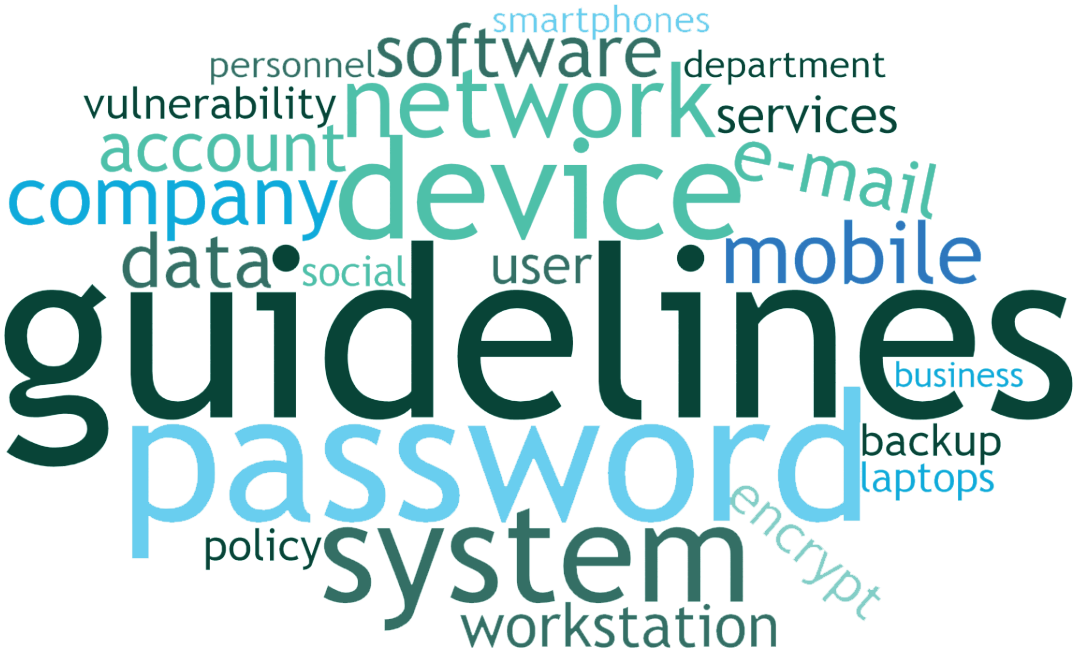
GUIDELINES FOR IT SECURITY
IN SMEs



unicri
United Nations
Interregional Crime and Justice
Research Institute

Fondazione
Cassa di Risparmio
di Lucca

United Nations
Interregional Crime and Justice
Research Institute

Guidelines for IT Security in SMEs

This set of guidelines constitutes the first update following the release of the study entitled "*Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels*", which was published in December 2014 by UNICRI. Within the study, the current situation concerning Italian small and medium enterprises (SMEs) and computer related crime was thoroughly investigated.

IT security for SMEs represents one of the most pressing challenges for both the economies of Italy and Europe. It is therefore necessary that a series of proactive measures be put into place with the aim of increasing awareness in this field.

SMEs make up 99.8% of European and 99.9% of Italian enterprises, respectively. In the European Union (EU), 86.8 million people are employed within this sector making SMEs the backbone of the Italian and European economies. While at the same time, they also represent a major point of weakness in terms of security.

Cyber crime provides a huge source of income for criminal organizations and is a key priority for the European Agenda on Security, alongside terrorism and organized crime[1]. The

1 *Communication from the EU Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions*, The European Agenda on Security, European

latest World Economic Forum (WEF) report[2] on global risks confirms that cyber attacks remain among the biggest threats to global security - both in terms of impact and likelihood of occurrence.

SMEs are a very attractive target for cyber criminals; nevertheless, decision makers working in these enterprises still often underestimate the threat posed by cybercrime. **No matter the nature of an SME's business, every company is seen as a lucrative target.** Various types of information, be it intellectual property, commercial data and contact lists, personal data, account credentials, and more can be sold on the black market to individuals intent on committing fraud, spreading malware and facilitating other crimes.

At the corporate level, damage is not only caused via a simple, one-off or indiscriminate attack. Instead, many attacks have long-term consequences. We are now witnessing an increase in targeted attacks that have the aim of appropriating sensitive data, deleting data altogether, or stealing copyrighted material.

Cyber crime is of a stronger nature and more widespread than one might imagine. In fact, most cyber attacks are still not being detected and/or reported. **Losses due to cyber crime for an individual company can reach up to several million euros.**

Due to large-scale cyber attacks in 2014, approximately one **billion records**[3] were compromised – affecting, on average, one in every three Internet users. Many of these records were totally unencrypted, and thus easy to exploit.

Additionally, ransomware is not showing any signs of decreasing in activity. The number of this type of attack more than doubled in 2014 – rising **from an estimated 4.1 million attacks in 2013, to 8.8 million in 2014**. From a psychological point of view, ransomware represents a very profitable form of attack because if a victim has not performed regular backups of their data, they are normally willing to pay the ransom in order to be allowed to retrieve it.

Alcatel-Lucent's Motive Security Labs[4] has estimated that **more than 16 million mobile devices around the world have been infected with malware** for the purpose of carrying out industrial and personnel espionage, to steal information and to attack

Commission, Strasbourg, 28-04-2015, in <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> (retrieved 09-06-2015)

2 The Global Risks 2015 10th Edition, World Economic Forum, in <http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf> (retrieved 06-05-2015)

3 Why SMEs are an attractive target for cyber criminals and what they can do about it, by Neil Ford, 02-03-2015, in <http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/> (retrieved 21-05-2015)

4 Motive Security Labs malware report – H2 2014, Alcatel-Lucent's Motive Security Labs, in <https://resources.alcatel-lucent.com/asset/184652> (retrieved 23-03-2015)

companies, private, banks and government. In 2014 alone, mobile device infections increased by 25% (an increase of 5% compared to 2013).

Phishing is still one of the most common methods of attack. Despite possibly being the most well-known cyber-attack technique, the percentage of users who click on phishing e-mails is still very high, even today. **The 80,000 security incidents analyzed in the *Verizon Data Breach Investigation Report*[5] have led to economic damage and data loss of more than $400 million for the companies involved.** The Verizon study therefore shows how highly profitable it is for a cyber criminal to use phishing techniques. Based on the data analyzed, for every ten phishing e-mails sent out, there was a more than 90% chance that at least one user would fall victim to an attack.

Considering the growing trend regarding this type of threat, it is more important than ever to develop efficient preventative security systems.

The presence of money or data which can be stolen, and the ease with which violating a target can take place, are the main factors that cyber criminals consider when carrying out their activities. Unfortunately, SMEs meet both these requirements. Nowadays, digital information security and proper use of the web and computer tools must be considered a priority by each individual citizen, and especially by companies.

In the event of a security breach, many companies do not even realize they have been attacked. Moreover, when devising a cyber security strategy, enterprises often do not know what can be done in order to protect themselves from cyber threats, and erroneously believe that defensive actions are expensive and solely technical in nature.

A framework for assistance in the implementation of IT security systems is a major aspect that is lacking in the Italian SME sector. Technical elements, such as antivirus software and firewalls, etc. are in use, but the formulation of a structured policy needs to be taken into account in order to build a base that can be adapted and re-implemented over time according to the evolution of cyber threats. **In response to this environment and the analysis of existing gaps, a suggested plan of action has been the creation of a framework of comprehensive, identifiable guidelines that are adaptable to the various types of SMEs present within Italy.**

Accordingly a set of guidelines was drafted, and subsequently submitted to and validated by IT security experts from leading companies, such as Fastweb, IBM, Kaspersky and Microsoft. Additionally, the guidelines were also reviewed by three IT managers from three different enterprises who were interviewed within the previous study on SMEs (Lucart,

5 2015 Data Breach Investigations Report, Verizon, in <http://www.verizonenterprise.com/DBIR/2015/> (retrieved 25-05-2015)

Lucense and Tagetik). Cyber crime poses a severe risk to all types of enterprises present throughout Italy. Preventing these risks requires implementing initiatives based on both education and awareness. Action in this field is not only required on behalf of SMEs, but also needs to be taken into account at the national level.

A sampling of viewpoints from leading companies in the cybersecurity field concerning the current state of protection for SMEs is listed below, followed by the set of Guidelines for IT Security in SMEs.

MICROSOFT *"The overall attack surface exposed by our digital civilization is growing faster than our ability to protect it."*

KASPERSKY *"Small and medium-sized enterprises need to realize that the threat of cyber crime is real. The consequences of this are considerable for victims, primarily for the loss of sensitive information such as intellectual property that can compromise corporate networks, disrupt business processes and for the loss data."*

IBM *"SMEs should be informed that they stand to lose information, which is vital to business continuity, forever - with direct effects on the ability to stay in business. A company will no longer be able to recover after a well-aimed cyber attack."*

FASTWEB *"A framework of assistance, support and information SMEs in the field of cyber crime is necessary, more than useful."*

This study was conducted by Dr. Flavia Zappa Leccisotti.

Disclaimer

The views expressed are those of the authors and do not necessarily reflect the views and positions of the United Nations. Authors are not responsible for the use that might be made of the information contained in this publication.
Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged.
The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.
The mention of specific institutions, companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the Secretariat of the United Nations or UNICRI in preference to others of a similar nature that are not mentioned.

Copyright

United Nations Interregional Crime and Justice Research Institute (UNICRI),
Viale Maestri del Lavoro, 10
10127 Turin
Italy
Tel 011-6537 111 / Fax 011-6313 368
Web site: www.unicri.it
E-mail: documentation@unicri.it

unicri
United Nations Interregional Crime and Justice Research Institute

Guidelines for IT Security in SMEs[6]

Administration area

- Manage user accounts of administrative personnel
  - Password security management
  - Use of certified e-mail services
- Human resources
- Sensitive data protection of all personneldata
- Company's mobile device use (e.g. smartphones and laptops)
- Social network management
- Manage physical accesses of company personnel

Marketing area

- Manage user accounts of marketing personnel
  - Password security management
- Customers and suppliers database management
  - Sensitive data protection of customers' and suppliers' data
- Security management in relations with suppliers
- Invoicing
  - Protection of invoicing data
- Company's mobile device use (e.g. smartphones and laptops)

R&D area

- Manage user accounts of research and development personnel
  - Password security management
- Know-how, intellectual property and corporate assets protection (e.g. patents, projects, catalogs)
  - Schedule continuous backup and devise disaster recovery plans
  - Use data encryption systems on all workstations, laptops, mobile devices and external devices (e.g. HD and USB sticks)
- Company's mobile device use (e.g. smartphones and laptops)

Logistics area

- Manage user accounts of logistics personnel
  - Password security management
- Warehouses and materials and products handling
- Company's mobile device use (e.g. smartphones and laptops)

Manufacturing area

- Manage user accounts of manufacturing personnel
  - Password security management
- Protection of IT systems of automated production lines
- Company's mobile device use (e.g. smartphones and laptops)

IT area

- Analysis of the IT environment of the whole company
- IT systems management
  - Workstations management
  - Network security
  - User accounts management
  - Schedule continuous backup and devise disaster recovery plans
  - Securely erase all data from devices no longer in use (e.g. HD, backup DVDs/tapes, USB sticks) even if marked for disposal
  - Data encryption policy
  - Social network management
  - Public sites and e-commerce management (if any)
  - What to do in case you have been attacked

6 These Guidelines have been formulated thanks to the advice put forth by Dr. Daniele De Nicolò, and they have been validated by Fastweb, IBM, Kaspersky, Microsoft and IT Manager by Lucart, Lucense and Tagetik.