks and Possible Solutions

BANCHE E SICUREZZA 2015
Rome, Italy
5 June 2015
Arthur Brocato, UNICRI

unicri
United Nations
Interregional Crime and Justice
Research Institute

UNICRI's Main Goals

The United Nations Interregional Crime and Justice Research Institute:

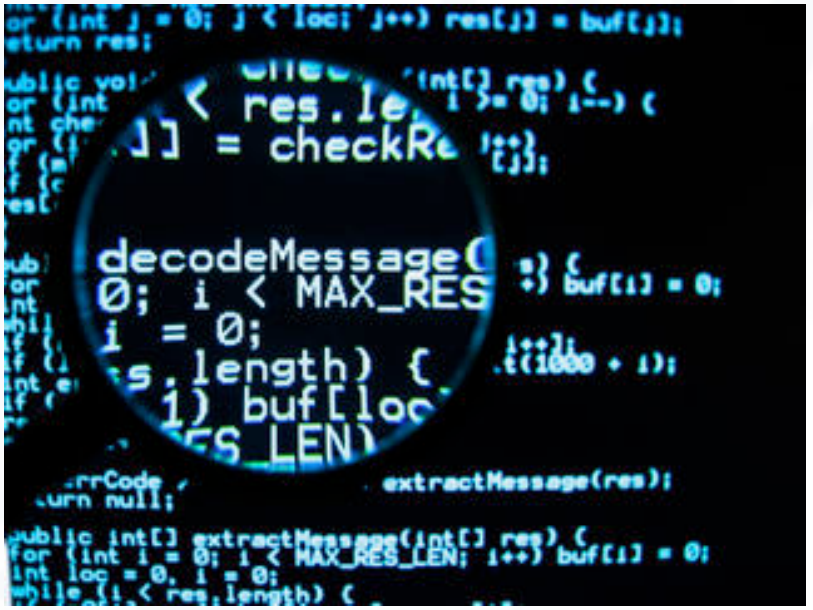
- Advancing an understanding of crime-related issues.
- Fostering just and efficient criminal justice systems.
- Supporting respect for international instruments and other standards.
- Facilitating international law enforcement cooperation and judicial assistance.

unicri
advancing security, serving justice, building peace
united against crime

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. Particularly, the unit deals with:

- **Cybercrime / Cyberterrorism**
- Counterfeiting
- Trafficking in persons
- Environmental crimes
- Corruption
- Victims' assistance



Why UNICRI is strongly committed to fight cybercrime:

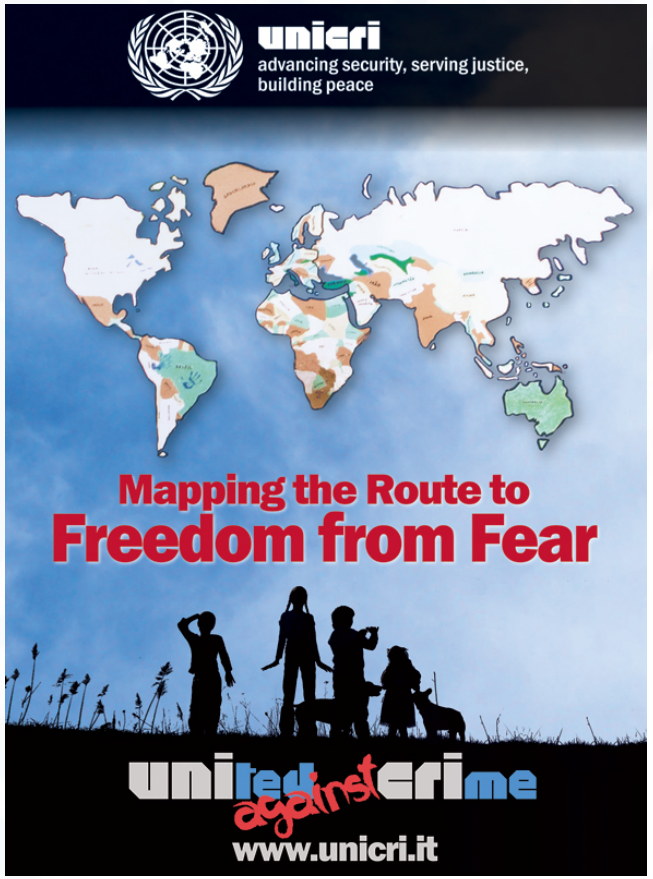
"I urge you to be more innovative when it comes to emerging threats such as cyber-crime, environmental crime and counterfeiting, we must stay one step ahead of the criminals. We must also be more effective in stopping the money flows enabled by corruption and money-laundering"

Ban Ki-moon, 2010

UNICRI: What we do…

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

- Misuse of technology and technology enabled crimes
- Evolution of the criminal business model: organized crime links
- Analysis of cybercriminals' modus operandi
- Evolution of cybersecurity
- Specific focus: terrorists' use of the internet, cyberwar and cyberterrorism



unicri
United Nations
Interregional Crime and Justice
Research Institute

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.

SMEs in the EU

- More than 20 million SMEs in the EU, representing 99.8% of total European enterprises
- Employ 86.8 million people
- Represent 66.5% of the EU labor force
- 92.1% of SMEs are micro enterprises
- Italian SMEs: the biggest sector in Europe
- 3.7 million enterprises
  - More than 18% of the EU average (European Commission data)

SMEs in Italy

- 99.9% of Italian companies
- +200 industry districts, representing the excellence of Italian products in the world
- Production of 68% of italian assets
- Employ 12 million people
- 94.4% of the total are micro enterprises
  - -Value in terms of employment: 46.1%
  - -21% in Germany
  - -22% in France
  - -27% in UK

Different threats

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

Different attacks

- Phishing
- Spear phishing
- Spam
- Pharming
- Malware
- Botnet
- Defacement
- DoS
- Social engineering
- Hacking

Different types of attackers

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

United Nations
Interregional Crime and Justice
Research Institute

- **Available 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 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.**

Research Methodology

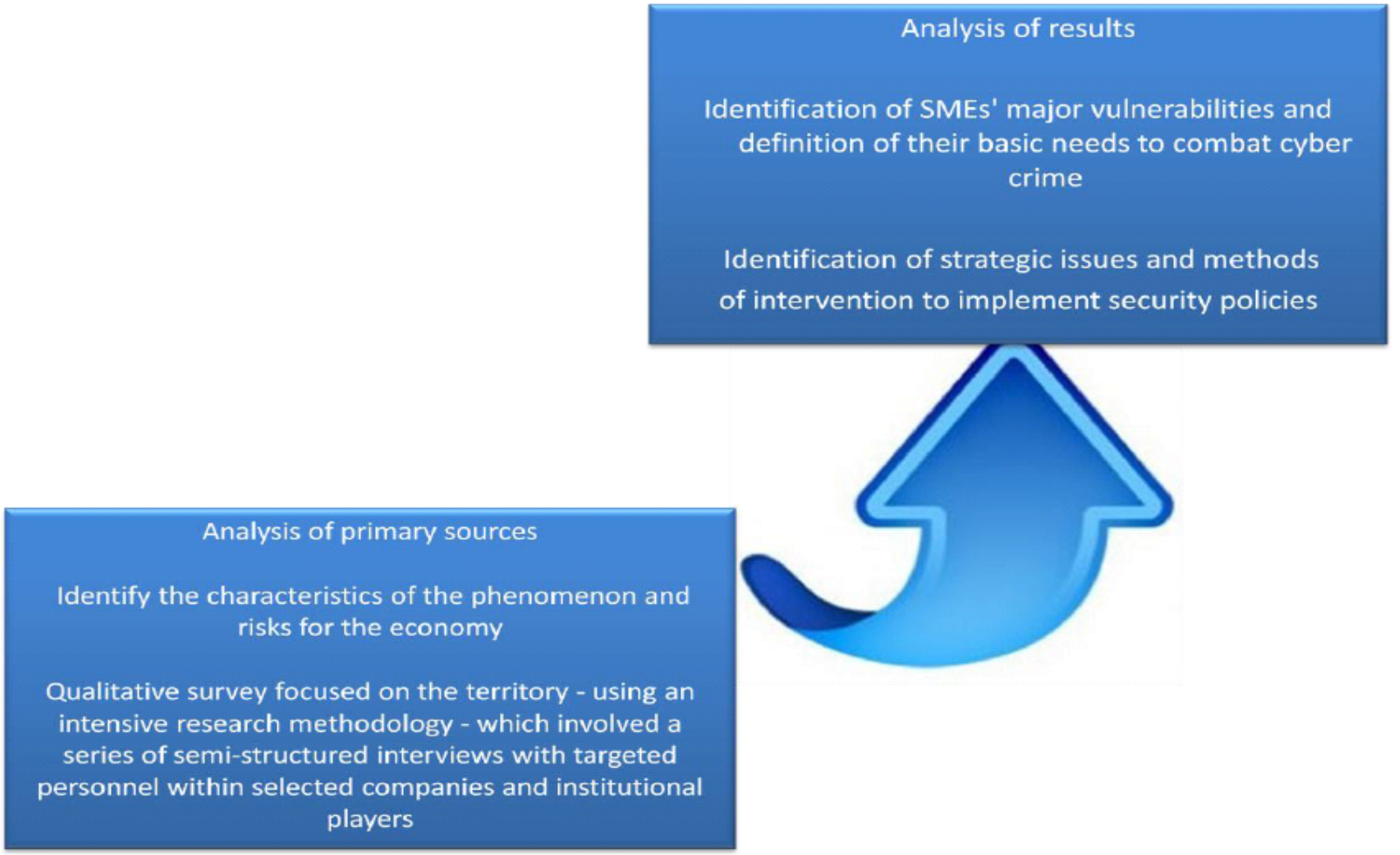


Figure 1 - Graph explaining the methodology used for the research

Major Findings:

- There is a need to invest in building capabilities via training programs and to remove cultural barriers that hamper awareness of risks.
  - Vulnerabilities associated with people's lack of capabilities and knowledge are more dangerous than those related to technical issues.
  - The human factor is crucial as cyber criminals often exploit human weaknesses for their own purposes.
- Crimes targeting specific organizations or individuals, such as spear phishing, have significantly increased in recent years.
- To implement countermeasures and concerted policies, IT managers, administrators, business owners, and boards of directors all need to be informed of the risks of cybercrime.

Major Findings (continued):

- There is lack of information sharing and cooperation among companies
  - Need to create networks between companies of the same sector or size to increase dialogue and sharing of best practices.
- Countering cybercrime is very difficult due to its transnational character.
  - International cooperation between different actors therefore plays a crucial role in the investigation and prosecution of such crimes.
  - In addition to strong legislative and law enforcement actions, the fight against cybercrime requires appropriate tools and cooperation, as well as a particularly higher level of knowledge and awareness.
- A full copy of the report can be found at:
  http://www.unicri.it/in_focus/on/Cybercrime_risks_economy

UNICRI Strategy

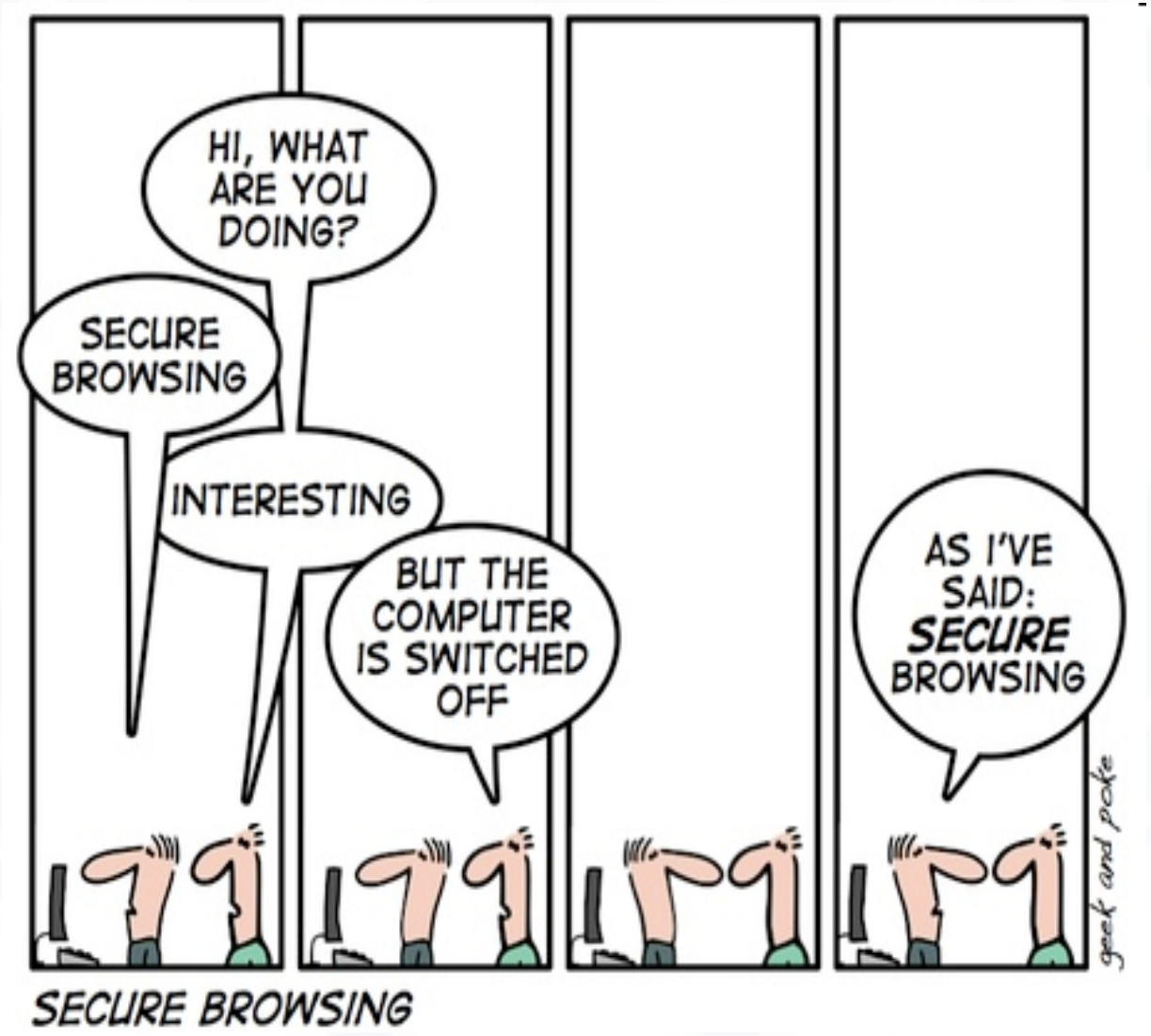
- The information collected in the research study allowed UNICRI to design and create a strategy based on the development of two complementary projects.

  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.

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

Contact Information

Mr. Arthur Brocato : Brocato@unicri.it
Cyber Crime Analyst, Emerging Crimes Unit

UNICRI: http://www.unicri.it/