"Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels"

The research study entitled "Cybercrime and the risks for the economy and enterprises at the European Union and Italian level" was conducted by UNICRI with the support of *Cassa di Risparmio di Lucca*.

Cybercrime is a multidimensional and complex phenomenon. It does not only target particular types of companies such as those in the Information Technology sector or those that produce highly specialized goods, but rather all types of companies.

Cybercrime is one of the most serious threats to the global economy, steadily growing over the past decade. The losses deriving from it are currently estimated to be between US$375 and US$575 billion per year[1]. However, Interpol has estimated that in Europe alone, the cost of cybercrime has apparently reached €750 billion annually[2].

Cybercrime's impact on national economies is also huge. In addition to large companies, small and medium sized enterprises (SMEs) are increasingly affected by cybercrime attacks. The research study aims to provide a framework to assess the impact of cybercrime on the economy, and to evaluate the vulnerabilities of SMEs to cyber-attacks. SMEs represent a pillar of the European economic and social structure, as well as 99.9% of Italian enterprises.

The research focuses on the impact of cybercrime at the international, national (Italian) and local level. Targeted interviews and case study analysis have been 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.

The main research findings are as follows:

- All interviewees highlighted the need to invest in building capabilities through training programs as well as the need to remove cultural barriers that hamper awareness of the risks of cybercrime. One important concern which emerged is that vulnerabilities associated with people's lack of capabilities and knowledge are considered more dangerous than those related to technical issues. The human factor is, in fact, crucial in this type of crime, 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.

---

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, available <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (retrieved 6-11-2014).

[2] *Opening Remarks by INTERPOL PRESIDENT KHOO BOON HUI. At the 41ST EUROPEAN REGIONAL CONFERENCE (ISRAEL, TEL AVIV, 8 MAY 2012),* available <http://www.interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (retrieved 10-11-2014).

- In order to implement countermeasures and concerted policies, it has been underlined that not only should IT managers be informed of the risks of cybercrime, but also administrators, business owners, and boards of directors.

- The research highlights a lack of information sharing and cooperation among companies and stresses the need to create networks between companies of the same sector or size in order to increase dialogue and the sharing of best practices.

- The investigative and judicial scenarios, as portrayed by the interviews, have shown that 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.

Cyber security is an added value, and the reliability of SMEs in this respect has to be considered as a crucial element for investors and clients.

Organizational culture is also an issue that needs to be addressed, and many preventative mechanisms can be implemented with limited costs. In addition to an internal security policy, it is necessary to encourage the sharing of information at multiple levels. Sharing best practices and information about threats internally and with supply chain companies, trade associations, and law enforcement agencies can help in preventing attacks and establishing initial countermeasures. At the operational level, during or after an attack: information sharing with other actors, such as law enforcement and financial institutions, can increase the resilience of production systems and mitigate economic and social damages.

The cross-border nature of cybercrime requires action at both the international and national level. In this regard, the European Union, in 2013, adopted its cyber strategy and invited Member States to do likewise. In 2014, Italy also published its *National Strategic Framework for Cyberspace Security (Quadro strategico nazionale per la sicurezza dello spazio cibernetico).*

To counter cybercrime, training and information sharing are crucial. The information collected in the research study allowed UNICRI to design and create a strategy based on the development of two complementary projects.

The first project 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 to IT staff.

The second project involves the organization of periodic roundtables among different actors, such as SME representatives, law enforcement, business associations, academic institutions, and advocacy and legal experts. The purpose of this project is not only to improve the sharing of information on emerging risks in cyberspace, but also to facilitate the creation of a leading 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 (a typical problem for classical best practices), and instead adapt themselves according to the evolution of the cybercrime phenomenon.