Clusit

Italian Information Security Association

2012 Report

on ICT Security in Italy

Clusit
Associazione Italiana
per la Sicurezza Informatica

SECURITY
Technologies
Management
Compliance
SUMMIT

Translated by Manuela Borghetti

Supervised by Raoul Chiesa

Edited by Ioan Landry

Cardi Editore

via Pier Luigi da Palestrina, 13

20124 Milano

Tel.(+39) 0267101088

www.cardieditore.com

Table of contents

It is with great satisfaction that CLUSIT introduces its first report on information security in Italy: it is an innovative analysis if we consider the approach and, above all, the leading role of the contributors in creating it and testing the veracity of the reported data.

The information security analysis has been written by experienced professionals, by users that deal daily with both threats and the application of policies as well as by operators in the field every day.

The CLUSIT Report gives an overview of the most important events that occurred in 2011[1], of the Italian ICT security market, of the new breed of professionals that will be needed soon and the problems that will come up in the near future.

Now that the Italian government is paying attention to the Digital Agenda, we believe that our Report may be an important asset to the national development of the Internet. It is indeed perceived as essential to growth conditions, and the foundations should be laid down to guarantee continuity, high quality and effective use by institutions, businesses and individuals.

Enjoy your reading.

Gigi Tagliapietra
CLUSIT chairman

[1] The current version of the CLUSIT Report also offers updates from the first months of 2012.

“A necessary publication”: this is the first comment after having read the CLUSIT Report on information and systems security in Italy. After the more resounding attacks of the past years, this topic seems to be abandoned by media and, even worse, by decision makers. All this happens while the phenomenon is spreading in terms of severity and scope.

If until a couple of years ago, this issue was limited to “information systems”, now there is no area, from factories to medical equipment, which has not been victim of any form of information attack.

As demonstrated from the data reported in the first part of the Report, today every strategic area has to cope with the pressing issue of security.

We need to learn how to live with a degree of insecurity, which is even more stressful due to the cultural divide that is characteristic of the average user. Social engineering shows on a daily basis that it’s much easier to have a private password dictated on the phone than trying to recover it through any time more accessible sophisticated intrusion techniques.

In this context, awareness is the main tool at our disposal to face information risk. The impact of a planned event is totally different if compared to unexpected attacks. In the last 20 years both industrial and academic researchers ratified tools and methodologies for incident prevention mitigation and recovery. Their use is far more efficient against the majority of information risks, but without a real commitment it is hard for these tools to be used properly.

Under this perspective this Report is not encouraging. In the last part of it, the articles written by Mr Manca, Mr Telmon and Mr Tieghi focus on specific sectors (PA, SME, and industrial control) slowly trying to face a phenomenon which is increasing exponentially. In the second part of the Report, impressions and feelings are expressed, confirming the data collected from a survey that CLUSIT conducted among users, businesses and information security suppliers.

At the end, the Report draws the reality of a country in arrears among the Western societies in terms of information risk awareness and management. A tiny justification to this can be found in the innovation delay of ICT technologies usage. A massive use of ICT technology would revitalise Italy and with this Report, CLUSIT is at the forefront to remind us that without a kick-start, Italy won't be able to come to terms with the concern called information security.

Prof. Danilo Bruschi

CLUSIT honorary chairman

Introduction to the Report

The technological innovation we are experiencing these years is so rapid that it creates consumption patterns previously unthinkable. Technological innovation has become part of our lives as citizens, managers and entrepreneurs and it affirms a new way of doing things: organising our businesses, our work and our lives. Understanding these changes is the first step to growth and to ability to profit from the opportunities given by technological innovation.

CLUSIT Report on ICT security in Italy helps underline the aspects of these transformations and the need that security comes along with these innovations overall.

The Global Risk Report 2012 written by the World Economic Forum analyses the 50 most important global threats for the next 10 years, ranking them on the basis of impacts and probability. In the *technology risks* section, the first place is given to cybercrime.

It is important that public opinion, businesses and politicians alike realise how much is at stake and how many coordinated initiatives are needed to increase security in many fields. CLUSIT is the mouthpiece of this message which is also the core of CLUSIT's institutional activities.

The Report turns to media, institutions, public administrations, as well as ICT security products and services suppliers since any of them have an important role and insights to share. Its aim is to contribute in making ICT more secure and to fight illegality: this can be done by embracing both global and local perspectives.

Pundits know that ICT security is a route whose arrival is gradually set a bit further. This is not a fixed and unchangeable state, but a way of being and becoming. Decisions are made based on best practices, risk analysis (or insights) and on evaluations of what has happened or is going to happen with a both strategic and adaptive approach. The Report is structured on chapters that aim to clarify different correlated aspects; each chapter handles the past to foresee the future.

The Report begins with a detailed overview of cybercrime-related events and the most significant information incidents that occurred in 2011 in Italy and abroad, as well as with the upcoming trends for 2012. Other aspects are taken into consideration in the Report: the emerging trends that were common in 2011 and that are still widespread today, such as hacktivism, espionage and sabotage/cyber warfare. A contribution offered by the Italian Postal and Communication Police gives a description of the crimes it deals with on a daily basis with yet unpublished data collected on a qualitative and quantitative basis of investigations throughout 2011.

The second part of the Report is dedicated to the Italian ICT security market and gives the results of a CLUSIT survey taken on a sample of 142 entities. It also focuses on key areas of interest and investment forecasts. As regards the labour market, the businesses involved outlined the most sought-after professionals and the requirements generally taken into account when choosing ICT security staff.

The last part of the Report is entitled FOCUS ON and it focuses on the most relevant areas for ICT security in Italy: Mobile Security, Social Media Security, Cloud Security, normatives for personal data treatment, the ICT security situation of the Italian public administration and facilities, internet and control systems protection in the industrial field and, at last, the ICT security situation for small and medium Italian enterprises.

Cybercrime related events and main information incidents and trends: 2011 and 2012 overview

This section of the CLUSIT Report aims at giving an overview of what happened last year and during the very first months of 2012 in the information security area. It also analyses some of the incidents occurred and their impact on people, society and business.

The number of incidents that took place in 2011 and in the first two months of 2012 is fairly impressive.

Today the direct income of the criminal market worldwide ranges from 7 to 10/12 billion dollars per year (Report 2011: Russian Cybercrime Market – IB Group / CARO 2011: Cybercrime in Russia – ESET) – estimated data, since organised crime doesn't keep official books. We know many criminal groups that with mere botnets can earn staggering weekly "salaries", and that in the security vulnerabilities market, the price of a non-public or "0-day" vulnerability ranges from 39,000 to 130,000 dollars.

Beyond being a global phenomenon**,** the impact of single attacks has also increased. The DDoS attack that hit Ukraine Telecom, Yandex and EvoSwitch, reached 100 GB/sec, and the highest amount of money stolen from cybercrime attackers from a single bank account is 14,8 billion dollars.

Unfortunately, 2011 ended the same way it began: resounding hacking attacks and personal data theft on a very large scale. A year that pundits won't easily forget.

At the end of the cybercrime-related events and information incidents analysis of the last 12-14 years, you will find the past and upcoming trends in Italy and abroad.

Analysis of the Main International Incidents

2011, the *annus horribilis* for ICT Security

During 2011 the total amount of attacks and security incidents increased significantly compared to the past, indicating a worrying tendency to increase throughout the year.

Even more concerning is that the varieties of attackers as well as victims widened, and made 2011 the *worst year ever* from an ICT security point of view. As from data gathered from January to April, the trend for 2012 looks even critical: the situation may further deteriorate.

We shouldn't be shocked, though, since the conditions for these factors for this to become true – which were very well-known by pundits – increased progressively to reach, at the end of 2010, such a critical mass able to determine the sharp increase in incidents we observed over 2011.

The severest growth is undoubtedly found in cybercrime turning into an industry worth billions of dollars that can potentially hit every Internet user, more or less 30% of the world population[1]. During 2011 a widely-known new phenomenon started to grab people's attention: on one side cyber war was a very discussed topic (often out of turn), while on the other it was a flurry of discussion on "hacktivism". The group known as "Anonymous" generated so much ado that it unveiled even more dangerous threats related to espionage and/or organised cybercrime.

Everything happened when the "defenders" were substantially unprepared and the "attackers" were operating unpunished. Hacktivists, cybercriminals, spies, wreckers, mercenary hackers, governmental or para-governmental cyber warriors were free to perpetrate information attacks against national and international institutions, critical facilities, any kind of industry, famous people and thousands of citizens, causing billions of dollars in damage.

Despite this out-of-control situation we noticed a common disregard shared by our technological stakeholders (politicians, institutions, businesses and citizens) towards InfoSec. They are part of a civilisation that digitalized itself very quickly but disorderly, that slowly placed more and more trust in personal computers, in the Internet, in mobile devices, and the countless services offered without understanding the difficulties and thinking of how to face inevitable risks properly.

Before going through with a statistical analysis of the data available, we would like to briefly linger over a couple of extraordinary cases in 2011.

Emblematic cases

Some of the hundreds of known attacks that we analysed are below, reported as examples of the presented and emerging tendencies. We want to underline that the choice of the cases to analyse has been tough given the high number, the gravity and the variety of the incidents.

1. "All against one"

Victim	Attacker	Techniques used
Entertainment multinationals	Hacktivists (Anonymous, LulzSec), Lone Hackers, unknown cybercriminals	DDoS, SQLi, social engineering, hacking

Between April and October 2011 a high number of attacks (into the tens) were committed against important entertainment multinationals. The attackers were many, most of them are still unknown, and each had different goals.

These attacks had remarkable consequences in terms of image, direct financial losses and compensations to the users that started a legal argument corresponding to a hundred million dollars in total expenses. The business, which was already affected by the Japanese tsunami, lost 30% of its

[1] http://secunia.com/?action=fetch&filename=secunia_yearly_report_2011.pdf

stock market capitalization.
Even without reporting the still unclear history of the events[2], the company suffered a lot of DDoS attacks, data thefts (more than 100 million users profiles have been stolen from the video game players network and the Online Entertainment platform) and intrusion into websites which led to the interruption of applications providing online games (used by 77 million users) for 24 days.
Hacktivists, lone hackers, and unknown attackers used sophisticated techniques (such as SQLi, social engineering, hacking of unpatched or misconfigured systems, and so on) and yet they successfully committed these attacks thanks to the poor security of the organisation. For instance, the tons of stolen user profiles were kept unencrypted and the company's staff didn't include a CISO.

2. “He who lives by the sword”

Victim	Attacker	Techniques used
US government contractor	Hacktivists (Anonymous)	SQLi, social engineering, hacking

In February 2011 the managing director of a well-known security company[3] with sensitive US government contracts announced that he had been able to infiltrate Anonymous and that he would be disclosing the names of the ring-leaders during an upcoming event set for the following week.
In reprisal, the CEO of the company was essentially lynched by Anonymous. The hacktivist group breached his Twitter account and published his address, phone number and healthcare details. Above all, Anonymous broke in the defensive systems of the company, stealing more than 6,000 private e-mails (some of which were quite embarrassing), erasing backup files and disabling the internal phone system.
Known and unsophisticated techniques were used in this case: social engineering and SQL injection. Passwords of compromised accounts published on the Internet turned out to be inadequate and reused by different systems. Lastly, the published e-mails were a bad blow for the company reputation since they referred to unethical activities conducted by the company, both of its own will as well as on behalf of customers.
As result of this attack, the CEO was forced to resign and he subsequently lost his next job[4] due to Anonymous as well.

3. “Take the money and run”

Victim	Attacker	Techniques used
Banks	Unknown cybercriminals	Exploit, RAT, ATM data theft

Unknown cybercriminals penetrated the primary network of an American bank[5], exposing more than 360,000 customers profiles with personal and financial data which led the bank to reissue more than one hundred thousand credit cards and to spend a huge amount of money to notify and to update its systems.
Another incident involved a South African bank[6], which after a “virtual robbery”, lost over 40 million Euro. The attack took place overnight and involved breaking surreptitiously into the bank's information systems and opening bank accounts, which were funded with money taken from legitimate customers' accounts and then withdrawn through many ATM terminals.
Even if different, both incidents were possible because of the lack of proper security and anti-fraud

[2] http://attrition.org/security/rant/sony_aka_sownage.html0
[3] http://it.wikipedia.org/wiki/Anonymous#Attacco_alla_HBGary_Federal
[4] http://www.huffingtonpost.com/2012/01/20/aaron-barr-cybersecurity-anonymous-occupy-wallstreet_n_1219328.html
[5] http://www.wired.com/threatlevel/2011/06/citibank-hacked/
[6] http://www.news24.com/SouthAfrica/News/R42m-stole-in-Postbank-hijacking-20120114

controls, which seems quite unjustifiable in today's world.

4. “Who defends the defenders?”

Victim	Attacker	Techniques used
Certification Authorities	Iranian hacker (governmental?)	Many vulnerability exploits

Some Certification Authorities have been compromised[7], enabling attackers to generate a lot of valid SSL certificates issued to: Google, Yahoo, Microsoft, Facebook, Twitter, Skype etc. The (apparent) intention was to use these certificates to aid in wiretapping communication streams – not only via e-mail – of Iranian citizens and dissidents, endangering 300,000 people[8] trough *Man in the Middle*[9] attacks.

The most sensational attack hit a Dutch CA used by the Dutch government, and was revealed *months after* it actually occurred. Hundreds of rogue[10] digital certificates have been created in name of delicate institutional subjects such as mossad.gov.il, cia.gov and sis.gov.uk. The CA interrupted its activities a couple of days after the disclosure of the piece of news when it was overcome by the scandal. Nowadays a thorough inquiry by the Dutch government[11]is still in progress.

Considering the importance of Certification Authorities in the management of digital certificates, these attacks displayed the fragility of the PKI system. Its functionality is the linchpin for many commercial activities on the Internet, for access to private sources and for authentication of remote systems. Many doubts on their reliability and concerns[12] towards their future role have been raised by these attacks.

5. “Operation Nitro”, “Operation Night Dragon” and “Project Enlightenment”

Victim	Attacker	Techniques used
Chemical and oil & gas multinationals, other companies	Unknown (Chinese espionage?)	Spear phishing, social engineering, many vulnerability exploit, malware (RAT)

In 2011 industrial and commercial espionage touched record levels. Continuous intelligence activities were brought to light, which were causing damage to important, mostly Western, businesses, and were conducted by high-level teams of specialists through sophisticated and sometime long-term intrusions. Among last year's cyber-espionage operations, “Option Nitro” [13]and “Operation Night Dragon”[14] stand out because they hit many chemical, energy and oil & gas multinationals. At the beginning of 2012 a wide series of violations, known as “Project Enlightenment”[15], hit law firms, ICT and other companies, think tanks and associations without distinction.

These activities require resources, organisation and cooperation at the state-level, so it is entirely conceivable that they belong to the pitiless commercial competition as well as geopolitical tensions; with this in mind, campaigns of this nature are bound to increase. Commentators recently affirmed

[7] http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars
[8] http://timesofindia.indiatimes.com/tech/news/internet/-300000-Iranian-users-victim-of-internet-spying/articleshow/9883306.cms
[9] http://it.wikipedia.org/wiki/Man_in_the_middle
[10] http://blog.gerv.net/2011/09/diginotar-compromise/
[11] http://cyberwarzone.com/cyberwarfare/diginotar-case-increasing-resistance-against-infringements
[12] https://blog.torproject.org/blog/diginotar-debacle-and-what-you-should-do-about-it
[13] http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secrets
[14] http://www.scmagazine.com/chinese-hackers-break-into-oil-companies-networks/article/196099/
[15] http://www.cybersquared.com/project-enlightenment-a-modern-cyber-espionage-case-study/

that we are experiencing the biggest wealth transfer of human history under the form of intellectual property theft from renowned multinationals and defense[16]contractors.

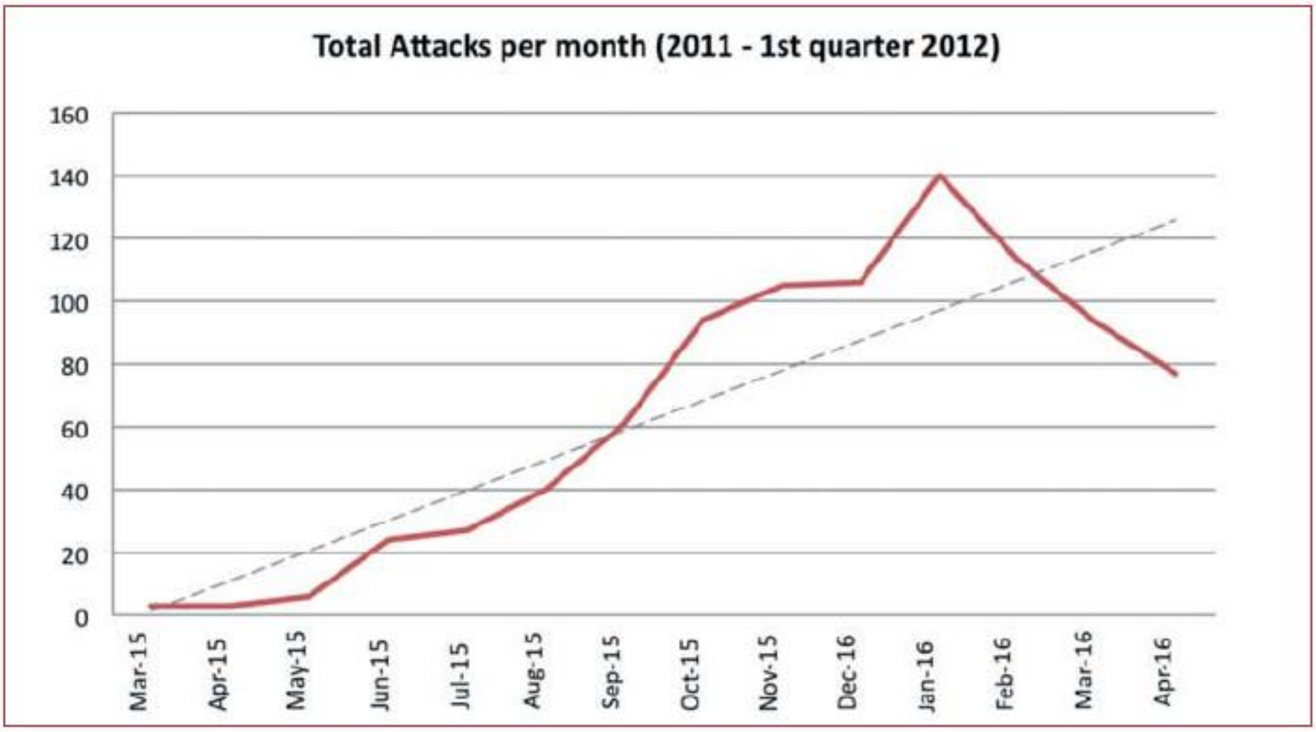
With targeted attacks like *spear phishing*[17], attackers took over employee laptops through malwares and/or monitoring their activities, so that they could leverage their VPN connections used to connect remotely to applications and to internal business servers.

These *stealthy* attacks need time (sometimes years) to be discovered; they are particularly insidious and hard to avoid. No organisation can be safe from them.

The tip of the iceberg

Without official data and exhaustive public sources, we tried to understand what happened and is happening now beginning from the list of the most remarkable attacks and security incidents of 2011[18] (around 470, more than 1 per day in average) and we classified them on the basis of the attackers, the goal and the techniques used. Similar in terms of dimension and in number are the attacks registered during the first 4 months of 2012 resulting in a soaring 300% increase in the frequency with 892 total incidents.

We have to state beforehand that the information we analysed have been collected using open sources and that, consequently, their qualitative value in terms of reliability and completeness have to be considered as extremely variable. That being stated, the growth tendencies of the main attacks of the last 14 months can be extrapolated from the following graph:



The peak in January 2012 is fairly impressive with 4,6 significant attacks per day, mostly by cybercriminals. The list does *not* include attacks (numbering in the *hundreds of thousands per year*[19]) that don't achieve a degree of severity or introduce new features to make them significant. For example, minor websites *defacement*, DDoS attacks on a small scale, malware diffusion [20] the spread of *botnets*[21], or conventional phishing were not taken into consideration because of their

[16] http://independentnewshub.com/?p=49536

[17] http://searchsecurity.techtarget.com/definition/spear-phishing

[18] 2011 Cyber Attacks Timeline Master Index: http://paulsparrows.wordpress.com/2011-cyber-attacks-timeline-master-index/

[19] http://www.nccgroup.com/NewsAndEvents/Latest/12-02-01/Origins_of_Global_Hacks.aspx

[20] http://www.trendmicro.com/us/security-intelligence/research-and-analysis/index.html

[21] http://www.crn.com/news/security/231000907/tdss-botnet-virtually-indestructible-kaspersky-researcherssay.htm

ordinary nature, even though they caused the majority of damage.
Downstream of this classifying job, we have been able to create statistics that in some cases showed our ideas to be true, in others outlined outstanding phenomena.

Our classification criteria and numbers follows. The criteria we adopted are high-level, since the often lack of detailed information on the incidents.

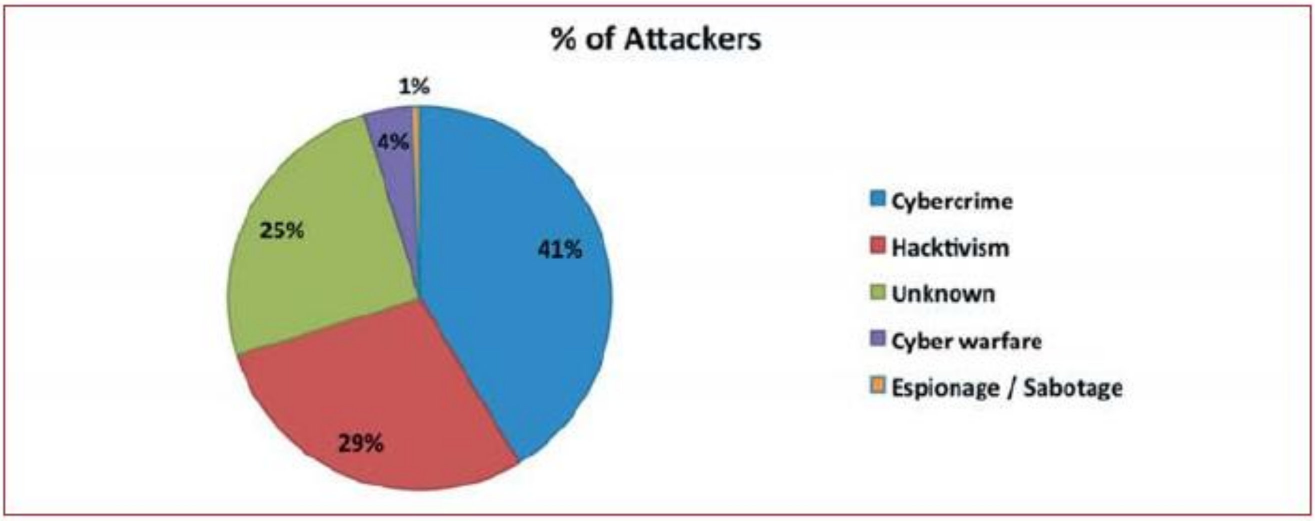
TYPE OF ATTACKER	2011	1Q 2012	Total amount
Cybercrime	170	175	345
Unknown	148	122	270
Hacktivism	114	106	220
Espionage/Sabotage	23	3	26
Cyber warfare	14	17	31
Total amount	469	423	892

TYPE OF VICTIM	2011	1Q 2012	Total amount
Institutions: Gov-Mil-LEAs-Intelligence	153	146	345
Others	97	95	192
Industry: Entertainment/news	76	56	132
Industry: Software/hardware vendor	27	18	45
Industry: Research -education	26	30	56
Industry: Gov. Contractors / Consulting	18	8	26
Industry: Banking/finance	17	16	33
Industry: Security	17	16	24
Industry: Online Services /cloud	15	28	43
Industry: Telco	11	6	17
Industry: Health	10	1	11
Religion	0	7	7
Industry: Chemical/Medical	2	5	7
Total amount	469	423	892

TYPE OF ATTACK TECHNIQUE	2011	1Q 2012	Total amount
SQL injection[22]	197	137	334
Known Vulnerabilities/Misconfigurations	107	69	176
Unknown	73	98	171
Malware	34	23	57
DDoS[23]	27	59	86
Account cracking	10	13	23
Phishing/social engineering	10	11	21
Multiple techniques	6	7	13
O-day[24]	5	3	8
Phone cracking	0	3	3
Total amount	469	423	892

[22] http://it.wikipedia.org/wiki/SQL_injection
[23] http://it.wikipedia.org/wiki/DDOS
[24] http://it.wikipedia.org/wiki/0-day

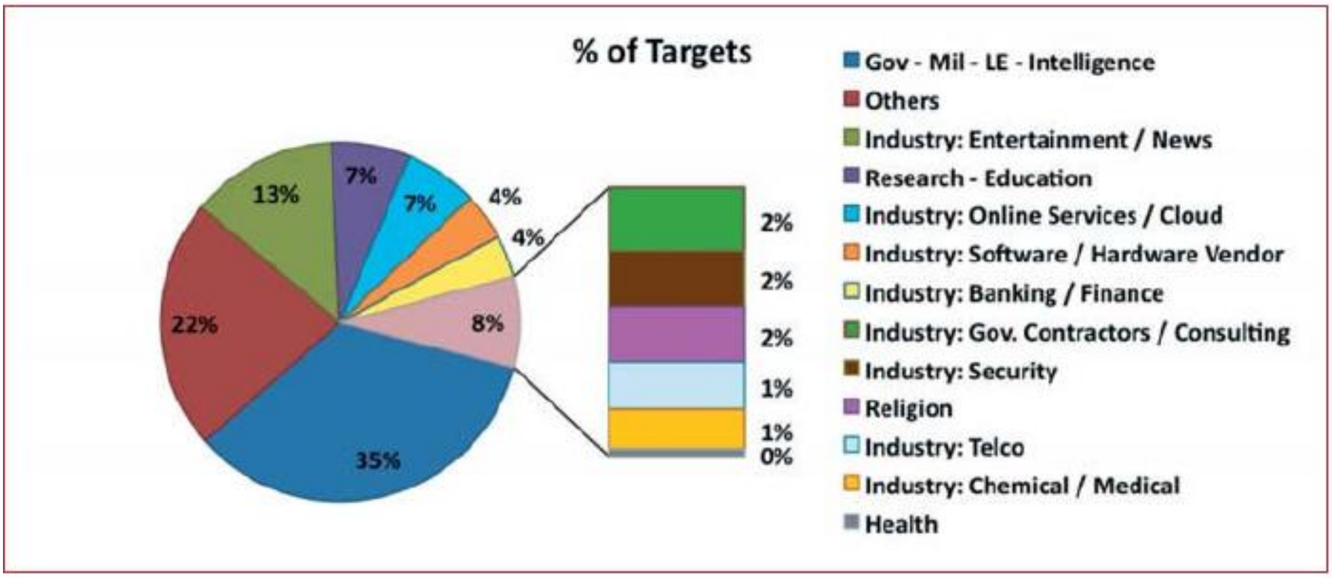
An important data is the increase of DDoS attacks, who doubled in the first 4 months of 2012.
The ratios which emerge from this data analysis deserve some observations. We shall start with the attack graph, classified by the **types of attackers**.



On the whole the incidents caused by cybercriminals (both profit-oriented, through frauds and thefts, and mere notoriety-oriented, through defacement, online dump of PII, etc.) are more numerous than the incidents caused by hacktivists, although the feelings conveyed by the media show the opposite. Commentators labelled 2011 as the “year of hacktivism”, whereas “year of cybercrime” would be more appropriate. This trend is currently growing + 5% from January to April 2012 (from 36% to 41%.)
It is also worth considering that more than 1/3 of the attacks have been committed by unknown attackers, which on one hand stresses the problem of *attribution*[25]. On the other hand, it is impossible to prevent such a high number of attacks as we don't know the features, skills and preferred targets of the perpetrator.
Beyond that, given the elusive nature of Anonymous, we believe that several attacks have been claimed by Anonymous to hide those really responsible through false-flag tactics[26].
Finally, activities connected to espionage, sabotage and cyber warfare represent an important share of the total amount, touching 5% .

The graph of the **targets and victims** is also interesting:

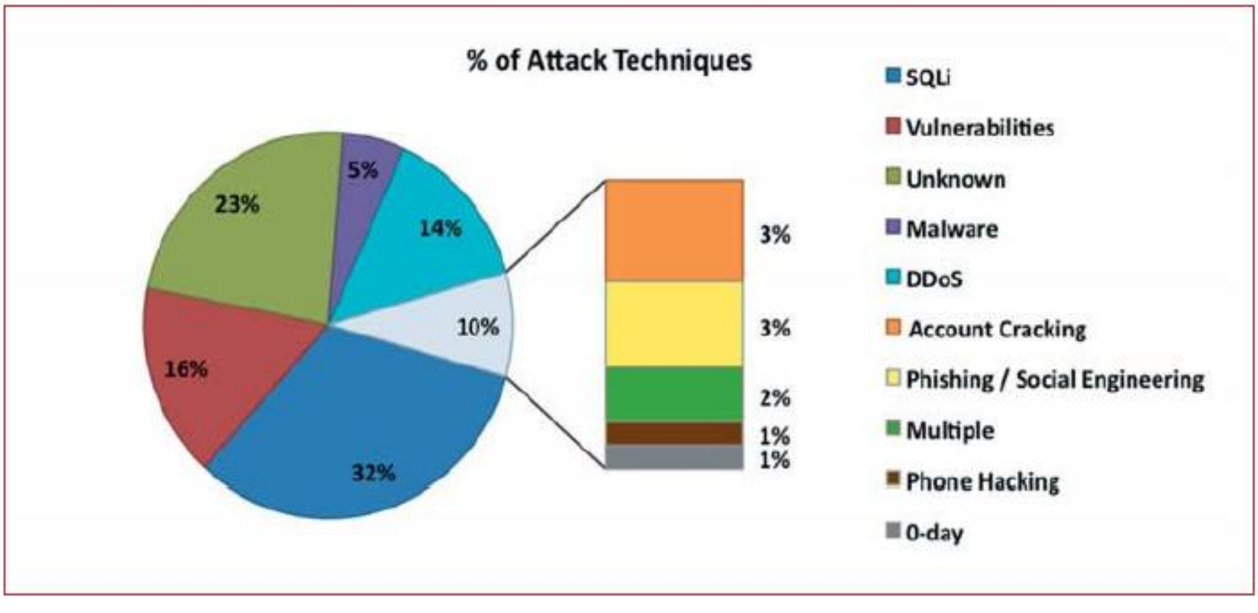
[25] http://en.wikipedia.org/wiki/False_flag
[26] http://en.wikipedia.org/wiki/False_flag



Aside from the clear majority of governmental or institutional victims and entertainment industry targets (50%), we can see that more than 1/5 of the attacks are against a group of subjects ("others") that don't belong to any main category. This means that no one is safe. We expected to find more attacks to the banking and telecommunication sectors and we wonder whether the percentages discovered actually correspond to the truth or they are due to poor public information.

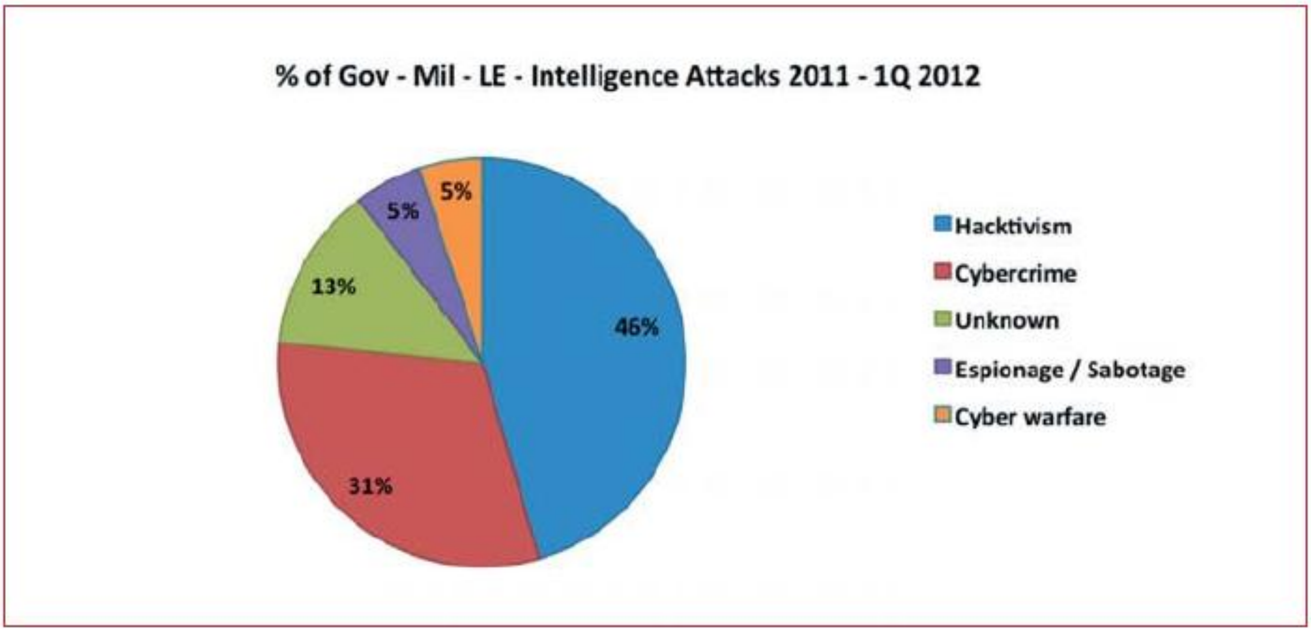
The graph of **attack techniques** offers a sadly familiar image. Most attacks (65%) have been often committed using common techniques: exploitation of a bad quality code, lack of patching, misconfiguration, organisational flaws, no user awareness and so on. These are all kinds of vulnerabilities that can and should be easily mitigated, if not eliminated.

This graph condemns security managers of the organisations affected and their stakeholders, because they clearly didn't make enough efforts to protect despite having the possibility to do so. In theory, at least.



If we move on the graph detailing **attackers per victims** interesting details come up. For example the sector more likely to be hit ("Gov.- Mil- Law Enforcement- Intelligence"). It suffered the highest number of attacks by hacktivists and received 1/3 of them by cybercriminals, plus the considerable number of attacks by unknown (which looks quite worrying).

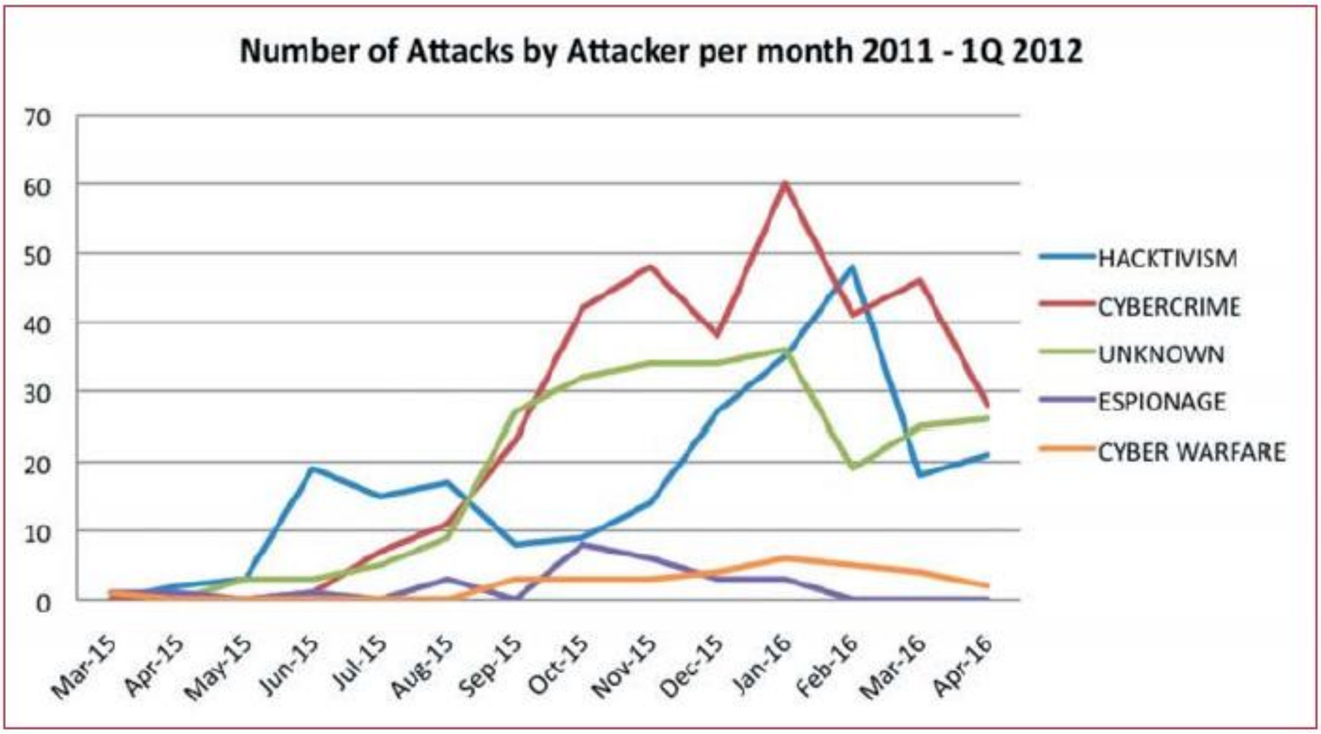
Around the half of the year, espionage/sabotage and cyber warfare attacks are getting more common, and our opinion is that these percentage are underestimated due to lack of information.



It doesn't seem possible a tiny 5% of attacks generally classifiable as "cyber warfare", when NATO[27] and the most important countries declared their defensive and offensive strategies in 2011, with military commands and specialized task forces dedicated and investing huge amount of money.[28]

It is more likely to be true that those activities are not known to the general public, and the activities that are known actions are frequently misattributed to other entities, such as cybercrime and unknown actors.

If we look at the graph focusing on actions per **type of attacker**, there is an impressive number of incidents caused by hacktivists, cybercriminals and unknown aggressors, that reached record peaks Trend confirmed for 2012 on the basis of up-to-date data (April).



[27] http://www.nato.int/cps/en/natolive/75747.htm

[28] http://www.guardian.co.uk/politics/2010/oct/17/cyberwarfare-defence-spending-increase-cuts

The resounding volume of known attacks conducted by cybercriminals (they usually have a really low-profile and tend not to be recognised), which increased over 60 times between June and January, with a peak of 2 main attacks per day in January 2012 while unknowns attacks increased *30 times* in the same period.

The growth of espionage and cyber warfare is there to be seen. It brings along a growth of the risks due to the inherent danger associated with these attacks.

Analysis of the Italian Cybercrime Situation and Perspective on Information Incidents

Italy is no exception to the 2011 growth trends of information attacks spotted in our annual 2011 data, and the main character is the phenomenon of hacktivism.

This emerging phenomenon helped raise the alarm and increase the sensibility of security managers, thanks to the media's tendency to grab popular attention. But, on the other hand, paying attention to the media distorts and diverts the attention away from a series of information incidents, some of which had a huge impact on both nation-states and their citizens.

Before moving on to the reconstruction of the chronicle of events, it is necessary to consider first the technological, social and economic factors that influenced the Italian environment;

- Technology. In 2011 Italy registered a higher number of online services accessed from mobile devices[29] and a growing number of users joining social networks such as Twitter. Although Italy is not included in the world "top 20"[30], the number of Twitter accounts[31] grew to 2 million by the end of 2011. Twitter has been considered a mean of evaluation for our analysis, as tweets turned out to be the most efficient method to communicate more or less dangerous cyber-attacks in the shortest amount of time and to the largest possible audience. In the case of hacktivism, Twitter was used to recruit proper and ad-hoc followers *while* coordinating protests at the same time.
- Culture. The notion and concept of hacking has changed along with the growth of social networks users. Sensational actions catch up, and sometimes even overtake, "traditional" devastating ones likely to remain in the shadows. Even if when clouded in doubt, these actions attracted the media because they were anticipated by a tweet, for suspense reasons, and then published on the *pastebin*[32] hacker wall. In Italy, this tendency is expressed by the alleged CNAIPIC (National Anticrime Centre) attack[33] and it encouraged a further proliferation of these sort attacks.
- Society. In the second semester of 2011 and in the first of 2012, global political instability and the general mistrust towards politicians contributed to the generation of the so called *digital natives* (note the low average age[34] of the members of the Italian Anonymous network which was broken up during the July raids) who voiced their disappointment by imitating the tactics mentioned above.

January-April 2011

The first months of the year were rich in hacktivist actions connected to the protests against the Italian intervention in Libya[35], against big strategic enterprises and against national defence entities due to alleged direct or indirect interests during the intervention itself.

[29] Audiweb Trends, December 2011

[30] http://semiocast.com/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_superseds_Japan

[31] http://www.pandemia.info/2012/02/01/2-milioni-gli-utenti-twitter-attivi-in-italia-a-fine-2011.html

[32] Pastebin (http://pastebin.com) is a website for developers. At the beginning, it helped the code stripes sharing within the community. It then turned into a virtual wall where hackers publish the outcome of their actions.

[33] http://www.repubblica.it/cronaca/2011/07/25/news/attacco_cnaipic-19587826/index.html

[34] http://www.corriere.it/cronache/11_luglio_05/anonymous-rete-svelata_7e9dffee-a6c6-11e0-bbaad83a3b6f7958.shtml

[35] http://punto-informatico.it/3102805_2/PI/News/anonymous-giorni-del-ddos-italiano.aspx

The media resonance of these actions took the attention from more important events, even from an ICT security perspective. It is hard to believe but in 2011 Italy was on the front lines of an alleged cyber war with huge consequences. On March 23rd, the American business Comodo, one of the authorities for digital certificates used for web authentication, declared that its southern European affiliate[36] had been compromised after an information attack. Although the certification cryptographic keys on which the whole core business is based had not been violated, this action let the attacker issue nine fake SSL certificates belonging to seven different Internet domains. Most of them used on the backend of webmail systems and widespread instant messaging systems[37] (mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com.)

The following March 26th an Iranian hacker and self-styled patriot declared himself responsible for the March 15th attack via a *pastebin*[38] release, offering details and proof of the attack. This information was helpful to identify the compromised business and the exploit used. The “"southern European" affiliate turned out to be Italian, whereas the breach that allowed the production of fake digital certificates was the usage of unencrypted and weak administrators credentials in the code of the certification service webpages.

Beyond Italy's borders, this wasn’t such a sensational event, even taking into account that the model given by the Certification Authority is the security pillar of web services. A relevant episode sadly happened in Italy but able to prove how bad the consequences of a low attention towards basic security rules can be. These consequences may indeed stake services management and, above all, final users.

May-August 2011

The period between May and August was characterised by the amazing actions of *LulzSec,*[39] whose effects were felt even in Italy. Even if the group spontaneously broke up on June 25th[40] (thanks to an international manhunt by police and *grayhat* hackers, who were against their ideology and methods[41]), many of the actions LulzSec carried out during its 50 days of activity/hacktivism generated enough publicity to win over many supporters in Italy as well as in other countries. Many criminal actions were conducted under the guise of digital protest (mainly *Distributed Denial of Service* – DDoS), undertaken in name of movements like Anonymous and Antisec. A key role was played by social networks, fundamentally important in the recruitment of proselytes.

The major consequences were registered between June and July 2011 when numerous institutional and enterprises were hit by a *Distributed Denial of Service*[42][43]– DDoS attack with a varying results based on the security posture and education level of the victims. This “hot” period's target list was wide and included Italian governmental websites, political parties such as Freedom People Party and Northern League, and organisations like Agcom, Poste, Telecom Italia and the Italian Stock Exchange.

In July the most sensational and confounding events took place. July 6th - straight after the postal police raid that netted 15 presumed Italian Anonymous group members (five of them underage,) data from 18 universities (Rome, Milan, Turin, Naples and Bari[44] (to state but a few) were published.

[36] http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/

[37] http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

[38] http://pastebin.com/74KXCaEZ

[39] Word coming from the union of two names: *Lulz*, slang term for laugh, and *Sec*, abbreviation for Security.

[40] http://pastebin.com/1znEGmHa

[41] http://arstechnica.com/security/news/2011/06/dox-everywhere-lulzsec-under-attack-from-hackers-lawenforcement.ars

[42] http://www.repubblica.it/politica/2011/06/21/news/attacco_hacker_ai_siti_governativi_anonymous_rivendica_l_azione-18022991/index.html

[43] http://www.repubblica.it/tecnologia/2011/06/28/news/anonymus_agcom-18348847/index.html

[44] http://www.repubblica.it/tecnologia/2011/07/06/news/hacker_di_nuovo_all_attaco_stavolta_delle_univesit_italiane-18761507/

Even if we dismiss the alleged *hacktivist* nature of the action and the poor value of the stolen information, the event is significant because it offers a merciless overview of the Italian situation: vitally important institutions were hit and, even worse, unencrypted authentication credentials became public, clashing with the law and the basic rules for safe data conservation. It is even more paradoxical if we think that universities have the know-how to manage their information assets securely.

The security incident that involved CNAIPIC[45] further proved that the Italian cyber-attacks were essentially "copy-cat" jobs and not a centrally organized activity. This event became famous for the media fuss about it and for the subsequent claims and denials by local Anonymous rather than the effective value of the data stolen and divulged. Many aspects of the episode are still to be unravelled, as well as the fact that the international attacks committed on law enforcement agencies and contractors[46] were committed at the same time. The attacks against the defence contractor Vitrociset[47] and the self-governing Correction Officers Trade Union[48] SAPPE have been probably influenced by the above-mentioned events. Both actors suffered from website *defacement* actions and, in the case of the contractor, even the publication of information related to the internal services structure.

In this scenario dominated by hacktivism there is one exception. In August an attack hit the Italian hospital and hospice Pio Albergo Trivulzio[49] and erased both patient and user data. A different attack from the previous ones with major and accountable impacts on people but, strangely, less on the media.

September – December 2011

During the last quarter of 2011, the negative wave stemming from August cooled down and attacks considerably decreased; only rare episodes were registered. This uniquely Italian tendency was in contrast with the rest of the world, where after the boost of global protests (from *indignados* to *OccupyWallStreet*) the number of information attacks generally increased.

January – April 2012

At the beginning of the year hacktivism percolated alongside the protests against SOPA and PIPA laws (the attacks a peak between January 19th and 20th when the FBI seized the MegaUpload servers) first, and after the ACTA treaty signed by 22 countries member of the EU.

In Italy organisations accused of defending the old copyright model (SIAE, copyright.it) and the Ministry of Justice[50] have, predictably, been in the hacktivists’ crosshairs. It was in protest against Fava’s bill (rejected by the Chamber of Deputies the following February 1st) - the Italian ACTA.

In March came further political instability and social unrest. For example the incidents in the building site of the TAV (*Italian acronym for Treno ad Alta Velocità i.e. HSR, High-Speed Railway*) in the Susa Valley, Piedmont, the attacks on the transport and energy sectors stepped up again.

Vatican State has been targeted in information attacks too: the institutional website suffered four DDoS attacks between March 7th and 22nd [51]and minor actions harmed relevant websites. The action stems from a hasty interview in the New York Times with a Vatican security partner who claimed he had profiled and thwarted an Anonymous attack attempt.

[45] http://www.corriere.it/cronache/11_luglio_25/attacco-anonymous-polizia_90f08330-b6b9-11e0-b3db-8b396944e2a2.shtml

[46] http://hackmageddon.com/2011/08/16/antisec-hacks-another-defense-contractor/

[47] http://www.repubblica.it/cronaca/2011/08/01/news/anonymous_attacca_la_vitrociset_non_meritate_i_soldi_pubblici-19879883/index.html

[48] http://www.repubblica.it/cronaca/2011/08/06/news/hacker_contro_la_polizia_colpito_il_sito_del_sappe-20122634/index.html

[49] http://milano.corriere.it/milano/notizie/cronaca/11_agosto_25/20110825MIL03_13-1901359693338.shtml

[50] http://cylaw.info/?p=72

[51] http://anon-news.blogspot.it/2012/03/vaticanva-4-0-benedictomexicomx-tango_22.html

Although the nature of the event has yet to be clarified, it is important to see that an alleged information attack on the SNAI (state-owned *Italian gaming company*) VLTs may have caused anomalous winnings on April 16th [52], due to alleged tampering of 3000 devices throughout the whole country. No payment has been given to the unwary winners. Whether the episode is true or false, gaming and gambling platforms are a juicy prey for prowlers.

Analysis of attacks distribution and type

From February 2011 to April 2012, 127 attacks took place in Italy; 112 of them (88% of the total amount) were committed by hacktivists. Only 15 cases can traced back to cybercrime (14 of them) and cyber-espionage.

From the sample data we can see that more than 43% of the targets are governmental or politically-related/general association sites, whereas education is in third place with an attack concentration in July, when 18 universities were simultaneously hit.

The entertainment industry, police and MP are far behind in the ranks, but they lead the other categories due to the January attacks during the SOPA/PIPA protests, the MegaUpoload shutdown and associated protests.

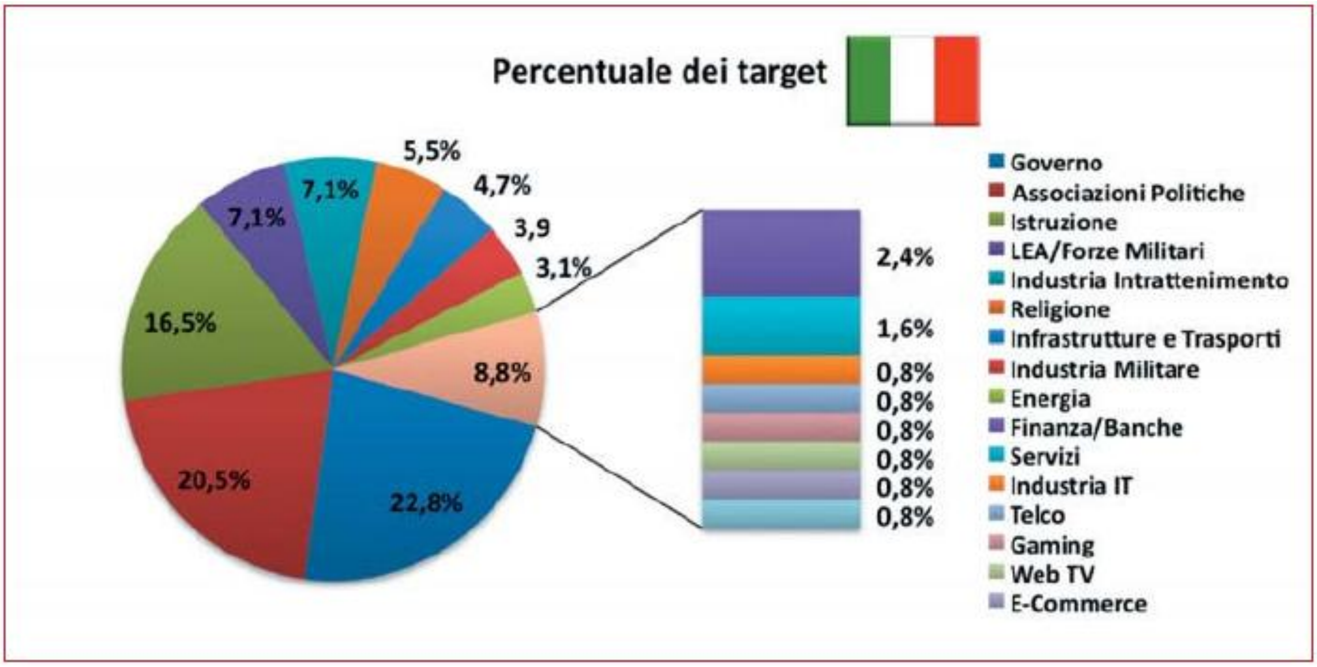
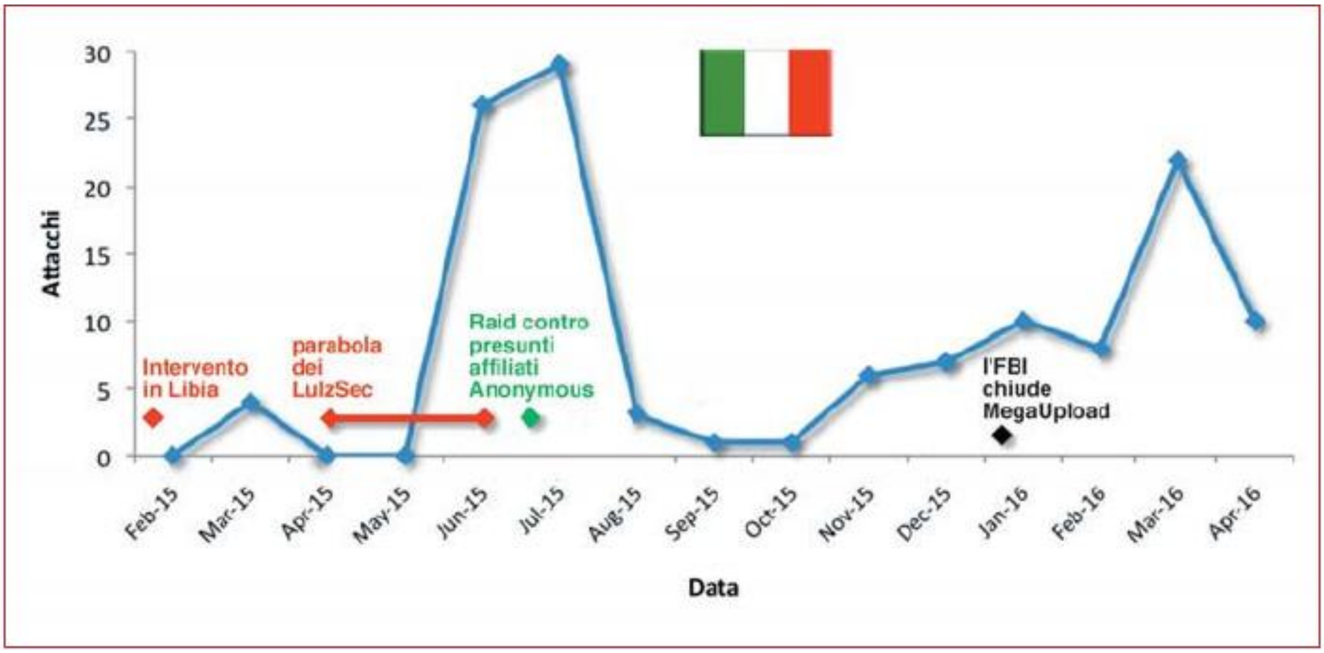


Figure 1: Target percentage

According to the trend analysis, Italian hacktivism feels the influence of external factors: the Libyan intervention first, the emotional impact of LulzSec and then the protests against bills considered repressive of Internet freedom of expression

[52] http://www3.lastampa.it/cronache/sezioni/articolo/lstp/450787/



Hactivism only? Not really..

Hacktivism contributed to a renewed focus on the issue of data protection, but it is not the only phenomenon that interested Italy. It would be a mistake to only consider DDoS attacks on websites. The case of Pio Albergo Trivulzio, for instance, shows that "minor" cases which had little, or no, resonance in the media compared to hacktivist attacks, often had a much bigger impact on the lives of citizens and users.

On the same level were the alleged attacks on the SNAI video lottery terminals. Unaware users could see their dreams (and their money) vanish within hours because of a malfunctioning terminal. The state-owned firm blamed the incidents on an alleged hacker attack.

For an average user, is it more important that a political party's website in not available for a couple of hours, or that his electronic medical chart has been deleted from a hospital's systems with no chance of recovery? Or again, that he can't cash in his winnings, or had his online money vanish?

Now that both public and private entities are prone to adopt new technologies and new ways of accessing and sharing information, the security of data and information facilities are popular topics. 2012 must be faced without feelings, prejudices and with a clear normative and technological strategy in mind.

On the technological side, personal affinities do not have to be taken into account from those responsible for the defence of an organisation and its data. They have instead to plan possible defences and investments neutrally, balancing the risks and focusing on the user.

On the legal side, the right to privacy and the informed consensus on risks(and responsibilities) of the online services have to be carefully considered by vendors. At the same time, users have a right to be informed of their situation and related responsibilities.

In this scenario - with some delay - institutions are trying to repair the situation by uniformly deploying the various European laws. A clear example of this trend is the initiative to create a community law[53] which protects the privacy of users and forces organisations to publicly announce a data breach within 24 hours.

A new concept of data security

In the technological and normative process cited above, the seemingly unstoppable glut of mobile devices in the hands of users works as a catalyst. At the end of 2012, the number of mobile devices will overtake the number of inhabitants in the world and, in 2016, the data will grow up to 1,4 per

[53] http://www.bbc.co.uk/news/technology-16722229

person[54]. The increasing usage and the familiarity with the technology pushes the user to use even more online services, creating a new scenario characterised by a new idea of data availability. This is not physically located on a device but inside a "cloud" for a real-time use possibility. It is a technology, normative and cultural revolution that involves adaptation of confidentiality, integrity and availability standards on which the risk analysis is based.

On the one side, we also have to stress that the most frequent 2011-2012 security events are DDoS attacks and on the other that it's not just information attacks threatening data availability for 2011. Most of the discomforts for the users were due to accidental service interruptions (like the notorious *Poste Italiane*[55] and Aruba[56] cases) that, according to the reactions[57], met totally unprepared users.

It is not only the user being unprepared

As demonstrated in 2011, Italy still has a lot to work ahead: this is seen in the way Italian businesses reacted to the news that a popular authentication technology deployed in many global enterprises, some of which are Italian, was violated: on March 17th 2011, RSA Security admitted it was the victim of an illegal intrusion[58] causing the theft of elements *"potentially capable of reducing the efficiency of the authentication system"*. It often happens that fears becomes reality and two months after, on June 2nd, news regarding a failed attack against an important American defence contractor and multinational, Lockheed Martin, was made public. The attack was a direct and subsequent result of the theft of RSA's authentication token IP in March[59].

These eventful days pushed many customers to request the substitution of authentication devices provided by RSA. The replacement operation cost 66 million dollars[60] to the provider (which, commendably, replaced the compromised devices for free) and, in the banking sector, roughly 100 million dollars were charged to the organizations[61] for the shipping and handling of the new devices.

Although the situation in the States was well known by the U.S. Senate[62], nothing similar happened in Italy. Even with the relatively small chance that an Italian RSA client was compromised, more transparency and an awareness campaign focusing on the issue would have been expected.

With strong indications of the intrusion being a foreign operation[63], it was then hypothesized that the same attack was committed against other 760 organisations in the world. Italian organisations were listed as possible targets which leaves us to a final open question: if the main businesses and local bodies based in Italy are already struggling to detect evident attacks like a DDoS, how many of them, if hit by the same sort of sophisticated attack mentioned above, would be effectively able to detect and thwart it?

Cybercrime and online security for citizens

Our focus on actions committed on a very large scale does not imply that we want to overlook the problem of conventional cybercrime which is much closer to citizens; incidents involving identity theft, fraud, online stalking and child pornography, appear all too often in our newspapers.

[54] http://arstechnica.com/business/news/2012/02/mobile-internet-devices-will-outnumber-humans-this-yearcisco-predicts.ars

[55] http://daily.wired.it/news/tech/2011/06/08/caos-sistemi-poste-italiane.html

[56] http://corrierefiorentino.corriere.it/firenze/notizie/cronaca/2011/8-luglio-2011/aruba-nuovo-crash-utenti-siinfuriano-rete-1901048893939.shtml

[57] http://palermo.repubblica.it/cronaca/2011/06/07/news/poste_in_tilt_tra_guasti_code_e_proteste_c_chi_ chiama_il_113_simulando_una_rapina-17319998/index.html

[58] http://www.rsa.com/node.aspx?id=3872

[59] http://www.rsa.com/node.aspx?id=3891

[60] http://www.theregister.co.uk/2011/07/27/rsa_security_breach/

[61] http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html

[62] http://www.reuters.com/article/2011/05/31/usa-defense-hackers-idUSN3110255620110531

[63] http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/

Although technology and current laws (in particular the Digital Administration Code, acknowledged by Italy with a legislative decree on December 30th 2010) enable the fusion real and digital identities in cyberspace, there is a lack of security culture and awareness of the risks on behalf of the users. They keep behaving dangerously as if the fact that they cannot be hurt physically would make the risk less probable or dangerous.

A recent study, published on the Safer Internet Day last February 7th 2012, confirmed this rather unappealing scenario[64]. In Italy only 2% of Internet users had an adequate grasp of the risks and had enough knowledge of the web to protect himself; 71%, even having a basic protection, would not be able to defend himself from the risks related to the improper use of their digital identity. Such a digital population is bound to be victim of one kind of online swindle or another.

Yet if the education of the digital citizen seems so low, cybercriminals are not wasting time and thus thinking of more aggressive and sophisticated offences able to hit the user psychologically: phishing e-mails written in an imperfect Italian is simply a fading memory today. An example of a new technique is the *ransomware*[65], which only recently arrived in Italy[66], able to deceive the victim by imitating a fake PC seizure by the Financial Guards (because it contained pornographic or illegal content, for example) By paying an online “fine” to the unknown criminals everything clears up, but this attack suggests that cybercriminals seek to exploit technological, cultural and emotional vulnerabilities of the user.

Technology unwillingly helps the proliferation of risks: studies show that social networks push the users to expose their digital identity[67] too much and they also risk new forms of cybercrime such as cyberbulling. The increasing use of mobile devices to access the net increases the exposure to threats like phishing[68], the installation of insecure application or improper use of details (it is hard to recognise a counterfeit webpage on a 3.7” screen.)

As concerns online pedopornography, despite last year's successful operations in combating this loathsome cybercrime (ex: *Fabulinus* operation[69] in January 2012 and two European raids in March[70] and December[71], among others) the phenomenon is expanding. According to data published by the National Observatory of *Telefono Arcobaleno* [72] in November 2011, the first eleven months of 2011 registered reports of 68,000 websites containing pedopornographic material from 17 countries, an increase over the 54,000 of 2010.

The reality of online security for the citizen will be thoroughly examined in the next chapter of the Report, where the Postal and Communications Police gives a detailed overview of these types of cybercrimes.

How much is cybercrime worth in Italy?

There are no official statistics on the frequency of these attacks; part of it is due to the “cultural difficulty” and the unwillingness of the victims to report them.

Data from companies busy in this sector[73] say that Italian citizens pay up to 6,7 billion euro per year; 6,1 billion of them are for the time wasted by the victims to repair the consequences of the attacks and the remaining 600 million are direct costs, which means money lost for the crime incurred.

[64] http://www.microsoft.com/italy/newscenter/Default2.aspx?id=541&pars={mcsi}{}{}{}{}

[65] Malicious software that limits the victim’s computer functions and ask for a ransom to restore the computer.

[66] http://totaldefense.com/blogs/security-advisor/2011/12/19/ransomware-exploits-the-italian-police.aspx

[67] http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1

[68] http://w2spconf.com/2011/papers/felt-mobilephishing.pdf

[69] http://www.televideo.rai.it/televideo/pub/articolo.jsp?id=11340

[70] http://punto-informatico.it/3111559/PI/News/pedoporno-retata-europea.aspx

[71] http://punto-informatico.it/3370257/PI/Brevi/pedoporno-nuova-retata-europea.aspx

[72] http://www.telefonoarcobaleno.org/?page_id=1123

[73] http://www.symantec.com/content/it/it/home_homeoffice/html/cybercrimereport/

Despite the impressive figures and the huge amounts of money "vaporized" by cybercrime, the risks remain underestimated. While an exact evaluation is not possible, we can take the data of the English economy as an example and compare them to the Italian case. In 2011, the United Kingdom announced that an annual cost of 32 billion pounds[74] was calculated. Commented on the source paper, former British Security Minister, Baroness Neville-Jones, stated, “cybercrime is a bit like terrorism - the more you know the more frightening it looks.” If that is true, the conditions are far from encouraging.

[74] http://www.zdnet.co.uk/news/security-threats/2011/02/17/cybercrime-costs-the-uk-27bn-a-year-40091851/

Main Trends for 2012

When putting together this chapter, which could have been a book unto itself due to the variety of issues covered, we thought that a summary would have been better. We will not delve too deeply into technical issues so to make it more appreciable by the highest number of readers, whatever their background.

In general terms, there are two macro-phenomena which will lead to an increase in security related issues in 2012, as it happened in the past but with major implications: first is the unstoppable spread of the latest technologies, tools and digital services, inevitable and existential components for many citizens whether living in industrialized or developing countries. On the other side, the lack of important improvements in the legal, organisational and operative fields of counter activity to cybercrime and all the other sources of risks (espionage, hacktivism, terrorism, cyber warfare) that are threatening ICT today.

Forecasts are made upon good sense, rumours between pundits and from the current analysis. The so called “black swan” - like high-impact, low-probability (HILP) - events have not been taken into consideration as they are extraordinary and unpredictable, though it would be important to state that the current trends of insecurity helps their development.

Cybercrime

The *Global Risk Report 2012* from the World Economic Forum[75] ranked cybercrime in first place in the “technological risks”. It analyses the 50 main global threats of the following 10 years and divides them on the basis of impact and probability.

The unstoppable growth of this new form of criminality will continue in 2012, reaching pathological levels causing direct and indirect damage costing hundreds of billions of dollars.

As no entrance barriers and few disincentives are in place to prevent it, other criminal groups will definitely join the ones already active, making the number of information incidents (traditional crimes and ones committed/guided by information systems) increase.

The cybercrime ecosystem will get more articulated, becoming a parallel economy where various players exchange services (until proper forms of “crime as a service” emerge) and learn by trading exploits, malware, access to compromised systems, personal and financial data and so on in a global illegal market, with international organised crime managers running the show, not *black hat*[76] hackers anymore.

Within this scenario, fields that show higher development rate in ICT, that is to say mobile systems (smartphones, tablets), social networks and the cloud, will be particularly, and not by chance, exploited by cybercriminals.

As regards **mobile systems**, it is reasonable to think that 2012 will be the first year for them to register an exponential growth of threats and attacks, as 2011 was for “traditional” ICT.

Mobile systems will constitute and escalating portion of botnets as they have valuable processing power and bandwidth, and most of them are not provided with effective anti-malware protections, users often tamper them to unlock some advanced functions, which often make them even more vulnerable.

Even considered as simple gadgets, mobile systems have advanced features that help attackers to exploit their distinctive characteristics (geolocation above all) to commit new and increasingly insidious forms of crime. We must underline the vast spread of these devices especially among youngsters will inevitably lead to a sharp increase of crimes against these population groups.

The portability and the convenience of mobile systems will also make dual use cases: the private

[75] http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf
[76] http://en.wikipedia.org/wiki/Black_hats

and/or business hybrid usage of the same device (commonly defined *IT consumerization*[77]) is becoming very common and will bring about new vulnerabilities which are hard to manage within the affected organisations.

The phenomenon will also become more intense because of the general lack of a specific know-how by IT managers, low awareness of the end user and the lower security inherent in the devices, which are significantly more immature if compared to PCs and more difficult to be placed within existing security and usage policies and control systems.

The large scale introduction of NFC (Near Field Communication) technologies and the "*digital wallet*"[78] to help users perform small transactions via smartphones let us easily predict a rise in fraud and attacks, making the situation even worse.

At last, the wide spread of mobile devices shows that Italy is going to be one of the countries mostly affected by the increasing number of incidents and attacks (with the related costs) and since no ad hoc structure are available in the country for data gathering, it will be difficult to track the situation properly. Consequently, counteract activities will become slow and hard to be supervised.

Whereas for **social networks,** the possibility to target a huge user base, the absence of effective controls and the impunity of the majority of cybercriminals will boost illegal actions through them so much so that in 2012 social networks will outclass e-mails as main attack carrier for private users and will become one of the most dangerous risks both for private users and organizations.

Identity theft, reputation and privacy damage, stalking, fraud, phishing, malware diffusion, social engineering activities and intellectual property theft will become even more common and are bound to hit millions of users and thousands of organisations every month.

Attackers will also arrange simultaneous exploitation of mobile devices - very common means to connect to social networks - and the social networks themselves to make their criminal campaigns increasingly effective.

Italy is today in the world's top ten for social network usage (37% of the Italian population, or more than 20 million people, have a Facebook account), so it is reasonable to think that every form of cybercrime victim in our country, from the lightest to the more severe, will be *hundreds of thousands* throughout 2012.

Considering the predictions, it is also possible that specialised social networking platforms will develop as non-generalist platforms closed to particular groups of interests with more limits in terms of membership, identity verification and real time monitoring of *social conversations*, aiding in the mitigation of risks related to their use.

A potentially dangerous phenomenon will also threaten **cloud computing**: the lack of proper controls that will make cybercriminal organisations use it as a tool to maximise their impact, buying (or penetrating) cloud services to propagate malware, to host illegal materials and to gain fairly endless processing power and bandwidth, *password cracking*[79] on a large scale n 79 is an example.

Cybercriminals will practically be able to gain by exploiting the cloud and obtaining their own facilities to repurpose their use to other criminal groups. As tough as it may seem, nipping this phenomenon in the bud without doubts or delays will be crucial to counteract to the growth of cybercrime in 2012 and in the following years.

Hacktivism

Hacktivism will respond to the same incentives that made cybercrime so common, plus the global crisis and the unavoidable consequences of social unrest.

While past activities have been demonstrative and aimed at creating furor so far, they could become

[77] http://en.wikipedia.org/wiki/Consumerization

[78] http://en.wikipedia.org/wiki/Digital_wallet

[79] http://www.darkreading.com/authentication/167901072/security/encryption/229000423/cloud-based-crypto-cracking-tool-to-be-unleashed-at-black-hat-dc.html

a constant phenomenon in the global ICT scenario and play the role of protest and pressure tool for rival groups of every ideology. The number and the gravity of the attacks will increase and more targets will be included.

Even without high impact incidents, hacktivism will presumably lead to serious consequences at some point in the immediate future.

The first negative outcome we notice is the explosion of imitators and copycat actors, and the growth of active supporters belonging to the most important hacktivist groups or brands, especially among youngsters. This may happen as it is very easy to find tools online to perpetrate DDoS attacks or intrusions in information systems.

This must not be underestimated because a DDoS attack committed by tens or hundreds of thousands of people (they don't have to be professionals, it is often enough to click on a link received via Twitter) can crash any type of system and organisations in the world, though admitting for a short amount of time, both civil and military.

Secondly, the possibility that hacktivists activities may be used by politicians, corporations, terrorists, intelligence agencies to hide other attacks has to be considered as well. Given that hacktivists announce and coordinate their actions, usually through social networks, it is possible that someone may try to take advantage from the chaos and the distraction of the targets to perpetrate stealthy operations of their own, with much more severe consequences.

As 2012 is going to be a year full of important events (Olympics, European Football Championship, American Presidential elections and so on) we should expect that many hacktivists groups will be tempted to commit extraordinary and unprecedented actions. Moreover, once hacktivists will have realised how strong they are and the media (and sometimes geopolitical) noise they can produce, they may gather in a united front (something that hasn't happened yet) and band together against common targets, amassing a considerable degree of “digital fire power”, equivalent in cyberspace to the superpower in the physic world.

Espionage

In 2011 cyber-espionage has been declared as the most important method of obtaining any kind of private information in the world. It is estimated that cyber-espionage operations against valuable IP could have a potential global up to one trillion dollars.

There are three kinds of cyber-espionage: by intelligence agencies (directly or via proxy, like mercenary groups), industrial (backed by various state or non-state actors) and the available-to-all Open Source Intelligence[80] (OSINT) operations.

We also need to add psychological warfare[81] (PsyOps), deception and disinformation[82] activities (Information Warfare) as well as new difficulties in counter-espionage, thanks to the fertile ground of cyberspace.

The USA and many other countries accuse China of being particularly aggressive in this field - even though the situation is, to be precise, far more complex - and after many confirmed and public incidents we can assume that cyber-espionage is widely used by every State and practised by allies without hesitation or limits.

Within this context, projects, patents, formulas, source code, financial information, business data, building plans of weapon systems, nuclear power plants, oilfields etc. are all targeted. Billions of dollars in research and acquisition funding have been suspended[83] or postponed and economic sectors suffered from the theft of information.

In 2012, thanks to the weak security posture of technologies being deployed, we will surely see an

[80] http://en.wikipedia.org/wiki/OSINT

[81] http://en.wikipedia.org/wiki/Psychological_warfare

[82] http://en.wikipedia.org/wiki/Information_Warfare

[83] http://www.theglobeandmail.com/report-on-business/small-business/sb-growth/day-to-day/potash-hackersa-wake-up-call-for-lawyers/article2261700/print/

uptick in cyber-espionage activities, causing damage to a higher number of players, in size and in scope.

As regards Italy, whose production is famously based on SMEs with a considerable amount of know-how, cyber-espionage may have a disparate and negative impact on Italian industry, which is unprepared for attacks of this calibre.

Institutions should alert and help Italian companies to reduce their exposure to cyber-espionage, to preserve their intellectual property and know-how which make them unique, or Italy as a nation risk major competitive failures in the global market.

Sabotage / Cyber Warfare

While there are many well-known examples of cyber warfare operations from the 80's on, the topic only hit the media in 2011 after top-ranking military officials and chancelleries began debating it openly.

A real war in cyberspace is unlikely to be fought, at least not in the coming years, but there are increasing sabotage activities in the so called “fifth domain of warfare”; cyberspace being the fifth after land, sea, air and space.

What is more likely to happen during 2012 is an increased "transparency", with states admitting their interest, forming organizational structures and units, and the accompanying investments from the great powers as they slowly research and acquire **cyber weapons**[84].

In practical terms a “cyber cold war” is going on at the moment. The impasse situation is due to the common fear of not being able to face a cyber-attack.

The major concerns include the impossibility - or huge difficulty - in determining where the attack came from and how to respond (eg, with reprisals for example). And, of course, the fact that the most technologically advanced countries are more vulnerable to these attacks, negating the traditional monopoly on advanced weapon systems.

From this scenario we see that the most common fear is the possibility of attacks on critical facilities, aiming at the weak computer-assisted industrial control systems that are used to manage these plants, from electricity generation to water distribution, transportation and goods production, etc.

In 2012 the *critical system failure* is going to increase, which means the possibility for critical facilities to trigger incidents with domino effect, negative impacts on the whole social and economic system of a state or geographic area.

While the information systems used from industrial automation were projected to offer the highest warranties of continuity and operative security, they have not been prepared for information attacks. The last years have shown that, starting with the international case of the cyber weapon Stuxnet[85], used against Iranian nuclear installations in 2010, the conditions have substantially changed and these information systems are today extremely vulnerable to any kind of attack with potentially devastating consequences.

The attention of the actors involved in cyber warfare was grabbed (many of these systems correspond to the ideal target, from a military point of view) and we are therefore now approaching a period of mounting risks, both of individual installations and of their distributed systems. There are indeed difficulties in the update and hardening of these systems and in the speed of growth of the threats.

Here, too, Italy appears to be vulnerable and not at all ready to face the issues. More attention has to be devoted to the issue as, even if Italy is not one of the leading economies in the world, it is one of the few industrialised countries with no national strategy on cyber warfare. Only the latest “Report on 2011 Information Policy for Security”[86] proves to be a very tiny step forward.

[84] http://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf

[85] http://it.wikipedia.org/wiki/Stuxnet

[86] http://www.sicurezzanazionale.gov.it/web.nsf/pagine/relazione/2011/le-sfide-globali.pdf

2012 and beyond?

Based on the preliminary data of the attacks committed from January to April of the current year, 2012 is bound to become a more complex year than 2011 as far as information systems, data and transaction security are concerned.

Although recent data indicates that the global ICT security market will reach 60 billion dollars[87] in 2012 the truth is that, in light of the critical period, the number is inadequate compared to the global GDP percentage produced directly or indirectly through information systems and the exponential growth of the threats.

Assuming that a third of the world GDP[88], 20 trillion dollars, is now produced by information application in any forms (web, communications, services, industry, transport and so forth), 60 billion dollars is only 0,3% of the wealth generated by ICT.[89]

Under another perspective, IT security expenses are today only 15% of the direct or indirect losses produced by security incidents (overall estimated in 388 billion dollars[90]): the disproportion is clear.

There is a lesson we all can and must learn from the analysis of what happened last year and it is that, whether we like it or not, we are now at a crossroads.

Unless we dedicate far more attention, time and sources to secure the information systems and to elevate the awareness level of the all players by adapting methodologies, processes, normatives and tools and by pushing vendors to create secure products, we will soon find it harder to apply ICT effectively and with the ROI we are accustomed to.

If we adapt the current tendencies to the near future, if the security incidents increase in terms of frequency and gravity for the next three years, *costs will increase quicker than benefits*. It means that a vicious circle of declining gains will trigger and we will have forget many of the advantages provided by ICT in the last three decades because of the endemic unreliability and riskiness of the new threats.

However paradoxical this hypothesis may sound, we should remember how far and remote a global economic crisis seemed in 2004, 36 months before it began. In a complicated and interconnected method based on just-in –time actions and hyper-efficiency, the dynamics changed very fast and the margins for errors were reduced to the minimum. On the other hand, economic, strategic and tactical advantages for prowlers are huge, whereas the risk of been caught is way too low.

In conclusion, we cannot idly abandon ICT to a sustainability crisis due to the insecurity and “Wild West” situation that is now taking shape. We have to act now at all levels and without hesitation to avoid the systemic effects that would stem and cause damages not even yet quantifiable, but certainly more severe for individual victims and, globally, harder to bear.

Italy, as industrialised country with a series of “original sins”(poor information culture, few investments in security, negligence of law makers for information security, SMEs as leaders in the production process not equipped against information threats) it is urgent to change this path.

After having stated the consequences of the above described actions, the ideal outcome is that the interested parties (citizens, institutions, enterprises, technology vendors) assume a diligent role and quickly elaborate strategies capable of counteracting a continued devolution of the current scenario.

[87] http://www.franchise.appinonline.com/security-market-size.html
[88] http://en.wikipedia.org/wiki/World_economy
[89] http://www.nsf.gov/statistics/seind10/c6/c6h.htm
[90] http://www.symantec.com/content/it/it/home_homeoffice/html/cybercrimereport

BIBLIOGRAPHY

[1] The State of the Internet, Q3 2011 Report – Akamay

http://www.akamai.com/dl/akamai/soti_slides_q3_2011.pdf

[2] Assintel Report 2011 – Assintel

http://www.assintel.it/jsp/download.jsp?go=../INDAGINI/2011_Assintel_Report.zip

[3] Annual Security Report 2011 – Cisco

http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf

[4] Cisco Connected World Technology Report - Cisco

http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011-CCWTR-Chapter-3-Media-Deck.pdf

[5] Panorama de la Cyber-criminalité – Clusif

https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER%2DCRIMINALITE

[6] Relazione sulla politica dell'informazione per la sicurezza nell'anno 2011 – Governo Italiano
http://www.sicurezzanazionale.gov.it/web.nsf/pagine/relazione/2011/le-sfide-globali.pdf

[7] Report IBM X-Force 2011 – IBM

http://www-01.ibm.com/software/it/itsolutions/security/

[8] McAfee and Security Defence Agenda Report 2012 – McAfee

http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf.

[9] Rapporti semestrali - MELANI

http://www.melani.admin.ch/dokumentation/00123/00124/index.html?lang=it

[10] Secunia Yearly Report 2011 – Secunia

http://secunia.com/?action=fetch&filename=secunia_yearly_report_2011.pdf

[11] Short Report Novembre 2011 – Telefono Arcobaleno

http://www.telefonoarcobaleno.org/?page_id=1123

[12] Survey – Trend Micro

http://www.trendmicro.com/us/security-intelligence/research-and-analysis/index.html

[13] Consumerization Survey – Trend Micro

http://partnerprogramme.trendmicro.eu/content/Collateral/CONSUMERIZ_SURVEY_TrendMicro_20_October.pdf

[14] Global Risks Report 2012 – World Economic Forum

http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Other sources:

[15] Report 2011: Russian Cybercrime Market – IB Group

[16] CARO 2011: Cybercrime in Russia – ESET

[17] Absolute Sownage, A concise history of recent Sony hacks – Attrition.org

http://attrition.org/security/rant/sony_aka_sownage.html

[18] Attacco alla HBGary Federal – Wikipedia.org

http://it.wikipedia.org/wiki/Anonymous#Attacco_alla_HBGary_Federal

[19] Aaron Barr, Cybersecurity Analyst Who Was Hacked By Anonymous And Infiltrated Occupy Wall Street,

Gets Fired - TheHuffingtonPost.com

http://www.huffingtonpost.com/2012/01/20/aaron-barr-cybersecurity-anonymous-occupy-wallstreet_n_1219328.html

[20] Citi Credit Card Hack Bigger Than Originally Disclosed – Wired.com

http://www.wired.com/threatlevel/2011/06/citibank-hacked/

[21] Postbank loses R42m to cybercrime syndicate – News24.com

http://www.news24.com/SouthAfrica/News/R42m-stole-in-Postbank-hijacking-20120114

[22] Comodo hacker: I hacked DigiNotar too; other CAs breached – Arstechnica.com

http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars

[23] 300,000 Iranian users victim of internet spying – The Times of India Internet

http://timesofindia.indiatimes.com/tech/news/internet/-300000-Iranian-users-victim-of-internetspying/articleshow/9883306.cms

[24] DigiNotar Compromise - Gervase Markham

http://blog.gerv.net/2011/09/diginotar-compromise/

[25] Diginotar case: Increasing the resistance against infringements – cyberwarzone.com

http://cyberwarzone.com/cyberwarfare/diginotar-case-increasing-resistance-against-infringements

[26] The DigiNotar Debacle, and what you should do about it – blog di torproject.org

https://blog.torproject.org/blog/diginotar-debacle-and-what-you-should-do-about-it

[27] 'Nitro' hackers use stock malware to steal chemical, defense secrets - Computerworld

http://www.computerworld.com/s/article/9221335/_Nitro_hackers_use_stock_malware_to_steal_chemical_defense_secrets

[28] Chinese hackers break into oil companies' networks – SCMagazine.com

http://www.scmagazine.com/chinese-hackers-break-into-oil-companies-networks/article/196099/

[29] Cyber War Against U.S. – China Involved In “The Greatest Transfer of Wealth In the History of the World” – Independent News Hub

http://independentnewshub.com/?p=49536

[30] Spear Phishing – Techtarget

http://searchsecurity.techtarget.com/definition/spear-phishing

[31] 2011 Cyber Attacks Timeline Master Index – hackmageddon.com

http://paulsparrows.wordpress.com/2011-cyber-attacks-timeline-master-index/

[32] Origins of Global Hacks – NCC Group

http://www.nccgroup.com/NewsAndEvents/Latest/12-02-01/Origins_of_Global_Hacks.aspx

[33] TDSS Botnet Virtually 'Indestructible', Kaspersky Researchers Say – CRN.com

http://www.crn.com/news/security/231000907/tdss-botnet-virtually-indestructible-kaspersky-researcherssay.htm

[34] Attribution in cyber attacks is difficult but not impossible – Secure Nation

http://securenation.wordpress.com/2010/02/27/attribution-in-cyber-attacks-is-difficult-but-not-impossible

[35] Defending against cyber attacks – NATO

http://www.nato.int/cps/en/natolive/75747.htm

[36] Cyberwarfare defence spending to rise despite cuts – The Guardian

http://www.guardian.co.uk/politics/2010/oct/17/cyberwarfare-defence-spending-increase-cuts

[37] Audiweb Trends, dicembre 2011 - Dati cumulati cicli 1, 2, 3, 4 del 2011 – Audiweb

[38] Brazil becomes 2nd country on Twitter, Japan 3rd Netherlands most active country – Semiocast

http://semiocast.com/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_superseds_Japan

[39] 2 milioni gli utenti Twitter attivi in Italia a fine 2011– Pandemia.info

http://www.pandemia.info/2012/02/01/2-milioni-gli-utenti-twitter-attivi-in-italia-a-fine-2011.html

[40] "Abbiamo attaccato i cybersegugi italiani". Su internet migliaia di documenti riservati – Repubblica.it

http://www.repubblica.it/cronaca/2011/07/25/news/attacco_cnaipic-19587826/index.html

[41] Anonymous, svelata la rete in Italia – Corriere.it

http://www.corriere.it/cronache/11_luglio_05/anonymous-rete-svelata_7e9dffee-a6c6-11e0-bbaad83a3b6f7958.shtml

[42] Anonymous, i giorni del DDoS italiano – Punto Informatico

http://punto-informatico.it/3102805_2/PI/News/anonymous-giorni-del-ddos-italiano.aspx

[43] The Recent RA Compromise – Comodo

http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise

[44] Comodo Fraud Incident – Comodo

http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

[45] A message from Comodo Hacker– Pastebin.com http://pastebin.com/74KXCaEZ

[46] 50 Days of Lulz– Pastebin.com

http://pastebin.com/1znEGmHa

[47] Dox everywhere: LulzSec under attack from hackers, law enforcement – Arstechnica.com

http://arstechnica.com/security/news/2011/06/dox-everywhere-lulzsec-under-attack-from-hackers-lawenforcement.ars

[48] Attacco hacker ai siti governativi. "Anonymous" rivendica l'azione – Repubblica.it

http://www.repubblica.it/politica/2011/06/21/news/attacco_hacker_ai_siti_governativi_anonymous_rivendica_l_azione-18022991/index.html

[49] Anonymous attacca Agcom. "Minacciata la Rete libera"– Repubblica.it

http://www.repubblica.it/tecnologia/2011/06/28/news/anonymus_agcom-18348847/index.html

[50] Gravissimo attacco hacker alle università italiane– Repubblica.it

http://www.repubblica.it/tecnologia/2011/07/06/news/hacker_di_nuovo_all_attaco_stavolta_delle_univesit_italiane-18761507/

[51] Anonymous attacca il sito dei cyber agenti – Corriere.it

http://www.corriere.it/cronache/11_luglio_25/attacco-anonymous-polizia_90f08330-b6b9-11e0-b3db-8b396944e2a2.shtml

[52] Antisec hacks another Defense Contractor – Hackmageddon.com

http://hackmageddon.com/2011/08/16/antisec-hacks-another-defense-contractor/

[53] Anonymous attacca la Vitrociset. "Non meritate i soldi pubblici"– Repubblica.it

http://www.repubblica.it/cronaca/2011/08/01/news/anonymous_attacca_la_vitrociset_non_meritate_i_soldi_pubblici-19879883/index.html

[54] Hacker contro la polizia. Colpito il sito del Sappe – Repubblica.it

http://www.repubblica.it/cronaca/2011/08/06/news/hacker_contro_la_polizia_colpito_il_sito_del_sappe-20122634/index.html

[55] Attacco hacker, il Comune accusa il Pat – Corriere.it

http://milano.corriere.it/milano/notizie/cronaca/11_agosto_25/20110825MIL03_13-1901359693338.shtml

[56] opMegaupload, ACTA SOPA web @ war… Major Tango down websites list (updated 1-02-12)– CyberLaw.info

http://cylaw.info/?p=72

[57] EU data protection law proposals include large fines – BBC News

http://www.bbc.co.uk/news/technology-16722229

[58] Mobile Internet devices will outnumber humans this year, Cisco predicts – Arstechnica.com

http://arstechnica.com/business/news/2012/02/mobile-internet-devices-will-outnumber-humans-thisyear-cisco-predicts.ars

[59] Il caos alle Poste? Tutta colpa della nuvola – Wired.it

http://daily.wired.it/news/tech/2011/06/08/caos-sistemi-poste-italiane.html

[60] Aruba, nuovo crash e gli utenti si infuriano in rete – Corriere.it

http://corrierefiorentino.corriere.it/firenze/notizie/cronaca/2011/8-luglio-2011/aruba-nuovo-crashutenti-si-infuriano-rete-1901048893939.shtml

[61] Poste in tilt, tra guasti, code e proteste. C'è chi chiama il 113 simulando una rapina – Repubblica.ithttp://palermo.repubblica.it/cronaca/2011/06/07/news/poste_in_tilt_tra_guasti_code_e_proteste_c_chi_chiama_il_113_simulando_una_rapina-17319998/index.html

[62] Open Letter to RSA Customers – RSA

http://www.rsa.com/node.aspx?id=3872

[63] Open Letter to RSA SecurID Customers – RSA

http://www.rsa.com/node.aspx?id=3891

[64] ecurID breach cost RSA $66m– The Register

http://www.theregister.co.uk/2011/07/27/rsa_security_breach/

[65] EMC’s RSA Security Breach May Cost Bank Customers $100 Million – Bloomberg

http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html

[66] Senator monitoring developments on SecurID safety – Reuters

http://www.reuters.com/article/2011/05/31/usa-defense-hackers-idUSN3110255620110531

[67] Who Else Was Hit by the RSA Attackers? – Krebs on Security

http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/

[68] Safer Internet Day: la protezione online di base non è sufficiente, lo rivela l’Indice di sicurezza di Microsoft. – Microsoft

http://www.microsoft.com/italy/newscenter/Default2.aspx?id=541&pars={Parola+Chiave}{2012%7c2}{}{}{}

[69] Ransomware Exploits the Italian Police – TotalDefense.com

http://totaldefense.com/blogs/security-advisor/2011/12/19/ransomware-exploits-the-italian-police.aspx

[70] The Socialbot Network: When Bots Socialize for Fame and Money – Yazan Boshmaf, Ildar Muslukhov,

Konstantin Beznosov, Matei Ripeanu - University of British Columbia

http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1

[71] Phishing on Mobile Devices – Adrienne Porter Felt, David Wagner - University of California, Berkeley

http://w2spconf.com/2011/papers/felt-mobilephishing.pdf

[72] Operazione 'Fabulinus'. Quando l'orco viaggia sul web – Rai.it

http://www.televideo.rai.it/televideo/pub/articolo.jsp?id=11340

[73] Pedoporno, retata europea – Punto Informatico

http://punto-informatico.it/3111559/PI/News/pedoporno-retata-europea.aspx

[74] Pedoporno, nuova retata europea – Punto Informatico

http://punto-informatico.it/3370257/PI/Brevi/pedoporno-nuova-retata-europea.aspx

[75] Cybercrime Report 2011 – Symantec

http://www.symantec.com/content/it/it/home_homeoffice/html/cybercrimereport/

[76] Cybercrime costs the UK £27bn a year – ZDNet.co.uk

http://www.zdnet.co.uk/news/security-threats/2011/02/17/cybercrime-costs-the-uk-27bn-a-year-40091851/

[77] Cloud-Based Crypto-Cracking Tool To Be Unleashed At Black Hat DC – Darkreading.com

http://www.darkreading.com/authentication/167901072/security/encryption/229000423/cloud-basedcrypto-cracking-tool-to-be-unleashed-at-black-hat-dc.html

[78] Potash hackers a wake-up call for lawyers – The Globe and Mail

http://www.theglobeandmail.com/report-on-business/small-business/sb-growth/day-to-day/potashhackers-a-wake-up-call-for-lawyers/article2261700/print/

[79] Cyber-Weapons – The Rusi Journal

http://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf

[80] Information Security Business Opportunity – Appin Security Group

http://www.franchise.appinonline.com/security-market-size.html

[81] Science and Engineering Indicators 2010 – National Science Board

http://www.nsf.gov/statistics/seind10/c6/c6h.htm

[82] Project Enlightenment: a modern cyber eapionage case study –Cybersquared.com

http://www.cybersquared.com/project-enlightenment-a-modern-cyber-espionage-case-study/

[83] La leggenda dei jackpot che hanno sbancato la Snai – La Stampa.it

http://www3.lastampa.it/cronache/sezioni/articolo/lstp/450787/

The Italian Postal and Communications Police against Cybercrime

In this undisclosed contribution, the Postal and Communications Police of Italy describes the crimes it has to face and offers quantitative and qualitative data yet to be released on investigations and their outcomes in 2011.

Postal and Communications Police

In these last years, the technology evolution made the Internet the essential medium to exchange information, to access to big databases, for financial transactions and dispositions and to define new professional activities. Nevertheless, the fast spread of Internet usage underlines the weakest links of the net, in particular regarding information security.

In this scenario with the reform law of the Public Security Administration the Postal and Communications Police was born as a “Speciality” of the State Police of Italy in the forefront for the prevention and contrast of information criminality and willing to guarantee the constitutional values of secret correspondence and of every form of communication.

The main task of the Postal and Communications Police is to find most adequate control edges to the new technological frontiers used by criminals. Activities against criminals are the main tasks, more specifically:

- online pedopornography. Along with the National Contrast Centre against online Pedopornography (CNCPO, *Centro Nazionale per il contrasto alla Pedopornografia On line*), the Postal and Communications Police gathers notifications and coordinate inquiries on the spread of images of sexual abuse against children on the net and via other means of communication.
- Protection of the Italian critical facilities. These are those companies and bodies that support and guarantee the functioning of the country through information systems. They are monitored and protected from information attacks by a team of specialised investigators part of the National Centre against IT Crime and for the Critical Facilities Protection (CNAIPIC, *Centro Nazionale Anticrimine Informatico e per la Protezione delle Infrastrutture Critiche.*)
- E-banking. The new frontiers of commerce and money circulation on the Internet require investigations focus on monitoring the technology and study the related criminal phenomena. The aim is to react quickly in case of aggressions to the online transaction systems and e-banking in general.
- Copyright. File sharing services and other similar online services for the circulation of creative works strengthened the illegal spread of files and moved on copyright a constant attention.
- Hacking. Every Internet user that want to damage or hit on the net target related with the Internet itself are controlled by investigators.
- Cyber terrorism. A skilled team of investigators are always busy monitoring the net and bringing forward specialist inquiries on the more and more common use of new communication technologies by enemy groups and national and international subversives.
- Online games and gambling. By monitoring the Internet and dedicated sites, many activities not authorised by the Ministry of Finance – Independent Administration of State Monopolies have been found.
- Crime analysis of emerging phenomena. Investigators and psychologists work together to analyse and process data on the new frontiers of cybercrime. They mix their knowledge in order to carry forward effective preventive and repressive actions against information

crimes.

The service of Communications Police

The service of Communications Police, part of the Central Direction for the Specialities of the Public Security Department, was instituted after a Ministerial decree on March 31st 1998.

As an organism of the Ministry of Internal Affairs for the security and regularity of telecommunication services, the Communications Police is the benchmark for the coordination and project activities and for the operative planning of those activities led by the local offices of the Specialities, the Sections. is made up of three national centres: the CNCPO, the CNAIPC and the Virtual Police station.

In addition, since the Communications Police absorbs the important information on cybercrime, it has to:

- analyse the sphere of application of the laws in the field of communications;
- analyse under the crime perspective the criminal phenomenon connected to hi-tech tool, the high tech crime;
- detect contrast strategies to criminal phenomena that stem from the data transmission systems and computerised data process;
- participate in workshops organised by national and international bodies;
- select and educate Communications Police future personnel, in cooperation with Universities and telecommunication operators;
- cooperate with foreign police.

The sections

The Postal and Communications Police has 20 sections carefully distributed throughout Italy. The sections are structures organised on a regional basis and they work on different enquiries on cybercrime, keeping contacts with the main offices that focus in the field.

By knowing the territory they have to work in, the sections represent an added value and cluster the most important feature for an effective investigation.

The online station of the State Police.

The use of the Internet increased and the security expectations of the citizens along with it. For this reason the State Police, first in its kind in Europe, created an online police office, the Virtual Police station on www.commissariatodips.it

The "*Commissariato di P.S. on line*" (online State Police station) is the benchmark for who seeks information, suggestions, advice or wants to download forms or to lodge a complaint online.

Its main activities are:

- information. On the portal, in-depth sections on administrative procedures can be consulted and they give hints on, for instance, passport release, immigration practices, sections for youth, licences and competitions;
- prevention. There are sections where people can ask any information on the use of the Internet, suspected websites notifications;

- online complaints for thefts, losses and information crimes.

During the first five years we received more than 2,728,900 visits and a community of 120,000 subscriptions. The “Commissariato di P.S. on line” project was awarded with the “Most Inspiring Good Practice” prize at the European e-Government Awards 2007, organised by the European Commission as a token of innovation, effectiveness of the initiative.

The portal of the “Commissariato di P.S. on line” is currently under reconstruction to implement the services already available and to create new ones for the new use of the net, regarding social networks in particular.

The importance and the dimension of the service provided are certified by data on the portal activity, the analysis of these data give an overview of the criminal tendencies of the net.

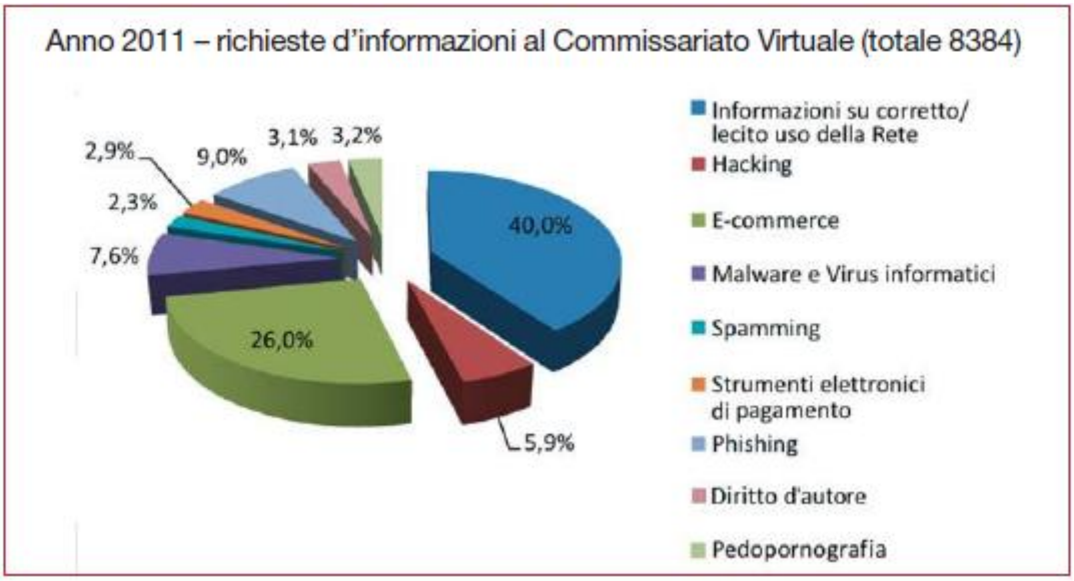


Figure 2: YEAR 2011- request of information to the Virtual Police station (total amount 8384)

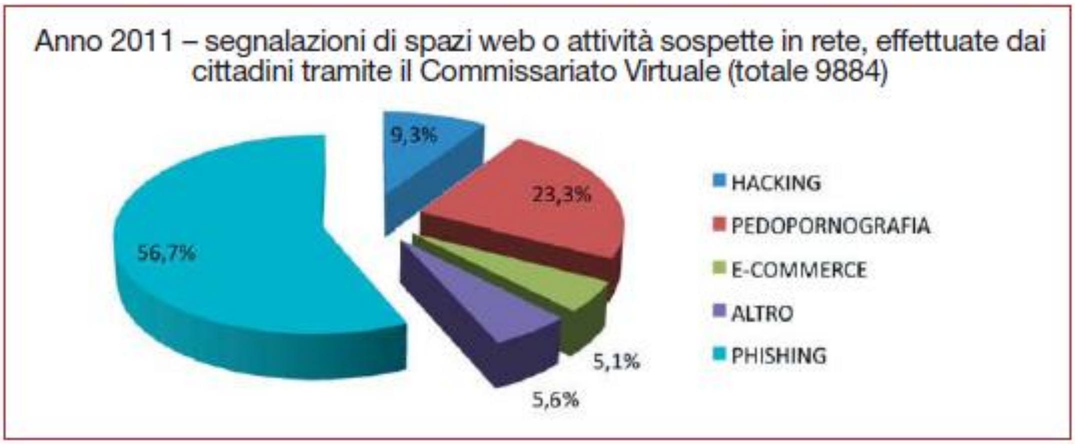


Figure 3: YEAR 2011- web spaces or suspected online activities notifications made by citizens via the Virtual Police station (total amount 9884)

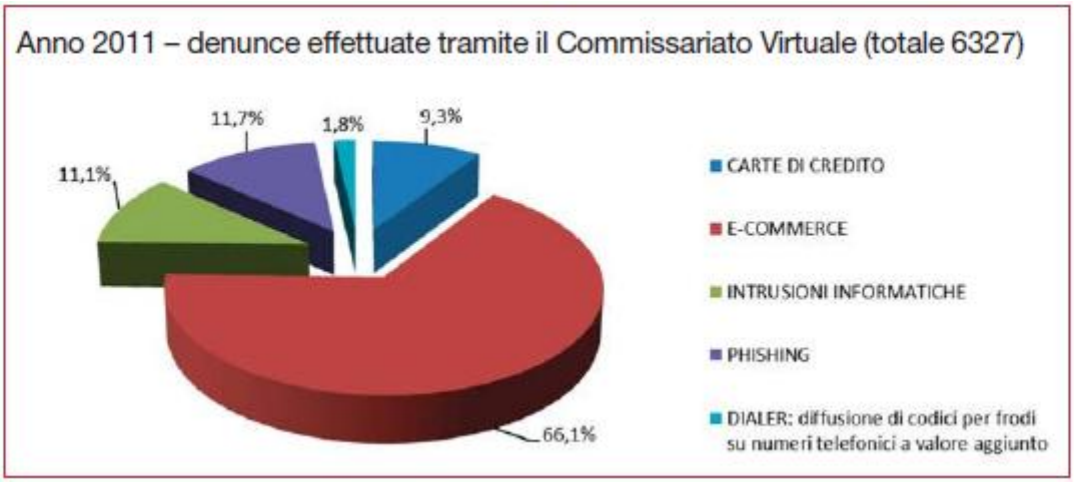


Figure 4: YEAR 2011- complaints via the Virtual Police station (total amount 6327)

C.N.C.P.O.

National Contrast Centre against online Pedopornography

All the inquiries on pedopornography online and the initiatives related to prevention and the management of information sources in the field are coordinated by the *Centro Nazionale per il contrasto alla Pedopornografia On line* – CNCPO, established with the law n° 38 of February 6th 2006 within the Postal and Communications Police Service.

The same law entrusts CNCPO the task to monitor the web thoroughly in order to find websites with pedopornographic contents. Its objective is to implement a black list to be transmitted to the Internet service providers so that they can apply filters and interrupt the fruition of the contents.

The CNCPO also works to disrupt the international "market" of pedopornographic material. In the reconstruction of financial flows it profits from the cooperation of banks, credit enterprises and the institutional coordination of the Bank of Italy.

The Centre works in connection with the Observatory for the contrast of Paedophilia created at the Department for the Policies for the Family as it is also active in the fight against online paedophilia.

A team of psychologists and criminologists from the State Police works in the Centre and analyses the data obtained from the contrast activities with advanced programs of data collection and analysis.

The activities of the CNCPO make use of the confrontation and cooperation of the all players, both institutional or not, that deal with the upbringing and the protection of minors.

During the last year the investigations focused on the identification of victims of sexual abuse who appeared in the materials discovered: it is a very intense activity that requires a historic and geographic reconstruction of the abuse, which often begins from few significant details, faces or backgrounds. The last three months effort has saved 15 children aged from 3 to 17.

The commitment of the Centre materialises through education and awareness raising activities set up with public and private non-profit bodies in the field.

Among the many initiatives, the D.I.C.A.M. project is worth mentioning. Financially supported by the European Commission, it is led by Save the Children Italy in partnership with C.I.S.M.A.I. (Italian Coordination of Services against Childhood Abuse) and the Service Postal Police and it aims at the examination of inquiry procedure and the treatment of pedopornography victims through meetings that will take place in the main cities of the Italian regions in the following two years.

The results of the project are going to be summarised in an operative manual of best practices that may inform professionals of the process that both child and family have to go through after sexual abuse. Another fruitful commitment is 24/7 web monitoring; the web monitoring is coordinated by the CNCPO and had virtual spaces closed where short films or images of minor sexual abuse were exchanged.

In 2011, the synergic cooperation with foreign Police and the reactive ability to contact administrators that unwarily hosted illegal material helped to shut down 237 pedopornographic websites.

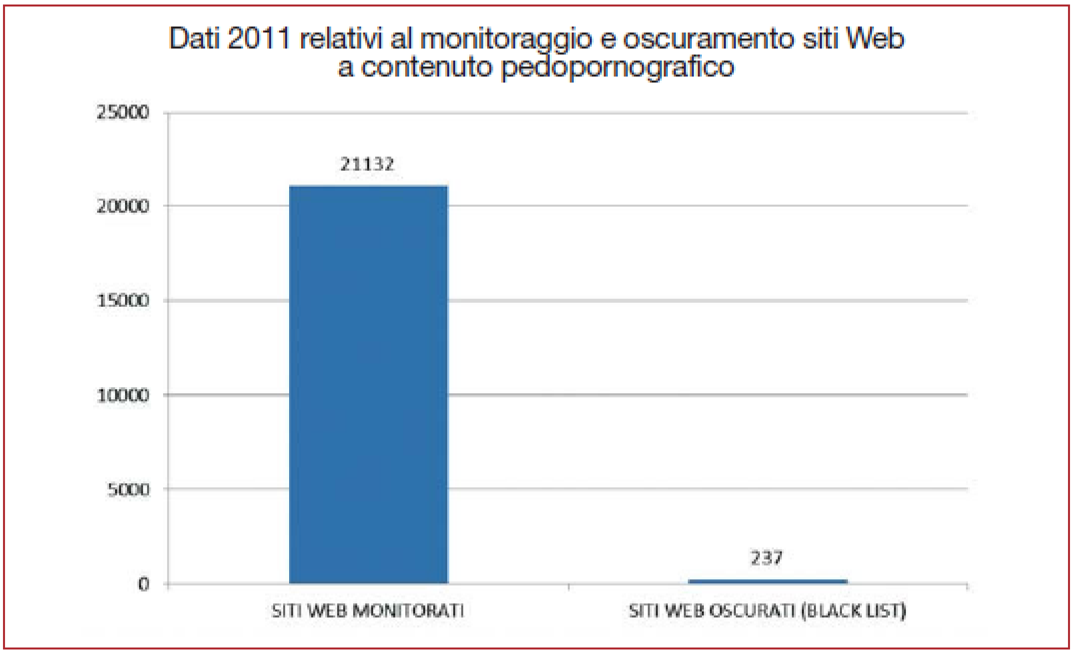


Figure 5: 2011 data on pedopornographic websites monitoring and blackout

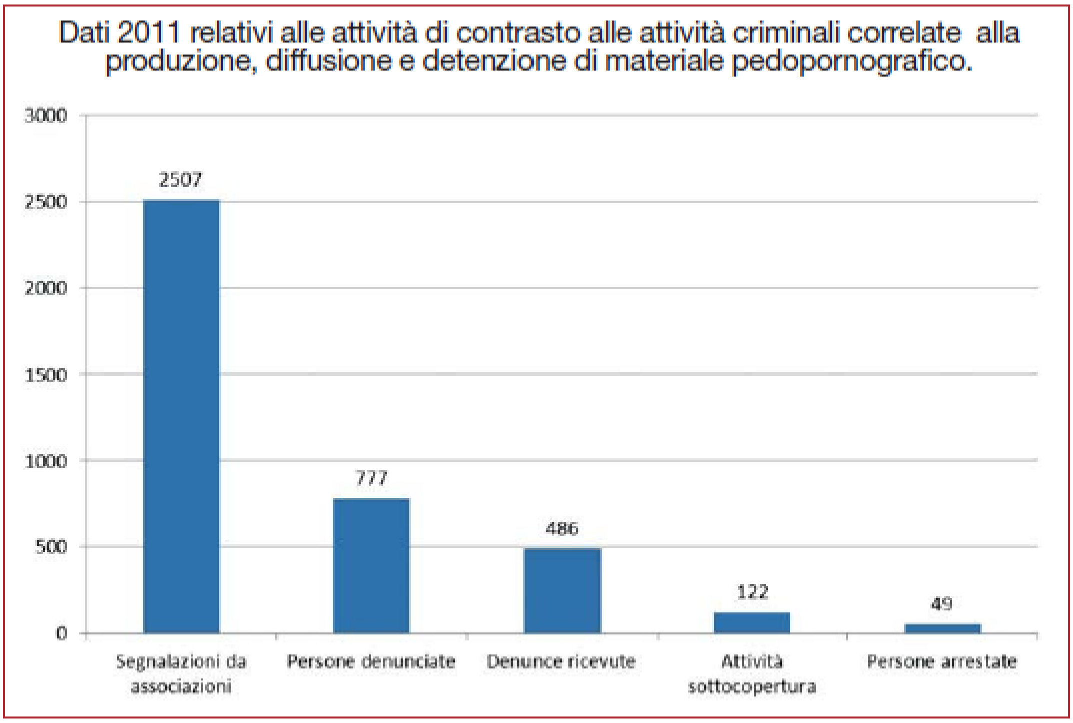


Figure 6: 2011 data on contrast activities to crimes related to the production, spread and detention of pedopornographic material

Contrast to e-commerce infringements

Year after year, the purchase of goods and services online registers a constant growth both in terms of sales proceeds and number of operations, but the growth of e-commerce is associated with the growth of related criminality.

Advertising goods and businesses and e-commerce on the net are a chance for many enterprises to develop, beyond the fact that it is very comfortable for users, but the proliferation of opportunities increases the risks of fraud. A list of some of the main frauds includes:

- fake auctions on the web with reduced prices on goods offered to the customers but never delivered;
- generic goods sale on an online catalogue, where the goods are not delivered to the customer, or they are different from the advertised material;
- offers of free services, which later turn out not to be free, non-delivery of services the customer paid for, or supply of other services than those advertised;
- hardware or software sale on an online catalogue, but the delivered goods differed from the advertised;
- pyramid investment schemes and multilevel business;
- in-house job offers with the upfront purchase of the material needed to work;
- loans with upfront commission required – the money will not be lent;
- fake services offering the removal of negative information, often bordering on extortion (i.e. removal of a name from a blacklist, real or imagined);
- fake promises of credit card concession – with an upfront commission – to people with bad credit records;
- expensive phone numbers to be dialled in order to discover the identity of a secret admirer or to collect a secret prize or a lottery win.

In most cases, the swindle starts with an e-mail sent to the potential victim. In case of doubt, the e-mail should be saved and the Communications Police immediately contacted.

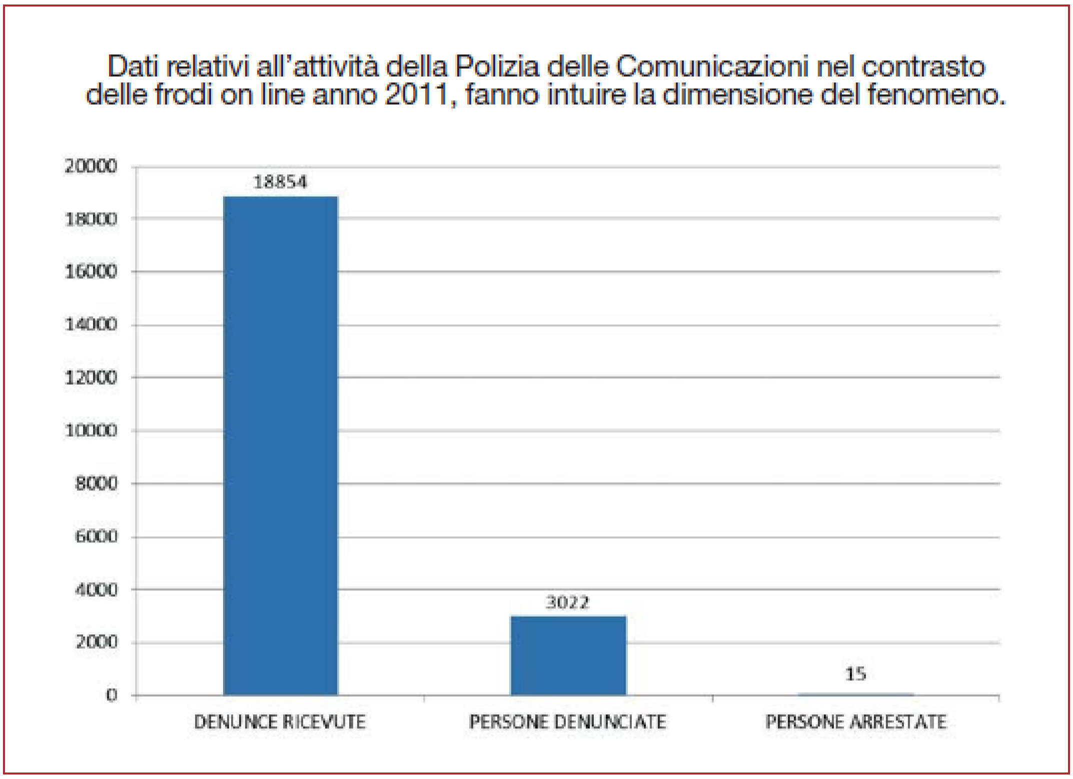


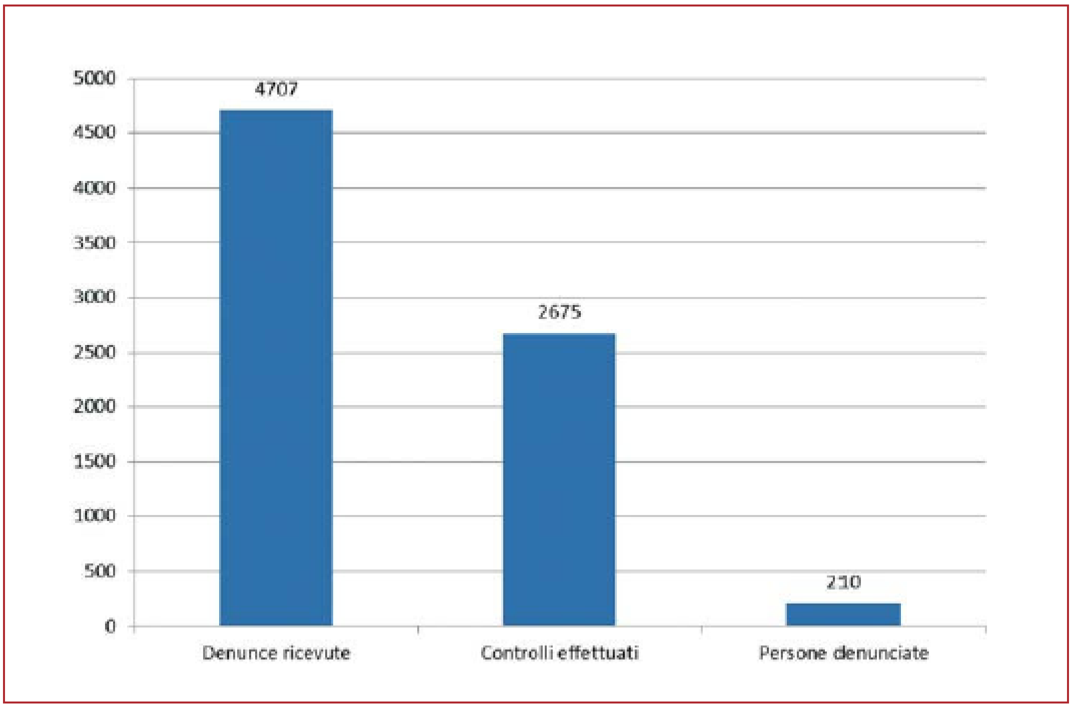
Figure 7: Data on Communications Police activity against online frauds in 2011, they show the dimension of the phenomenon

Digital identity theft

In the era of the information society, personal data have to be considered an important part of everyone's heritage, databases therefore represent “wealth” and have commercial value, and thus are a target of aggression by criminals.

Personal data theft, and identity theft in general, is now the most important crime on the net for its numbers and for the sign it gives if compared to the other information crimes.

An identity theft is defined as any time personal data useful to commit more crimes is gathered in a illegal manner. The data collection itself entails crimes such as unauthorised access to information systems, information fraud, spread of programs aiming at damaging or interrupting an information system. (artt. 615 ter and quintes, 640 ter cp)



Counteracting online economic and financial crime and electronic means of payment

The new frontiers of information allows us to extend to the virtual world that which was previously characteristic of the real world. Online payments transactions or virtual credit instruments are nowadays embedded within the information society and are widely used by the population. But the application of computer science to payment systems has become a new and profitable frontier for organised criminality. Postal and Communications Police counteract the illegal exploitation of these tools and lead a fight against those organisations, to generate security and aware use of payment systems and electronic credit.

Credit cards and electronic means of transport cloning

Data on the activities set to counteract organised criminality's daily attacks on payment tools such as the sophisticated cloning activities of credit cards and cash cards.

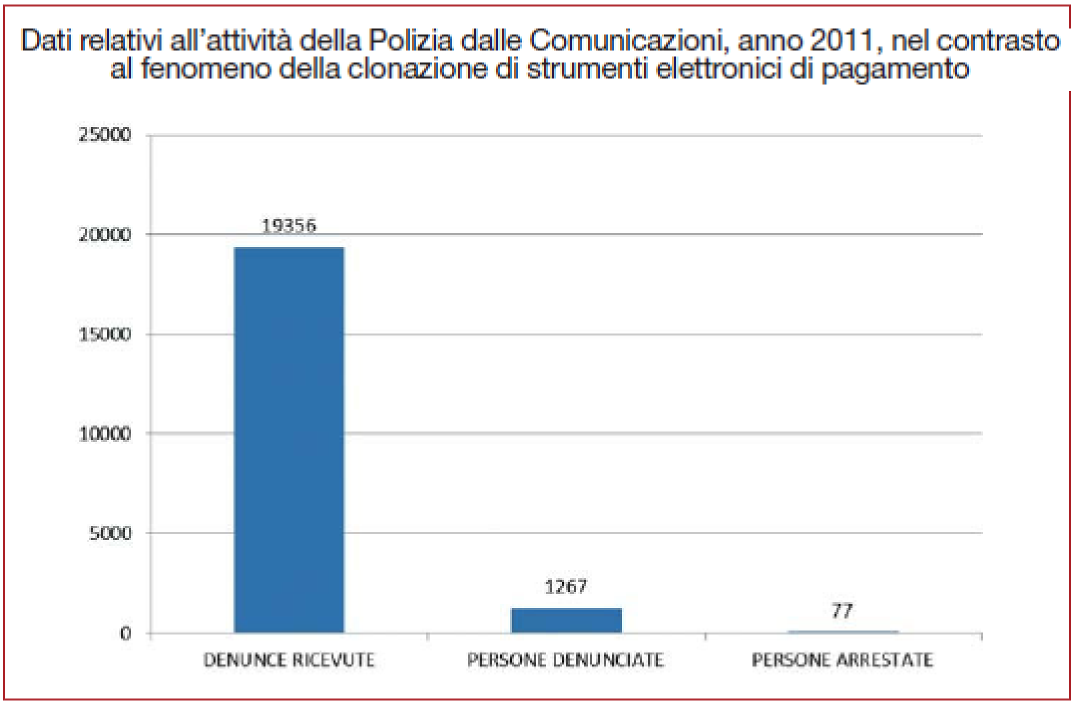


Figure 8: 2011 data on Communications Police activity against the cloning of electronic means of payment

Home banking information frauds

The expanded use of the Internet in the individual's financial planning entailed the need of countermeasures to prevent attacks to databases and to entire banking systems.

The appeal of digital data as a replacement of coins and banknotes is a fact that can be confirmed by the statistics of the activity to fight cybercrime, which is moving towards the deceitful exploitation of home banking.

The size of the phenomenon and the international nature of online banking criminality display a systemic dimension of the attacks and, considering the importance of online transactions, it can slow the economic development of a country or even undermine it.

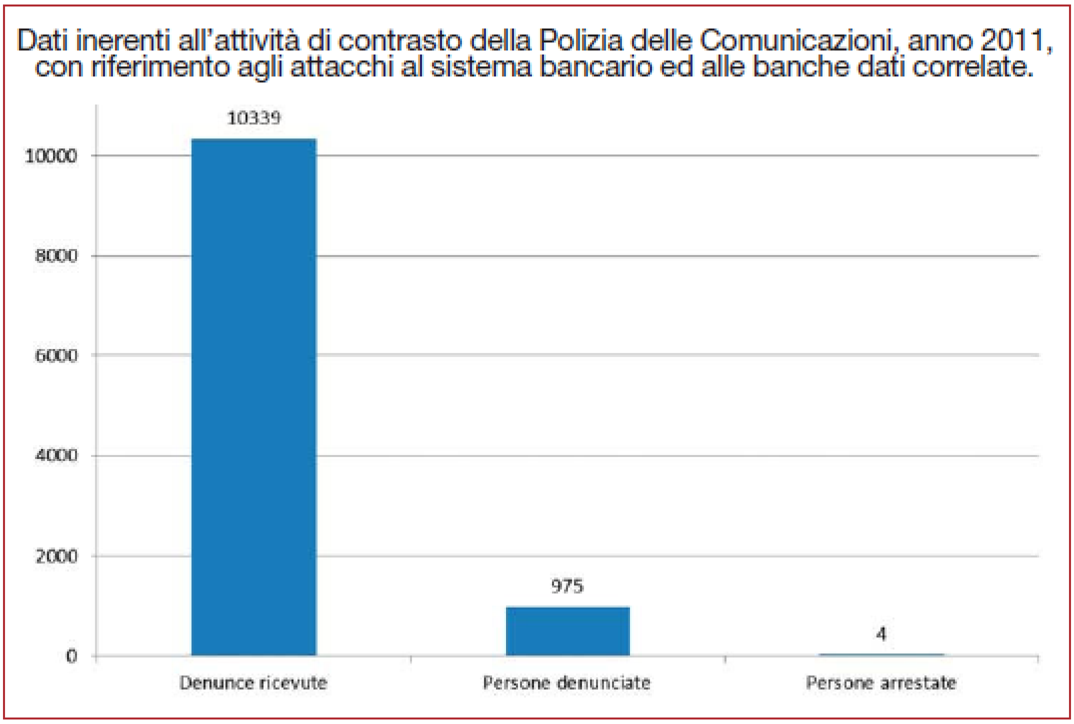


Figure 9: 2011 data on Communications Police activity against banks and databases attacks

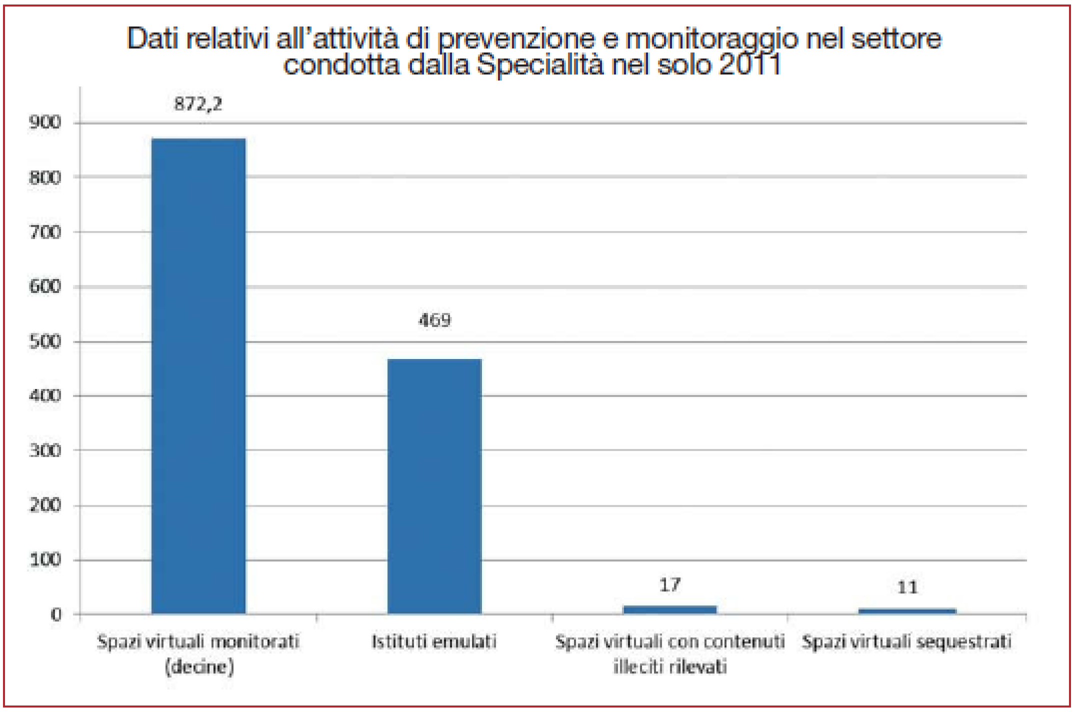


Figure 10: 2011 data on prevention and monitoring activity by the Speciality

Combating phishing

Identities are often stolen through social engineering, which are techniques used to manipulate people until they give confidential information.

Phishing is one of these techniques of obtaining personal information that automatizes these processes. It is often committed by copying websites that are authorised to possess those information. Personal data are then uploaded on websites that look exactly like the legitimate ones,

but belong to criminal organisations.
The phenomenon is so large that it is the number one increasing crime in the home banking sector.

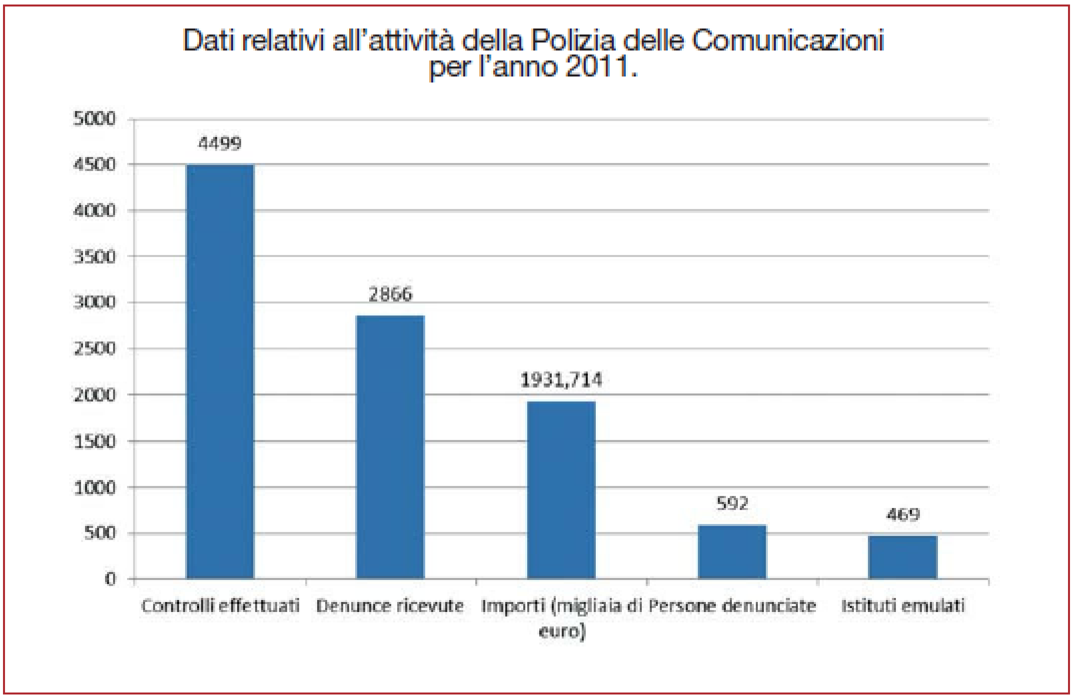
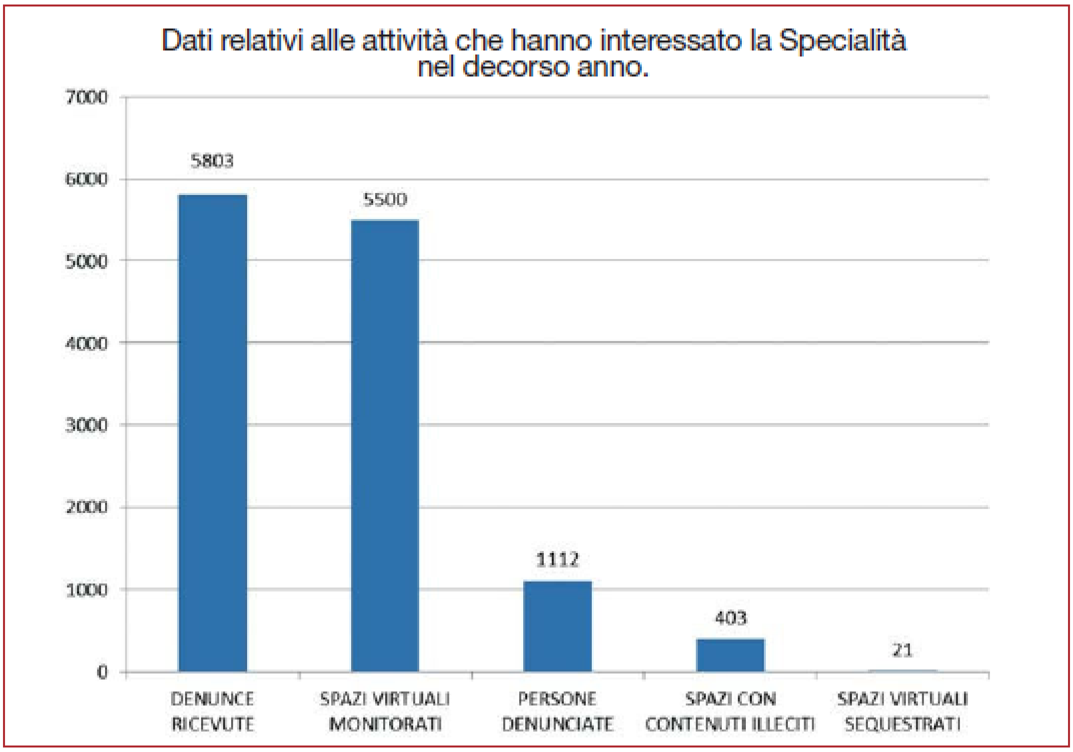


Figure 11:2011 data of the Communications Police activity

Crimes against the person

The many chances to communicate online, especially through social networks, led to the development of a "digital version" of some of the main crimes against the person, such as insults, threats and persecutory acts (cyber-stalking.)
The low self-perception on the net is an incentive to commit those crimes, that often involve youngsters.
The sheer volume of phishing cases is reaching critical mass, which is also related to the importance attached to digital reputation



.

Figure 12:2011 data on the Specialty activity

Protection of computerised critical facilities

Nowadays the cyber threat is analysed through many points of view and with more dedication and different strategic perspectives. It is qualified under the spheres that are hit during a criminal attack: cybercrime, cyber terrorism, cyber-espionage, cyber war. The Postal and Communications Police faces this threat with a global approach in mind, with the final objective being the safety of citizens, institutions, companies, and computerised facilities that use the net to communicate and to manage different services. The Postal and Communication Police is particularly busy with the prevention and the mitigation of information attacks on a large scale or to single but nationally important enterprises. In this way, data and information that make up the Public Administration and Italian industrial know-how are kept safe, together with the proper functioning of the services provided or controlled on the Internet, for the benefit of the society, public bodies and enterprises.

The National Centre against Information Crime and for the Critical Facilities Protection

The National Centre against Information Crime and for the Critical Facilities Protection – C.N.A.I.P.C. was founded with a decree law by the Ministry of Internal Affairs on January 9th 2008 to actuate the art. 7 bis law n° 155 of July 31st 2005 that entrusts the Service of the Postal and Communications Police (as the central Ministry of Internal Affairs organism for the security and regularity of services and telecommunications) to be exclusively competent to supply information protection services to the computerised critical facilities of national interest (I.C.) The same decree established as I.C. the information systems and services that support institutions, Public Administration, private or public corporations and businesses working in the following fields: international relations, security, justice, defence, finance, communication, transport, energy, environment, health and water. These areas are considered to be of interest to the Ministry, also proposed by the prefects (*prefetti* – regional public safety authorities), for public order and safety. Information protection is guaranteed through special electronic connections between C.N.A.I.P.C.

and the I.C. on the basis of agreements set with the Public Safety Department.

C.N.A.I.P.C. tasks

C.N.A.I.P.C. is part of the Postal and Communications Police and can use its advanced technologies and high qualified personnel. It is responsible for the prevention and the mitigation of information threats motivated by terrorism or criminality, aiming at the protection of I.C. and it works in the following fields:

- operation room, univocal contact point available 24/7 devoted to the I.C. Information exchange;
- intelligence; gathering of data useful for risk prevention. This task is performed via Internet monitoring and cooperation with other law enforcement agencies, corporations and ICT security businesses, both national and international;
- analysis, examination and comparison of data, provisional reports on information threats and vulnerabilities, techniques and criminal initiatives;
- investigative and operative response when a crime takes place and damages a I.C. The response is conducted through cooperation with the 20 sections, the peripheral part of the Postal and Communications Police and foreign or international police services, like Interpol, Europol, G8 Subgroup on High Tech Crime.

Cybercriminality analysis unit

The unit is composed of three State Police psychologists and seeks to complement conventional cybercrime mitigation techniques with their social and psychological skills.: this combination creates a strong, detailed examination of cybercriminality, which becomes integral to institutional knowledge. Last year, the unit's activity focused primarily on two research-intervention projects:

A – Digital profiling. A detailed analysis of online behaviours, surfing attitudes, chat and social networks conversations between sexual offenders via the net allows the unit to delineate behavioural patterns and tools to evaluate if a situation is dangerous. These tools are tailored to combat Italian online paedophilia. Profiling activities involve a step-by-step confrontation with foreign policies, so that crime related information can be productively shared.

B – Personnel support. Since 2010 a research-intervention project involving around 400 operators, executives and managers from peripheral offices who study and prevent specific stresses in the workplace. Through surveys, individual meetings and publications, the unit studies the effects, possible strategies and procedure to protect people who work against online paedophilia both emotionally and psychologically.

International cooperation

Contacts and information sharing with international institutional interlocutors are fundamental for the Speciality to be effective, as the Internet can be thought as a territorial reality and the entire world can perpetrate crime actions against the entire world.

Therefore it is essential to extend contacts with foreign entities for a productive confrontation of the main issues and for the update of investigative techniques. The Postal and Communication Police service has taken part in the G8 Subgroup on High Tech Crime and to the Information and Communications Police Committee (I.C.C.P.) of the Organisation for the Economic Cooperation and Development (OECD) and it takes part in their political and administrative panels.

The service offered by the Postal and Communication Police is an international contact reference for information emergencies within the G8 networks and in the Council of Europe working 24/7.

To fulfil its task against online pedopornography, the Communications Police service participates in the Electronic Crime Task Force (ECTF) and European Financial Coalition (EFC) meetings and it is part of the police network called Virtual Global Task Force (VGT.) Moreover, it joins in the European Working Party on Information Technology Crime that gather by the Interpol General Secretary in Lyon of the Europol High Tech Crime Committee and European Commission round tables.

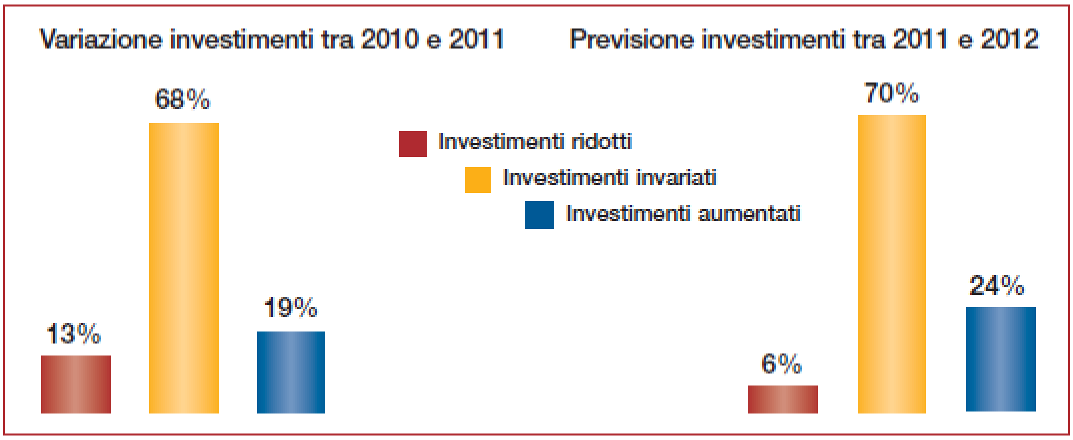
ICT Security Market and Job Market

The perspectives of businesses-users and vendors on the priorities and values in the ICT security are similar and disparate Some of these differences are due to the natural opposing roles they play (supply and demand) Nevertheless, in our opinion, they hide some strategic disagreements that should make anyone (users and vendors) think thoroughly on the evolution and the dynamics of the ICT security sector.

There is one topic where both perspectives coincide, though: that this sector requires and expects more investments.

Investments: will the market start to grow again?

Investments in the ICT security market are expected to see growth of up to 5% in 2012 compared to 2011. This percentage is what emerged from a survey of enterprises that were interviewed for our research. The sign is positive because it suggests that, even in such critical period, security is an issue that is taken seriously.



The situation is indeed better than that of past years. Whereas in 2011 the businesses that increased their investments were only 19% of the sample, in 2012 the percentage gains 5 points to 24%. The percentage of businesses that simply to keep their investments stable has also increased, from 68% of 2011 to 70% of 2012. In consequence the percentage of businesses willing to cut their expenses on protection has decreased, from 13 % of 2011 to 6% of 2012.

Vendors against Users

The analysis of the key questions of our research shows that, besides the legitimate distance between buyer and seller, users and vendors have different priorities and visions, even when asking for competence. Their differences are quite glaring when approached with questions such as where the future areas of interests will be, or where investments should be focused.

Different priorities for users and vendors

For vendors there are two emerging priorities: personal device (tablets, smartphones, laptops, desktop PCs) security and cloud computing security. This means that their orientation leans towards the latest technological trends the update of equipment and the reassessment of industrial processes as mobile devices and cloud computing force the companies to reassess their operative methods.

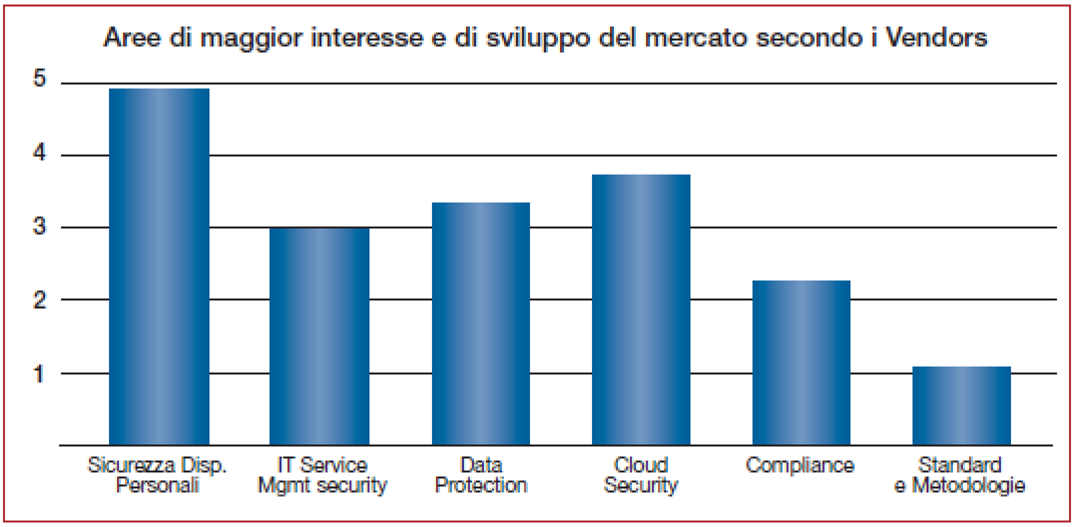


Figure 13: Vendors: most interesting markets and developing areas

Users disagree. Their main concern is that current IT security services are not dealing with today's threats adequately while seeming more interested in tomorrow's opportunities. The difference between “here today” and “tomorrow” is transmitted by users and vendors different view of the cloud.

Vendors place cloud security third, as they favour a projection toward the future that sees the sector developing.

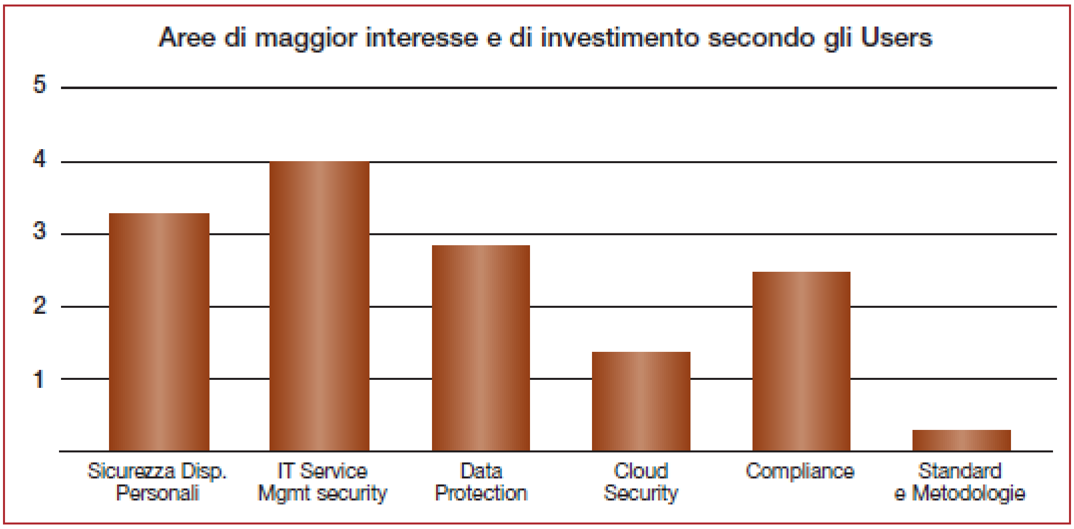


Figure 14:Users: most interesting markets and developing areas

Businesses users place cloud security issue at the bottom of the list, as second last, just before standards and methodologies. This difference is that whereas attention to standards and methodologies has already consolidated and less attractive, cloud is the opposite. Cloud is an option that don't match with many businesses' views probably because it requires a fresh technology and organisational approach, and in such a high tension period as this, it is not included in the top priorities. The interest in security steps aside as one of the issue not considered by the industrial development strategies.

Users and vendors do agree on the two very last topics of interest: data protection and compliance, their visions more or less coincide but the topics still don't represent their top priorities. Compliance was in the past years an area on which they invested and it seems today a goal successfully achieved and an area in which the ordinary maintenance is more important than innovation. No important evolutions are expected in this field, unless the key laws change of course.

Data protection is a slightly different topic. It is often debated as the heart of the matter and it is plain that data protection has to be the centre of IT security managers and vendors attention, but its development is by now routine.

Comparing reliability and economy

Distinct perspectives between vendors and users can be found on the key elements that make them chose the right supplier. Even in this case it is clear that the two parties conceive it differently and this is often due to their specific role. Nevertheless, the difference between vendors and users' insights on it is remarkable.

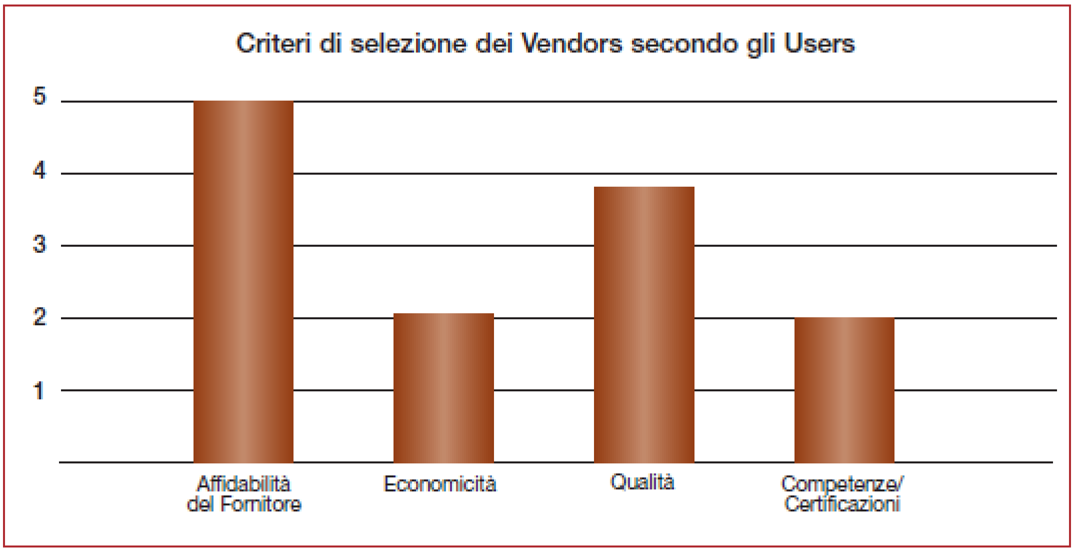


Figure 15: Users: vendors selection criteria

Users believe in reliability and they consider it on top of the vendors selection criteria, and successful and solid vendors that have been active in the market for a long time are often strongly preferred to high quality vendors or to vendors with lower price-points. Users believe that the price of a vendor's proposal should be placed third, at the same level as compliance.

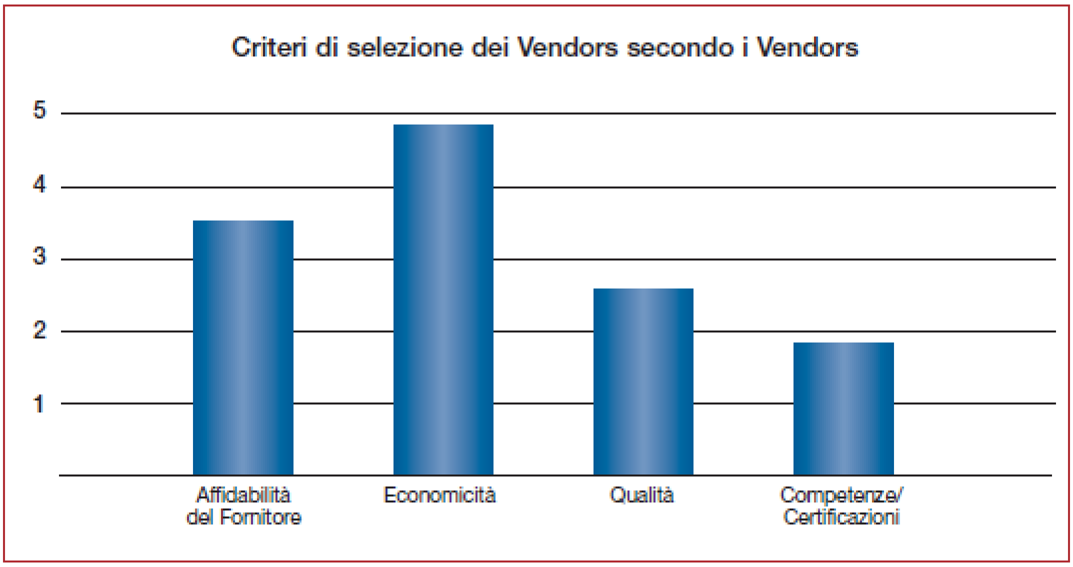


Figure 16: Vendors: vendors selection criteria

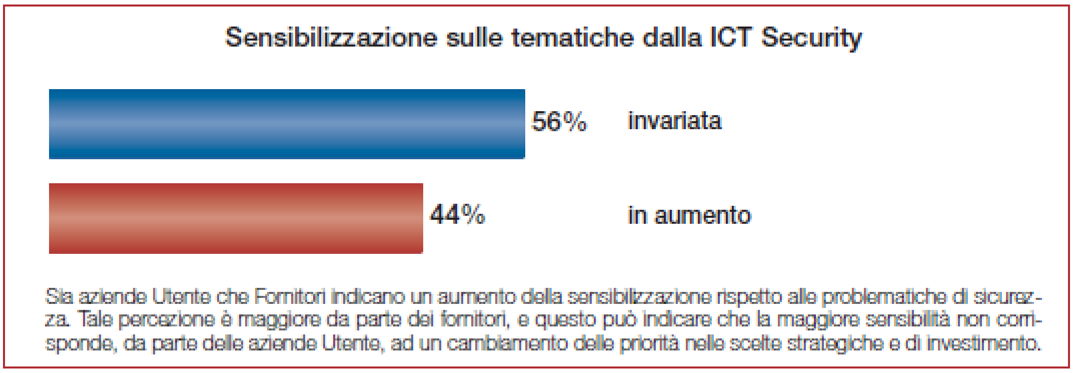
The overview is the opposite on the vendor side as they prefer lower price points. The quality of the offering is a factor that can be neglected since vendors place it third, after reliability. Users look for reliable vendors with high quality proposals, whereas vendors prefer to seek offers with lower prices because this is what their customers ask for and it has to be included in the business proposal.

The last place is clearly occupied by compliance and certification, both perceived as predefined option for the market players and therefore a non-qualifying element.

Is the glass half full or half empty?

Even if vendors and users clearly have different views on many topics, there are some points on which they both agree. The first of all is the general feeling that attention to the issues remain high though stable over the last 12 months. 56% of the interviewed sample say that despite the stream of financial and governmental websites attacks and privacy scandals damaging IT companies, the topic is still undervalued.

Remaining 44% of the interviewees declares that attention toward on topic has increased but we believe that general the level awareness that would imply a strong change in the investments preferences in IT security has yet to be reached.


Sensibilizzazione sulle tematiche dalla ICT Security

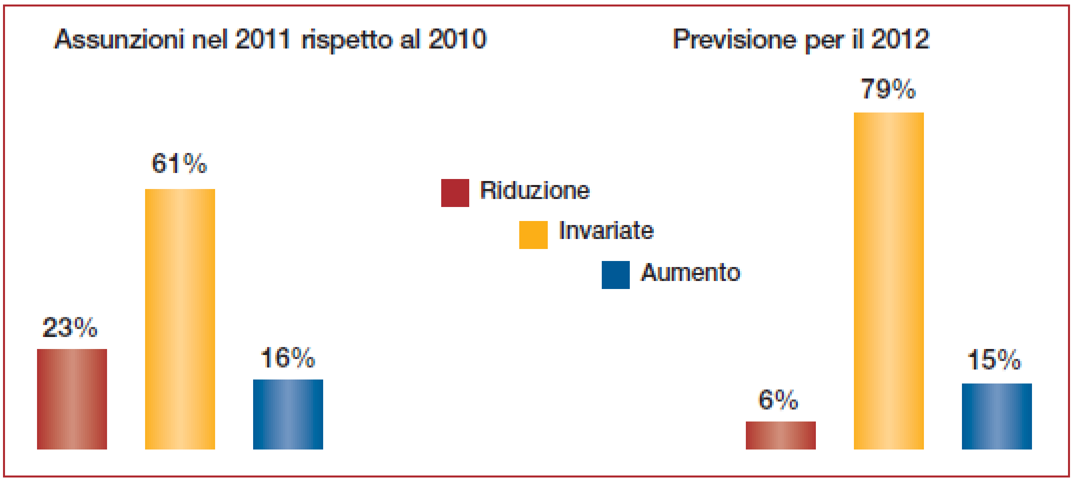
Sia aziende Utente che Fornitori indicano un aumento della sensibilizzazione rispetto alle problematiche di sicurezza. Tale percezione è maggiore da parte dei fornitori, e questo può indicare che la maggiore sensibilità non corrisponde, da parte delle aziende Utente, ad un cambiamento delle priorità nelle scelte strategiche e di investimento.

Figure 17: Awareness on ICT security topics

The number of employees remains stable

The feeling that attention given from businesses to the role of security is still too low is confirmed by research on the number of employees in a company that deals with it. In 2011 vendors and users kept the same number of employees working on security (61%) or sometimes even reduced it (23%), but only a small amount of the interviewees declared to have added more employees (16%.) Considering the economic crisis, 2012 could not be comforting and the situation is stable. 78% of the businesses are not willing to modify the number of its staff, and those who will hire skilled personnel only number 15%. We shall take comfort in the percentage of who will divest in security: 6%.

Hiring in 2011 against 2010 **Forecast for 2012**



Consultants first

Analysts, programmers or developers? Which are most wanted professionals on the market these years? Vendors and users think differently again. Users seek consultants, security auditors, analysts and so on, whereas vendors are more technically oriented and they search for developers, administrators and project managers. Less relevant is the request for management assistants, program managers, or advisors.

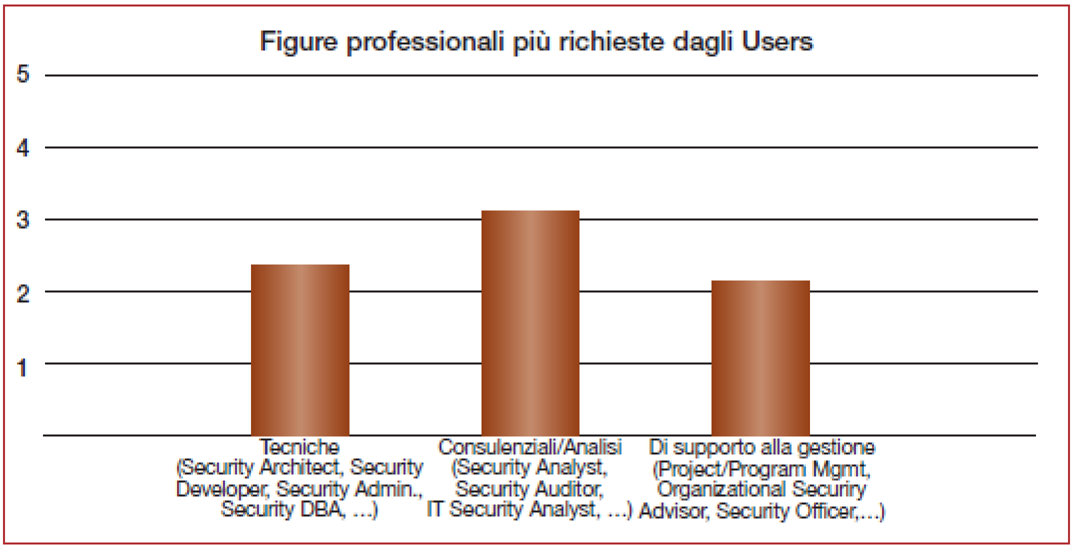


Figure 18: Users: most popular professionals

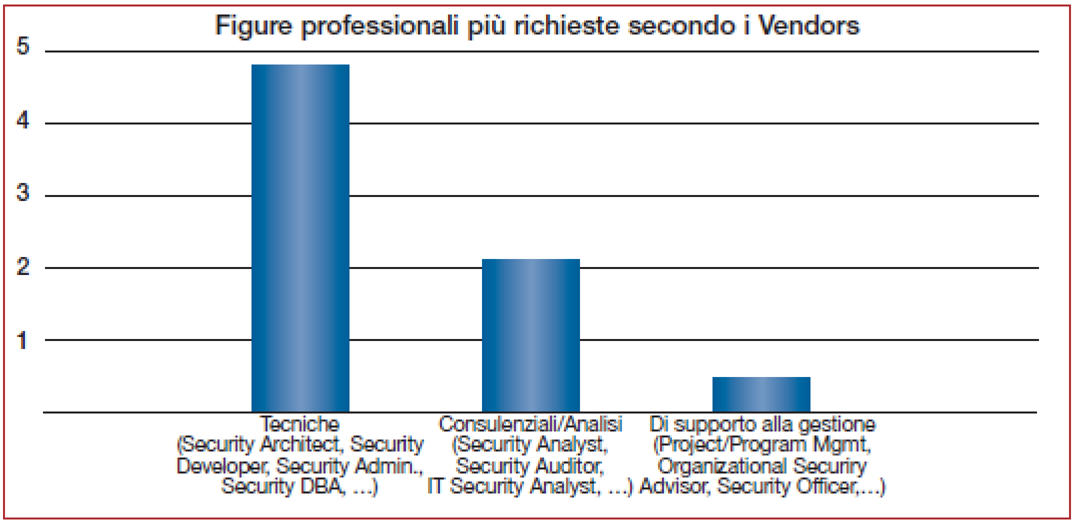


Figure 19: Vendors: most sought after professions

Certification vs. work experience

An interesting piece of data comes from the analysis of the necessary requirements to hire new people. Despite those who believes that work experience is more important than education, users and vendors believe that a certification obtained by neutral organisms is worth 5 years of work experience in the field. However experience is considered the second most important qualification in the resumes.

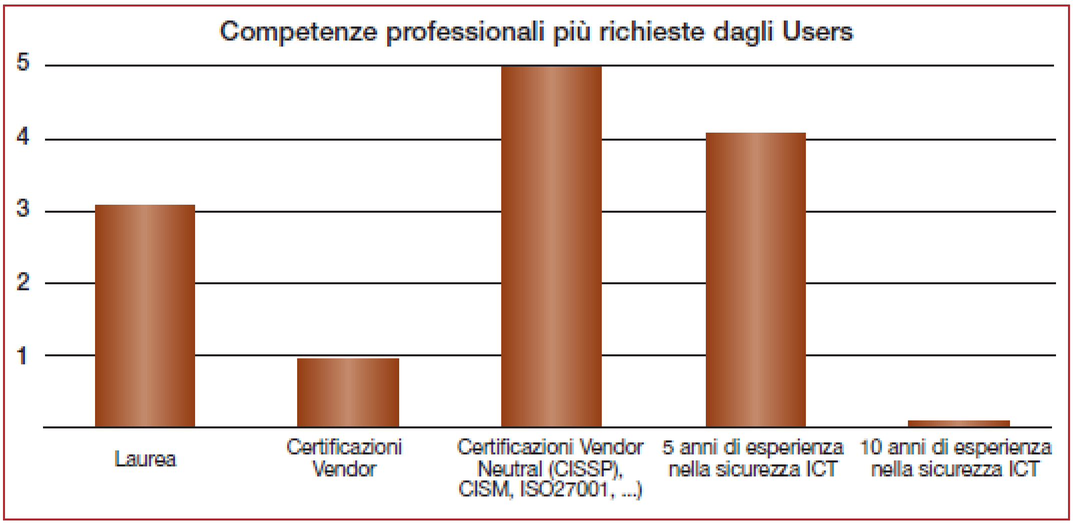


Figure 20: Users: most requested professional competence

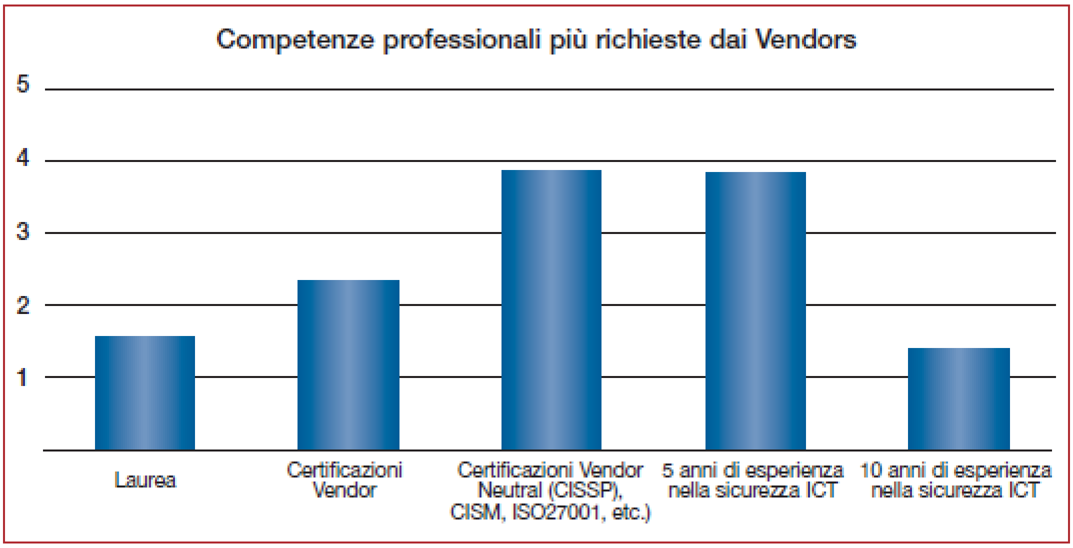


Figure 21: Vendors: most requested professional competence

A Master's degree is more appealing for users than the certifications issued by vendors or even than 10 years of work experience.
On the contrary, vendors prefer a certification issued by other vendors and put a Master's degree and a 10 year work experience on the same level.

Methodological note

The research has been made on a sample of 142 Italian enterprises of any size. 77 of them are vendors and they offer ICT services and products; 65 of them are users and use services and products.

The interviewees have been given a survey with polar questions.

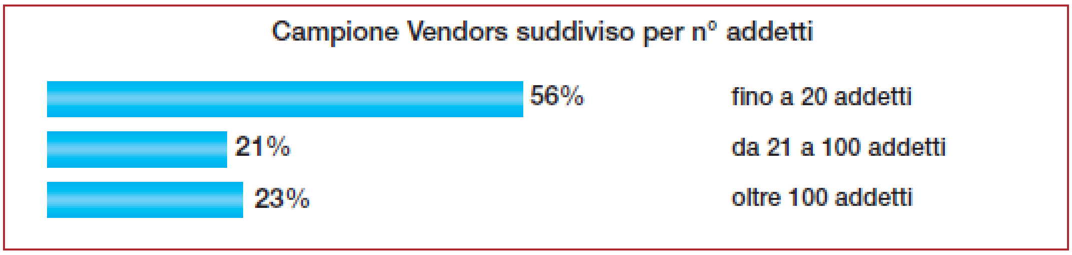


Figure 22: Vendors per n° of employees

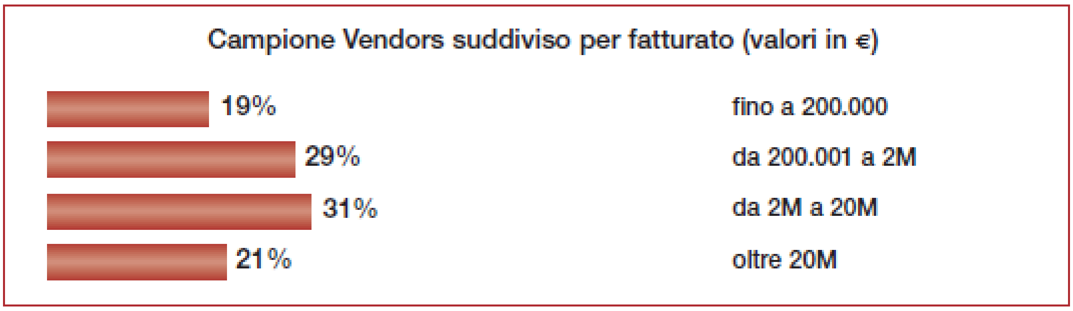


Figure 23: Vendors per turnover (in Euros)

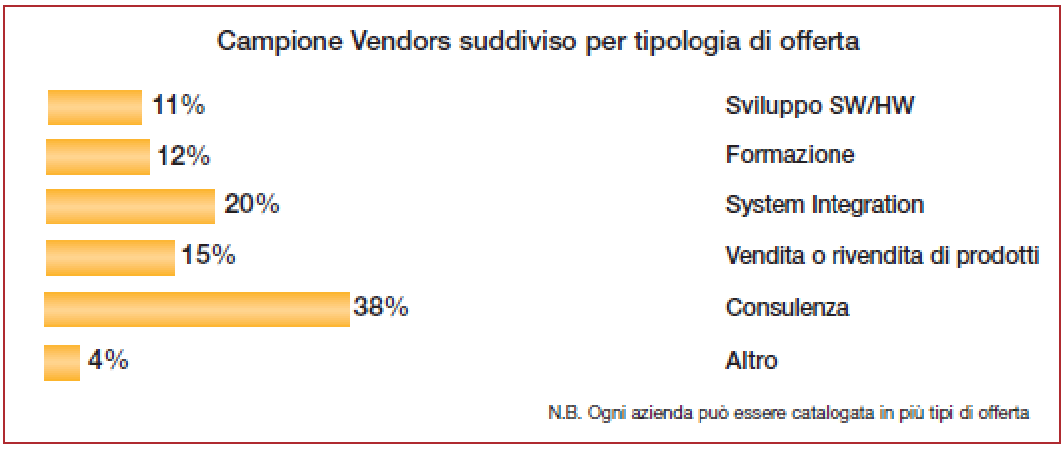


Figure 24: Vendors per offer

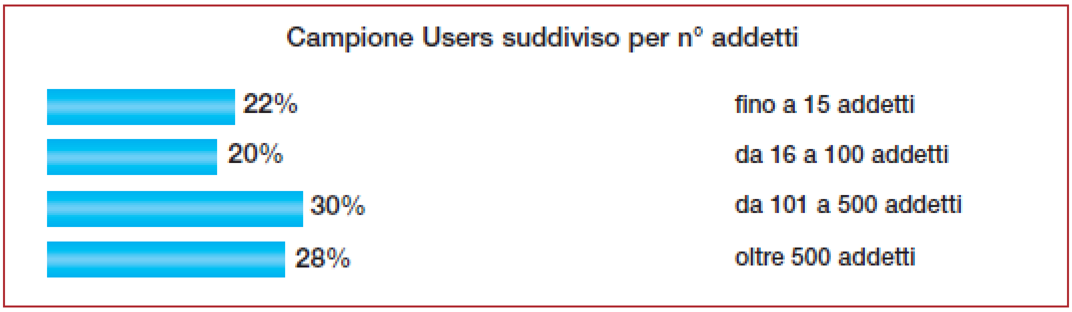


Figure 25: Users per n° of employees

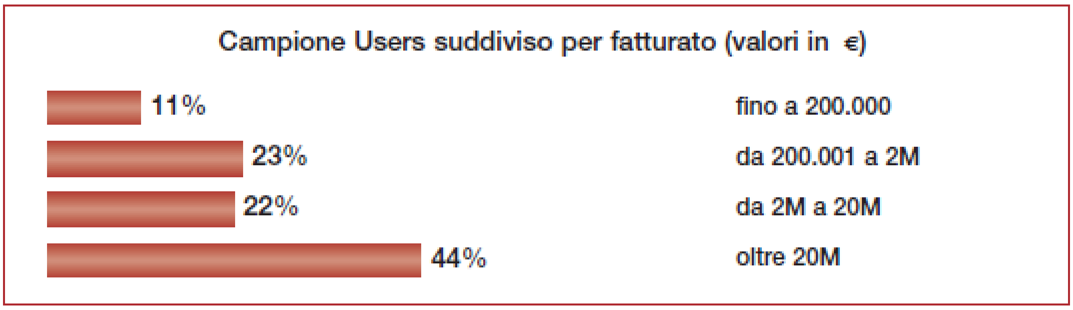


Figure 26: Users per turnover (in Euros)

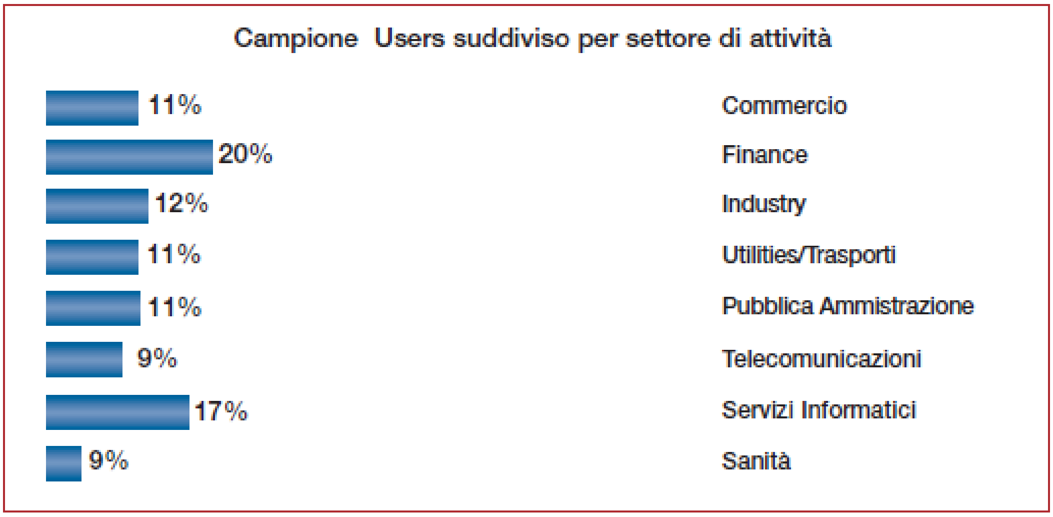


Figure 27: Users per activity

CLUSIT Report 2012 – FOCUS ON

This section of the 2012 Report is devoted to the most important areas for ICT security in Italy.

We have asked to some of the major Italian experts of the individual area to delve into the following topics:

- mobile security;
- social media security;
- cloud security;
- personal data treatment regulations, updates over the last 12 months;
- ICT security situation in the Italian Public Administration;
- Internet and control systems protection in the industry (and in the infrastructures);
- ICT security situation in the Italian small and medium enterprises.

The following "focuses" have many reasons to be considered important: they go side by side with the changes in the way people and business live and work (mobile and social media). They entail possible and significant transformations in how ICT is available (cloud). They touch on particularly Italian situations (SME and PA). They inform of the latest changes in privacy laws that produced a huge impact on businesses (personal data treatment regulations). They remind us that ICT security is still underestimated by too many Italian firms and it can bear on their capacity to innovate (industrial security).

Mobile Security

by Antonio Ieranò

A revolution in progress

For a long time mobile users with Internet access have remained on the side-lines. It was mostly about laptops which could connect to the company's network through a modem, or through the rare high-speed lines offered by hotels. In Italy, the backwardness of Internet connectivity made it difficult for mobile users to leverage online services. People who used home connections were growing along with the success of phenomena like blogging, before, and social networking, today.

The scenario radically changed in the last years with smart devices that offer services such as Internet and access to corporate e-mail accounts.

The explosion of the use of the net dates back to June 29th 2007 when the Apple iPhone was launched. Mobile connectivity has grown exponentially since and it has changed the access and creation of content both at home and in the offices.

Facebook, Twitter and LinkedIn led users to expose themselves online longer and through more devices. With business laptops, smartphones or any other Internet-ready device, Web 2.0 access is continuous, no matter whether the tools are personal or from the office. Quite the opposite, the blend of personal and corporate frequently fades the distinctions the distinctions between those two concepts.

Smartphones and tablets

The introduction of tablets dates to March 12th 2010, when Apple began collecting orders for its iPad. Although these platforms were already available on the market[1] they were not met with any initial success. The iPad's[2] success was comparable to the one that iPhone had, creating a new demographic. The tablet's targets are professionals and managers who then brought these devices within a company. Apple has to compete with Google and its Android platform, whose first version was released on September 23rd 2008[3] on HTC Dream(G1.)

Mobile users rise (even within businesses)

For a clear view of the all-pervasive nature of mobile devices, we need only look at the indexes. An effective indirect index is the analysis of the mobile marketing market, as strictly connected not only to the platform spread, but also to their usage.

The increasing spread of smartphones and broadband in Italy is persuading many businesses to communicate with customers through mobile devices.

The analysis performed by the School of Management Observatory of Politecnico University of Milan on mobile marketing performance shows that:

- 35% of Italians has a smartphone, 12% more if compared to 2009. The European average is 10% .
- 53% of the users go online on their mobile devices and use it to log into social networks, 49% to see maps and itineraries and 38%to look for service information like timetables and bookings.
- Mobile advertising has grown 15% against 2009 data, it reached an investment worth 38

[1] The first Apple Tablet was the Newton MessagePad 100, introduced in 1993

[2] ^ “Apple Sells Three Million iPads in 80 Days”. June 22, 2010. Retrieved June 22, 2010.

[3] ^ Morrill, Dan (23 September 2008). “Announcing the Android 1.0 SDK, release 1”. Android Developers Blog. Retrieved 2011-01-12.

billion of Euros.

- Among the first 100 main Italian investors, 41 of them created an app.
- In the whole world, in 2013 users that connect to the web through mobile devices will overcome those who connect from a home computer.

Matching the above data with the consideration that Italy is the first nation in the world for mobile phone usage, it is obvious that mobile marketing will become a preferential channel between businesses and customers.

From these numbers we can deduce how important it is to the development of smartphones and tablets.

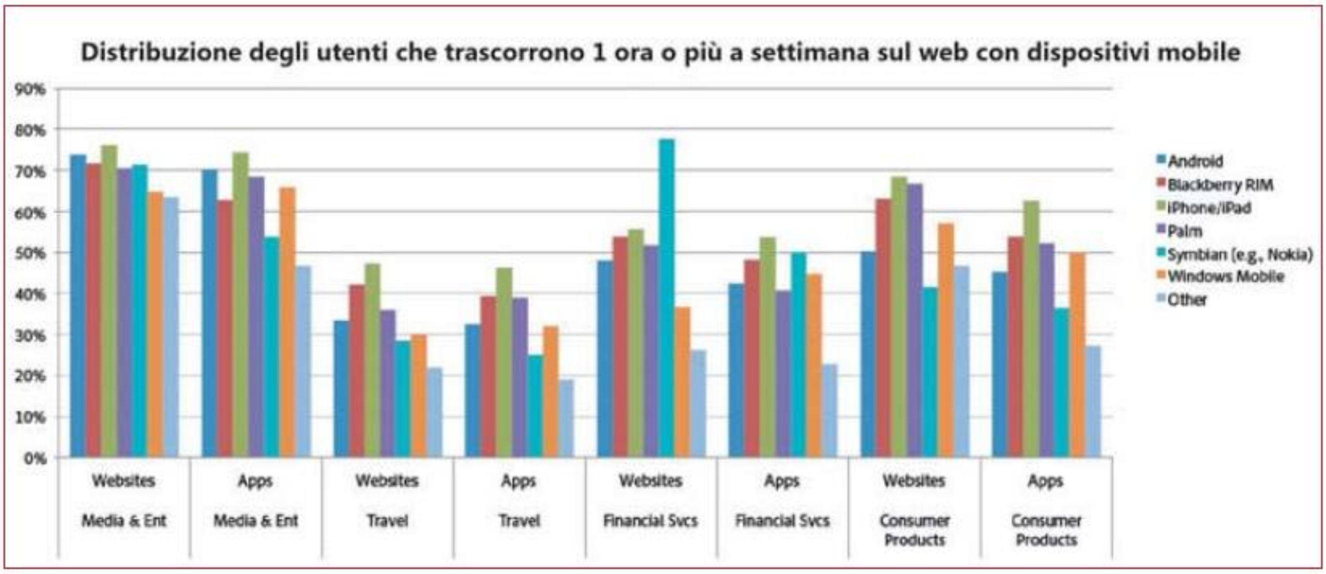


Figure 28: Mobile Internet users that spend 1 hour or more online[4]

New devices, new habits, old problems

The spread of mobile devices brought with it the spread of such new forms of risk that we have to redefine the concept of social media security. It is not only about malware that targets a mobile operating system as a specific target, but also new or "repurposed" attack techniques that exploit pre-existing but ineffective, technologies on PCs.

A glaring example is the Firesheep plugin for Firefox[5]. Firesheep leverages a classic (and wrong) free hotspot configuration that allows an unencrypted connection. The plugin allows anyone, even people with no information knowledge at all, to “read” social networks login information (Facebook, Twitter among the others) of users connected to the same hotspot.

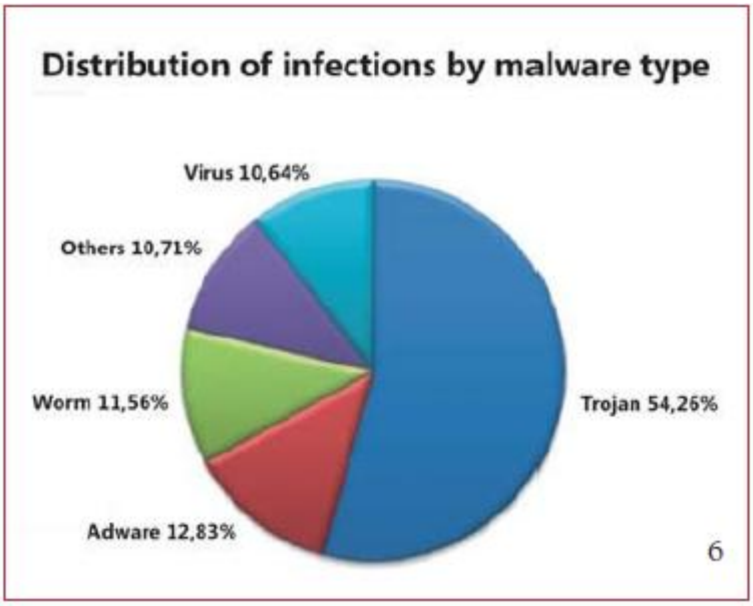
Mobile computing security in Italy is not at all only about malicious codes or “man in the middle” sort of attacks, but even social engineering, phishing and spam. Statistics say that users are more prone to fall prey to these sorts of attacks when surfing on mobile devices rather than laptops. It is sadly very tough to give official data on mobile security in Italy because of the chronic Italian hesitance to disclose attacks and breaches, though information can be found on the Internet and in books on a global scale. There is no reason why we should think that in Italy the situation is better, considering that Italy is particularly exposed. Two factors have to be taken into account: Italy has the highest relation between user/mobile phone of the world and, at the same time, it has the highest relation between user/Facebook access.

[4] http://www.turismoeconsigli.com/statistiche-web-mobile-2010-abitudini-preferenze-degli-utenti/

[5] Developed by Eric Butler: Butler, Eric. “Firesheep - codebutler”. Retrieved December 20th, 2010.

From the few data sources available it emerges that phishing attacks are commonly performed, a lot of social engineering, a good deal of information or identity stealing, but also:

- connectivity - “man in the middle” attacks, HTTPS protocol attacks, public wireless sniffing;
- operating systems – vulnerability, jailbreak/root, keylogger, worms, trojan, virus;
- application sphere – compromised applications, backdoor, browser vulnerability.



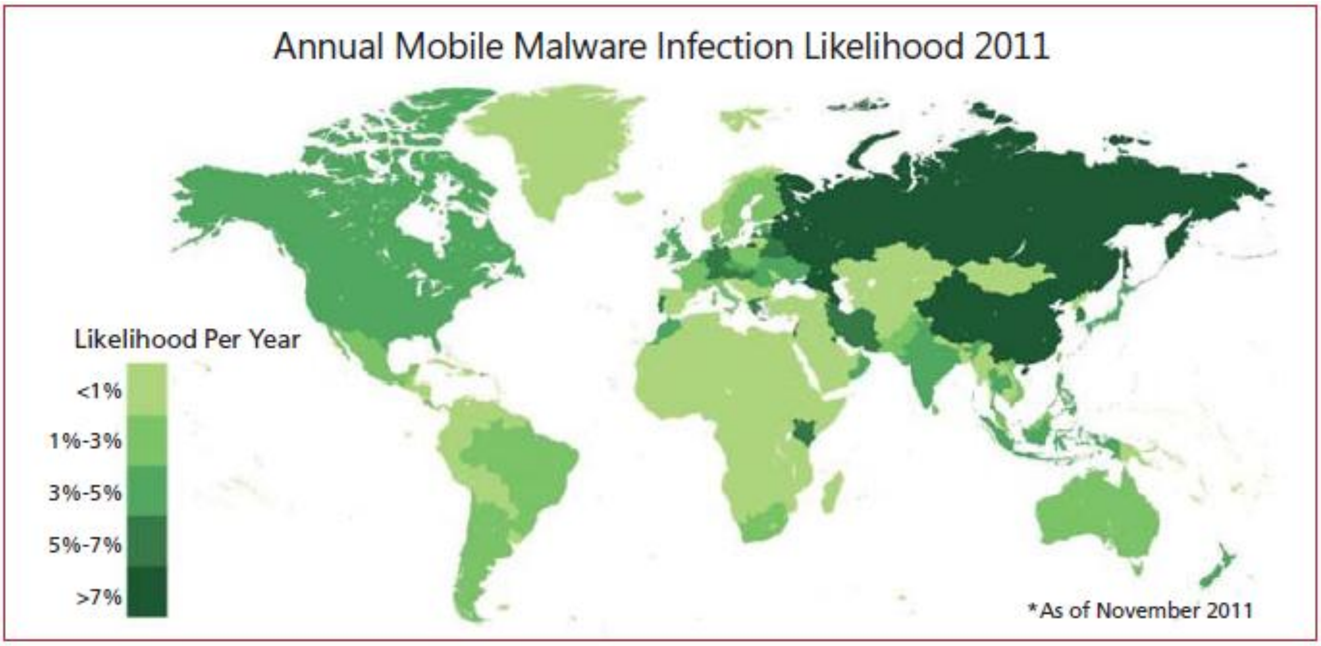
[6]

The main emerging facts is the need to give more attention to the user behaviour on mobile devices, and providing them with anti-malware (local or cloud) protection, and the need to protect their connectivity.

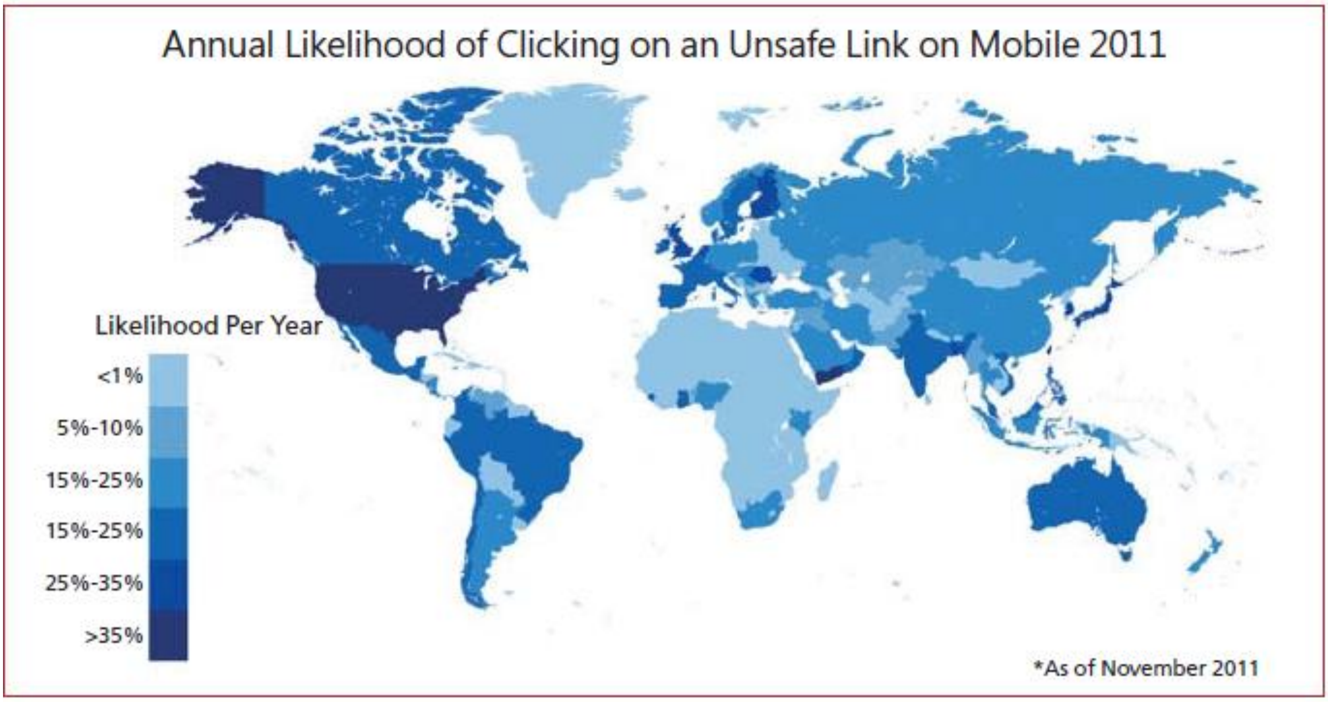
2011, the year of malware

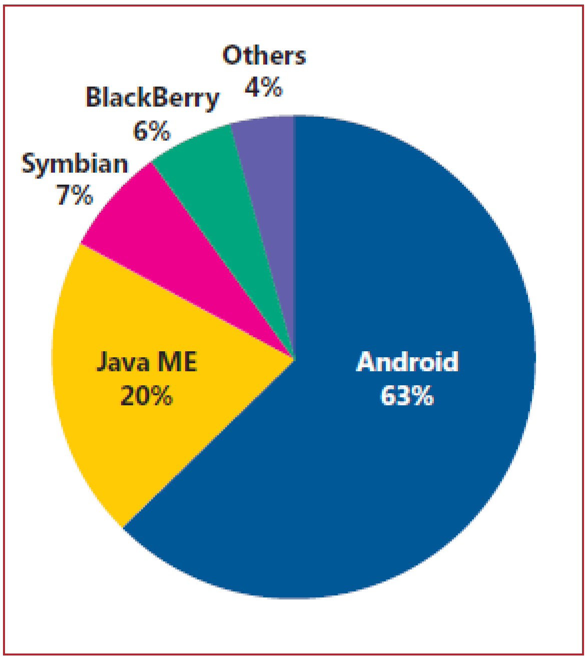
As it is very difficult to find statistics for Italy, we will see what happened in 2011 from the mobile security point of view.
The image below shows the probability to be infected by a specific malware for mobile devices. Italy is in the same range as France, whereas England is in line with the other English speaking countries. Risks are more concentrated in the East.

[6] Source: Microsoft



The image below shows regions most likely to click on a malicious link:



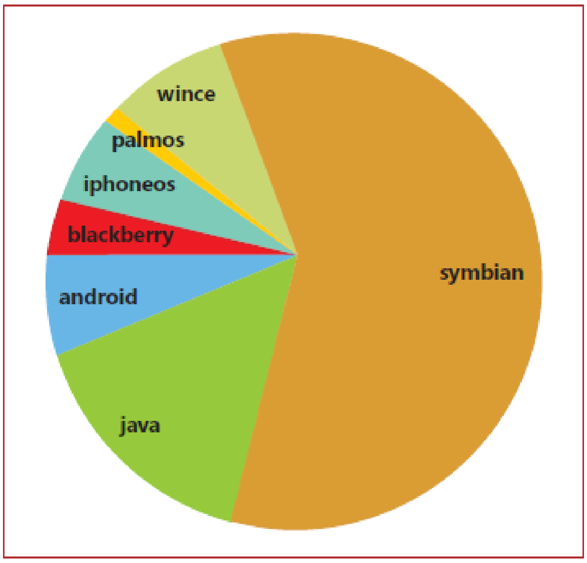


The year has been marked by the appearance of the first botnets entirely constituted of mobile devices, as well as the very high increase (400% for the Android platform) of malware associated to the various application stores.

The lion's share is of these affect the Android operating system, which, after its success and the opening of an Android Market, saw the multiplication of malware applications.

In the pie charts (source: McAfee) we can see the malware distribution according to platform. It is plain that Android has a lot of malware, and they are mostly distributed through the Android Market application. The Android Market kept an open policy towards software developers by introducing an automatic control mechanism for malware.

Despite all, Android is not the only platform to have viruses written for it. Another interesting statistic comes from Fortinet and demonstrates the number of unique malware found per platform. Symbian is still the unquestioned leader.



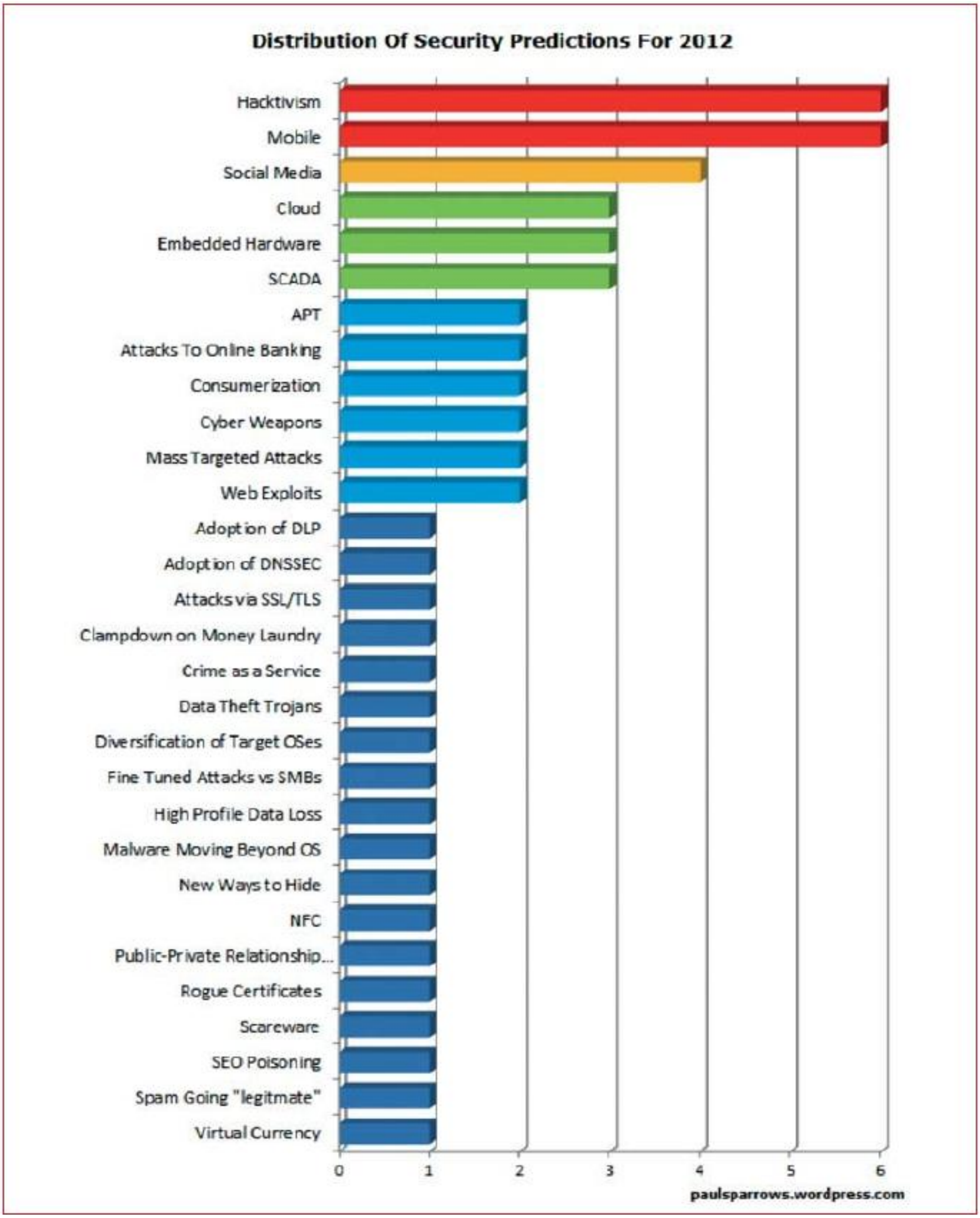
Besides malware, the year has also been characterised by privacy issues. The two main platforms, Android and Apple iPhone/iPad, have been in the eye of the storm more than once for tracking user data and for the possible geolocation that modern devices offer thanks to 3G, Wi-Fi and GPS technologies.

It seems clear that an inherently secure platform does not exist in the mobile environment and, to be honest, there are no coherent implementation polices that consider the introduction of mobile devices in the professional world. Although the BYOD (Bring Your Own Device) concept is often discussed, management policies are still quite impromptu. By contrast, we see a spread of software thought to be able to protect mobile users: the majority of antivirus vendors pounced on the market. Nevertheless, there are no statistics showing if an approach based on the installation of a protection software on a mobile device works effectively.

What we should expect from the future

A recent study by Cisco Systems underlines that the number of mobile devices is bound to increase until it will overcome the number of inhabitants of our planet. Which influence will it have on the mobile security environment?

All the forecasts agree on considering mobile security a key element for 2012. The tendencies that came up will repeat themselves despite the fact that the main players (Google, RIM and Apple) are addressing the issues of with security and privacy.


Distribution Of Security Predictions For 2012
Hacktivism
Mobile
Social Media
Cloud
Embedded Hardware
SCADA
APT
Attacks To Online Banking
Consumerization
Cyber Weapons
Mass Targeted Attacks
Web Exploits
Adoption of DLP
Adoption of DNSSEC
Attacks via SSL/TLS
Clampdown on Money Laundry
Crime as a Service
Data Theft Trojans
Diversification of Target OSes
Fine Tuned Attacks vs SMBs
High Profile Data Loss
Malware Moving Beyond OS
New Ways to Hide
NFC
Public-Private Relationship...
Rogue Certificates
Scareware
SEO Poisoning
Spam Going "legitmate"
Virtual Currency
0
1
2
3
4
5
6
paulsparrows.wordpress.com

Social Media Security

by Andrea Zapparoli Manzoni

2011: social networks revolution

North Africa and the Middle East - Tunisia, Egypt, Libya (and Algeria, Bahrain, Yemen, Jordan, Syria[1]) –, Russia, with post-electoral protests[2], England with the riots in London, Birmingham, Liverpool and Bristol[3] and the entire world (USA and Europe in particular.) What happened in 2011 in these countries after the activity of the hacktivists[4], those who hide under the pseudonym Anonymous[5], is indicative of the quick development of new cultural, politics, social and economic dynamics worldwide. These dynamics were conveyed and made possible thanks to the increasing spread of social networks.

North Africa registered the most extraordinary effects and the combination of the growing availability of connectivity (mobile especially), an average age of 25 and social networking technologies was disruptive, together with the common displeasure toward decades of misgovernance and the current global economic crisis.

The combination was so surprising for the Egyptian government that it was pushed to do something that never happened since the birth of the Internet: it disconnected the whole country[6] in a foolish attempt to stop the coordination of the crowds and the world receiving unfiltered information. Inevitably, this attempt, even if it technically succeeded, did not have the desired results and information kept on flowing through thousands alternative channels thanks to the main social platforms (Google, Twitter, Facebook)[7], that proved in this context to be the real "politics actors" on the international scene.

The planetary disdain and the reaction caused by the repressive action of the Egyptian government showed that the Internet, and the most common social networks, Facebook and Twitter, are by now considered the global meeting and expression platforms of the masses. An access without constraints is reckoned as fundamental as phone, radio and television access, if not even more important as free, immediate and (apparently) uncensored, peer-to-peer means of communication.

Five years ago this situation would have been considered impossible. International analysts certainly did not value the phenomenon with due attention, they were taken aback from the events and unable to react effectively also because of the lack of national and international laws,

[1] http://it.wikipedia.org/wiki/Primavera_Araba

[2] http://it.wikipedia.org/wiki/Proteste_post-elettorali_russe_del_2011

[3] http://it.wikipedia.org/wiki/Disordini_in_Inghilterra_del_2011

[4] http://it.wikipedia.org/wiki/Hacktivism

[5] http://it.wikipedia.org/wiki/Anonymous

[6] http://www.newscientist.com/blogs/onepercent/2011/01/egypt.html

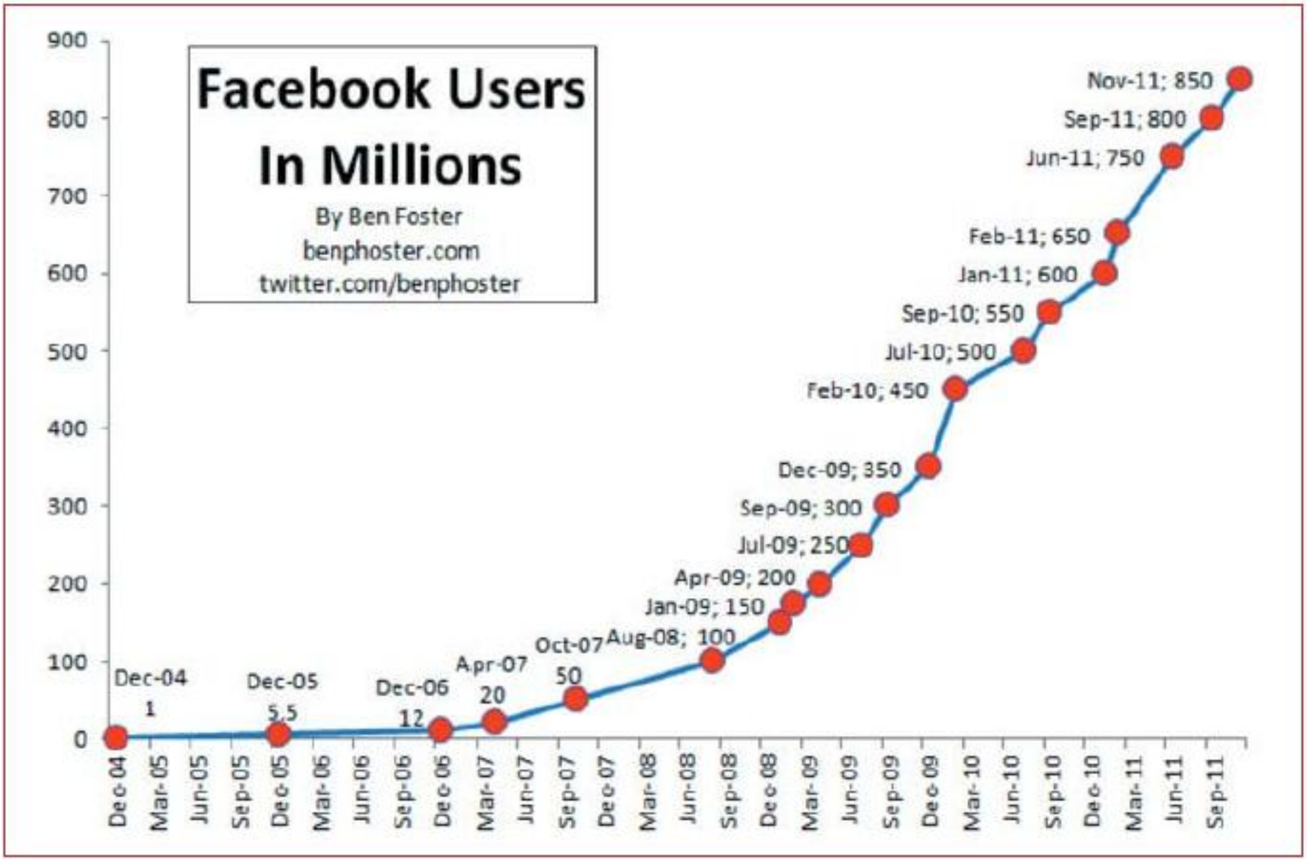
[7] http://www.trust.org/alertnet/blogs/technotalk/google-and-twitter-help-egyptians-bypass-internet-closure

emergency plans and ad hoc structures.

We therefore need to think of how quick and pervasive social networks are to understand the size of the epochal change we are approaching and to frame it in the topic of this short essay. As an example we report data on the most used social platform in the Internet, Facebook.

Facebook, the third nation of the world

Facebook, a private society born in 2004 and estimated to value between 50 and 100 billion dollars, has 800 million users in the world[8] (with, on the whole, 60 billion connections) and over 21 million of them are in Italy.
Between 2009 and 2011, an average of 7 new Facebook accounts were created every second. With a monthly 3.5% growth of 2010, Italy was the country with the fastest adoption rate in the world. In 2011, Brazil, India and Indonesia[9] registered the highest growth rates.



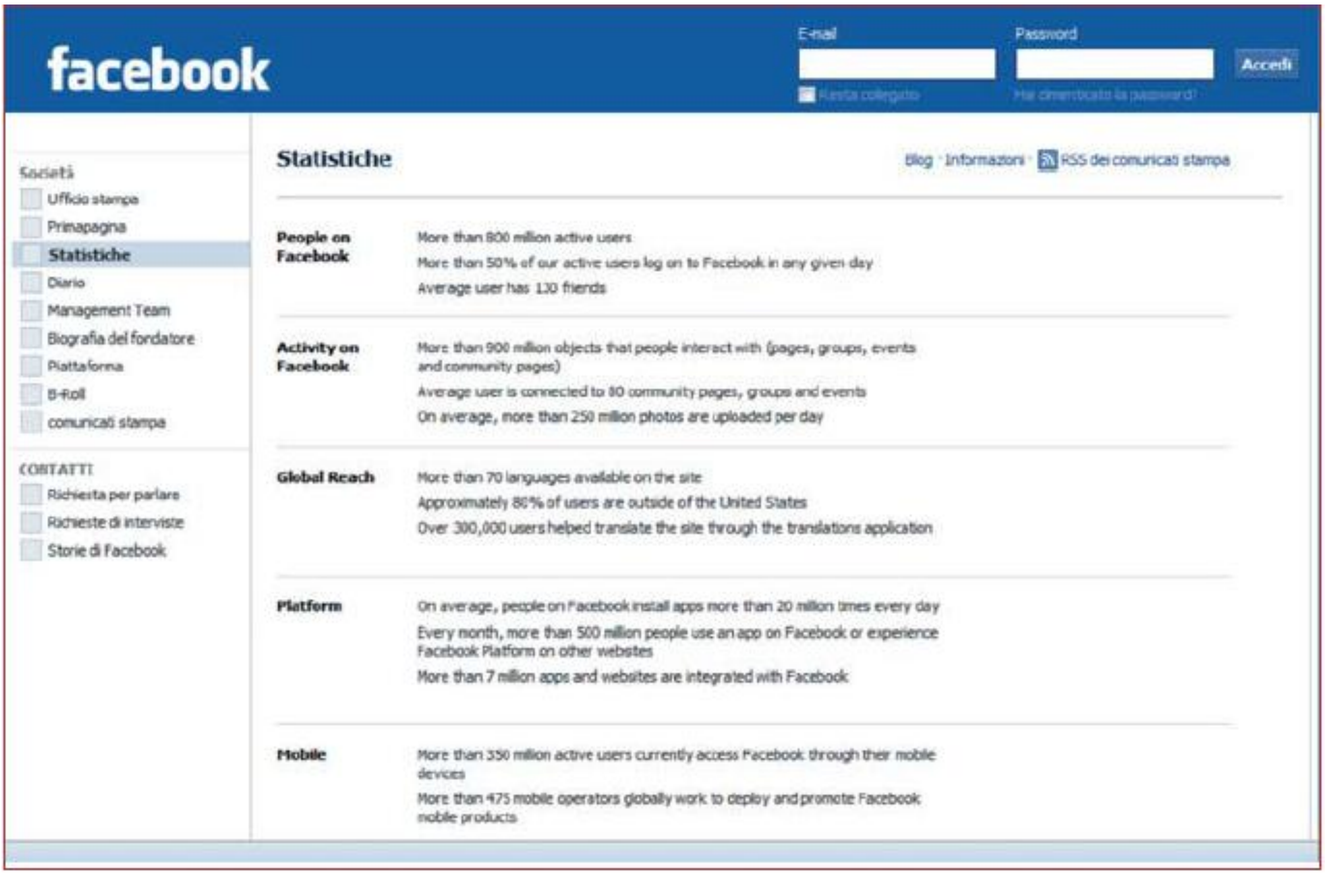
From the 2011 Nielsen Report "State of the Media: The Social Media Report" it comes out that Italy has the highest percentage of social networks users of the world, 86% of Internet users. Brazil is placed second with 85% of Internet users, whereas the States follow with 79% of Internet users joining some kind of social network.
Italy is also one of the countries where users dedicate more time in online social activities. Nearly a third of the time spent by the Italians on the net is on social platforms, whereas the same percentage for the States decreases to a fourth of their time online[10].
The average Facebook user has 130 friends, joins 80 groups and communities and spends one hour a day on the website. Every day 24 billion minutes are spent on Facebook – which is equal to more than 45,000 man years.
At the end of 2001, from the 800 million people (if Facebook was a country, it would be the third

[8] http://www.facebook.com/press/info.php?statistics

[9] http://optim.al/facebook-has-added-7-users-a-second-for-the-last-1001-days-and-other-fun-facts

[10] http://blog.nielsen.com/nielsenwire/social

biggest in the world, after China and India) 350 million logged in Facebook from mobile devices (they were 150 million in 2010) and turned out to be twice more active than traditional users, as they are always online.



Statistiche

People on Facebook	More than 800 million active users More than 50% of our active users log on to Facebook in any given day Average user has 130 friends
Activity on Facebook	More than 900 million objects that people interact with (pages, groups, events and community pages) Average user is connected to 80 community pages, groups and events On average, more than 250 million photos are uploaded per day
Global Reach	More than 70 languages available on the site Approximately 80% of users are outside of the United States Over 300,000 users helped translate the site through the translations application
Platform	On average, people on Facebook install apps more than 20 million times every day Every month, more than 500 million people use an app on Facebook or experience Facebook Platform on other websites More than 7 million apps and websites are integrated with Facebook
Mobile	More than 350 million active users currently access Facebook through their mobile devices More than 475 mobile operators globally work to deploy and promote Facebook mobile products

As for economic impact, the Facebook COO, Sheryl Sandberg, said on January 2012 in Devos that the company's European operation is worth 15,3 billion euros with 232,00 workplaces[11].

We will not go in the depths of the figures, but we point out that, besides from Facebook, other social networking platforms with their features had success, like Twitter, LinkedIn, Google+, Orkut, Renren, Foursquare, Badoo and many others.

Even if the above-cited numbers are extremely high, these platforms are not revolutionary under the technology perspective compared to what happened in the last 15 years.

Way back in 1999, America OnLine (AOL) built a community of over 10 million users (almost the total amount of the American Internet users of that year) with many of the social networking features we are used to today: it consisted of "Web 2.0 platforms" (within the technological limtis of the time, of course) offering functions such as chat, e-mail, instant messaging, picture, file and link sharing... all features that met a lot of success many years later. What reason lies behind the importance of social networks over the past 2-3 years?

An unlimited global space (for better or worse)

Any Internet connection (even a slow one) or any terminal (even a phone) with a web browser are enough for anyone to get instantly in touch with someone and to start sharing content, personal or otherwise, with the world.

From gossip to sports, politics to fashion, next Saturday night's plans to the next revolution – everything is posted, discussed, forwarded, commented at the speed of thought, anywhere people

[11] http://www.independent.ie/business/irish/facebook-brings-400m-to-economy-3002997.html

are, with a viral mechanism of information and memetic[12] transfer that is first in history for quality, quantity and the number of participants.

This new way to interact is, for the "digital natives" generation above all, is so pervasive that it alters brain processes, memory and general brain-based skills[13] and it also opens new methods in communication, marketing, CRM and e-commerce.

For better or worse, the revolutionary aspects are: on the one hand the critical mass made of numerous users, on the other hand, thanks to always-on connections, everybody can live in an unlimited social space with hundreds of people from the whole world and interact with them in the real time, irrespective of age, social status, geographic position and, within certain limits, the political and religious regime of their country.

These aspects are all positive and they can foreshadow social, economic, cultural and political developments that we never experienced before, but the dark side of social networks has to be taken into account, because they inevitably attracted the attention and interest of prowlers , became threat carriers, even very dangerous ones[14].

The dark side of social networks

Surprisingly, despite the impressive numbers mentioned before and the many signs of danger, the implications in terms of safety due to the spread of social networks have not generally been considered too much, especially in Italy.

Many digital communication experts generated miraculous expectations when they promoted the extraordinary development and the benefits arising from the use of social networks in terms of marketing and customer relationship management. They masked the reality of an exponential growth in the use of social networks to perform industrial espionage, countless types of criminal activity and even military and intelligence operations (in a spectrum ranging from OSINT to information warfare and activities that backed to operations on the field, as in the case of Twitter used by insurgents to communicate the coordinates of loyalists targets during the recent freedom of Libya[15].)

The potential consequences of cybercrime, espionage, cyber warfare[16], sabotage and similar activities committed on a global scale, in real time and via social platforms are not totally understood by politicians, law makers, mainstream media and security managers, although security recently started to interest Italian[17] authorities as well.

Even without reliable data for the nature of cybercrime, it should be remembered that the trans-national organised cybercrime is clearly facing an exponential growth (+250% in 2011 compared to 2010) having reached an estimated turnover of 7 billion dollars[18], with direct or indirect damage estimated to be beyond 350 billion dollars (at a ratio of 50:1), a bigger sum than the GDP of Denmark.

An increasing share of these crimes are performed with different techniques that exploit the inherent vulnerabilities of social networks. Nevertheless, the public opinion keeps ignoring the issue because of its occasional and fragmentary perception, which make people have a superficial attitude while exposing themselves to evitable risks.

[12] http://en.wikipedia.org/wiki/Internet_meme

[13]http://beth.typepad.com/beths_blog/2009/01/does-immersion-in-social-media-change-our-brain-functionsthis-is-your-brain-on-social-media.html

[14] http://www.slideshare.net/idialoghi/clusit-edu-social-business-security

[15] http://www.physorg.com/news/2011-06-tweets-nato-potential-libya-air.html

[16] http://www.unveillance.com/wp-content/uploads/2011/05/Project_Cyber_Dawn_Public.pdf

[17] http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Documents/Ricerche/2012/cybersec_20111109_0846.pdf

[18] http://www.slideshare.net/hackitoergosum/hes2011-raould-chiesa-hackers-cybercriminals-from-wargamesto-the-underground-economy

Social networks threats and risks

General threats that a rise from the use of social media and related risks can be summed up as it follows[19]:

Threat	Frequency	Level of risk
Malware (trojans, worms, rookits)	Very high	Very high
Spam and any kind of fraud (often combined with malware with drive-by download)	Very high	Very high
Phishing	High	High
Identity theft, identity substitution	High	High
Sensible data theft	High	High
Applications from unreliable third parties that often contain malware	High	High
Defamation	Medium	High
Stalking	Medium	High

Without considering threats coming from information warfare[20], terrorism[21] and governmental espionage[22], threats hailing from social media in a non-private context (business, PA, non-profit bodies) and their risk are summarised as follows:

Threat	Frequency	Level of risk
Social engineering or spear phishing	Very high	Very high
Private data/creative works loss or theft	High	Very high
Image or reputation damage	Medium	Very high
Open Source Intelligence (OSINT) from competitors	Medium	High
Lower productivity from co-workers	Medium	High
Third parties damages (civil and penal responsibilities)	Low	High

Since there is a very low awareness of social network risks among the population, but also among top managers, law makers and people working with IT, laws, policies, virtuosities and counter-measures have a severe delay to technology.

This delay causes a problem difficult to manage for the security teams on the one side because the huge number of users and transactions, on the other side because:

- social networks are inherently based on a unfounded sense of trust towards their members;
- authentication methods are not efficient and users identity cannot be confirmed (nor checked);
- attacks are mostly on a semantic level, with social engineering and misleading messages, which goes far beyond the traditional defences;
- spread of personal smartphones and the increasing tendency of industrial IT consumerization[23] (which entails a dual use of the devices) making security policies unenforceable.

Consequently, nowadays an organisation that use social networks for external but also internal communications is immediately exposed to a spectrum of risks including reputation, responsibilities towards third parties (users, customers, partners), Open Source Intelligence from competitors or prowlers (spammers or cybercriminals), sensible data (in accordance with the privacy or businesses law[24]) or access details (for bank or e-mails accounts[25]) loss and social network accounts[26] (or

[19] http://www.idialoghi.com/Press/iDialoghi_La_Sicurezza_dei_SOCIAL_MEDIA.pdf

[20] http://www.rawstory.com/rs/2011/07/20/pentagon-looks-to-social-media-as-new-battlefield

[21] https://365.rsaconference.com/blogs/securityreading/2011/05/01/global-terrorism-and-new-media-thepost-al-qaeda-generation

[22] http://www.forbes.com/sites/kashmirhill/2011/11/02/the-spy-who-liked-me/

[23] http://en.wikipedia.org/wiki/Consumerization

[24] http://www.infosecisland.com/blogview/9276-Is-Social-Networking-Disclosing-Your-Trade-Secrets.html

[25] http://www.infosecisland.com/blogview/8592-Social-Media-is-a-Criminals-Playground.html

information systems) hijacking.

Future outlook and possible counter-measures

On the basis of the data gathered by the SDA Bocconi[27] Marketing Observatory (*Osservatorio Marketing di SDA Bocconi)* and published in the recent research "Social Network and Business", the penetration of social networks within Italian businesses is around 40% and bound to increase during 2012.

The research also shows concerning data, such as 22% of businesses having a social media marketing strategy, 43% of users claiming not to monitor social networks whereas 34% does monitor them manually. No business seems to worry about the security, compliance and risk management implications.

Nevertheless, all the international analysts (think tanks, vendors, consulting societies) that work with social network security issues[28] agree with the foresight that the above-cited risks will increase in 2012 before a turnround can be achieved.

In light of the current on-going dynamics, the lack of user awareness and accountability (and therefore low retribution for many of the online crimes) and the insufficient ability of social network managers to counteract the above-mentioned threats is inevitable.

Businesses, corporations and institutions will be the main targets for espionage, IT systems violation and hacktivism, while people will suffer from phishing, identity theft and financial fraud.

The issue is complicated and the are no pre-packed solutions. Many factors are involved and security issues have to be confronted on many levels, not only on the technological side, to be solved effectively. Consistent and relevant solutions can be outlined if IT and budget aspects are taken into account with educational, organisation, legal and human-resource management elements.

In addition to an IT security information and education, the strategies to pursue for a risk management solution are to:

- compensate for the lack of standard procedures, policies, tools, solvency plans and industrial culture;
- implement effective technology tools to monitor and control. Firewall, proxies and antiviruses are no longer enough;
- assign responsibilities to users and business using social networks. Security is a common concern and not limited to IT managers and legal representatives;
- reduce risky behaviours against the businesses policies, which also have to be regularly updated and respected with appropriate processes.

A serious debate between institutions, companies and associations with security, marketing and legal experts has to start in order to define common objectives involving many areas, focusing on common interests and putting partial interests aside. An unstructured management of social networks risks with a medium-long term vision that emphasizes positive aspects to negative is a mistake. It can still avoided, but the time slot at our disposal to avoid that the situation slips out of our hands is getting smaller and smaller.

[26] http://news.cnet.com/8301-27080_3-20104165-245/nbc-news-twitter-account-hacked/

[27] http://www.sdabocconi.it/it/about_sda_bocconi/news_080106/2011/11/aziende_i_clienti_vi_giudicano_sul_web.htm

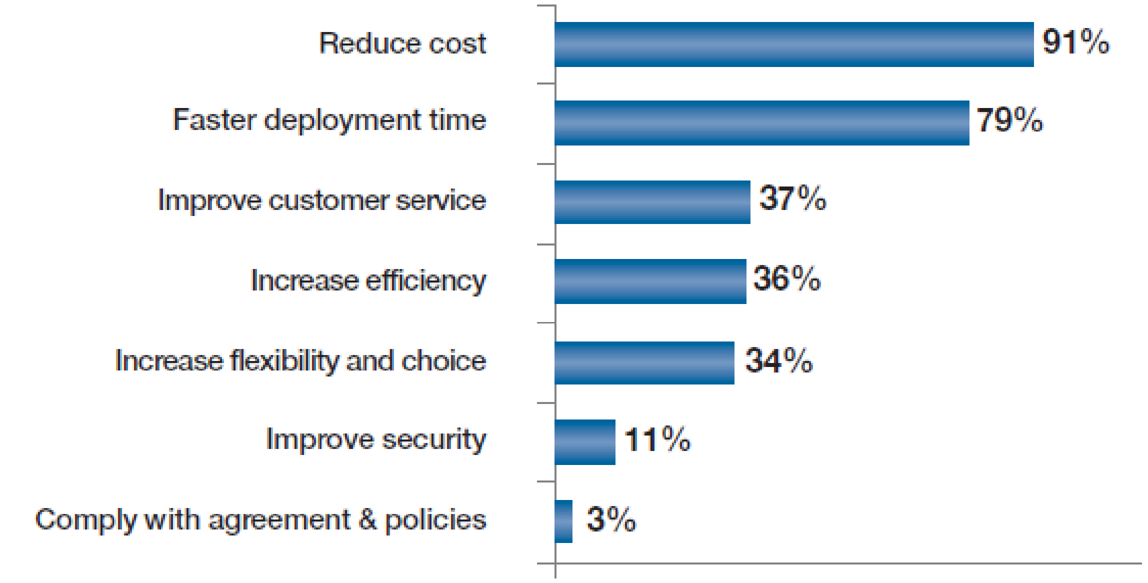
[28] http://xcluesiv.com/2012/01/23/top-5-security-threats-for-2012/

Cloud Security

by Matteo Cavallini

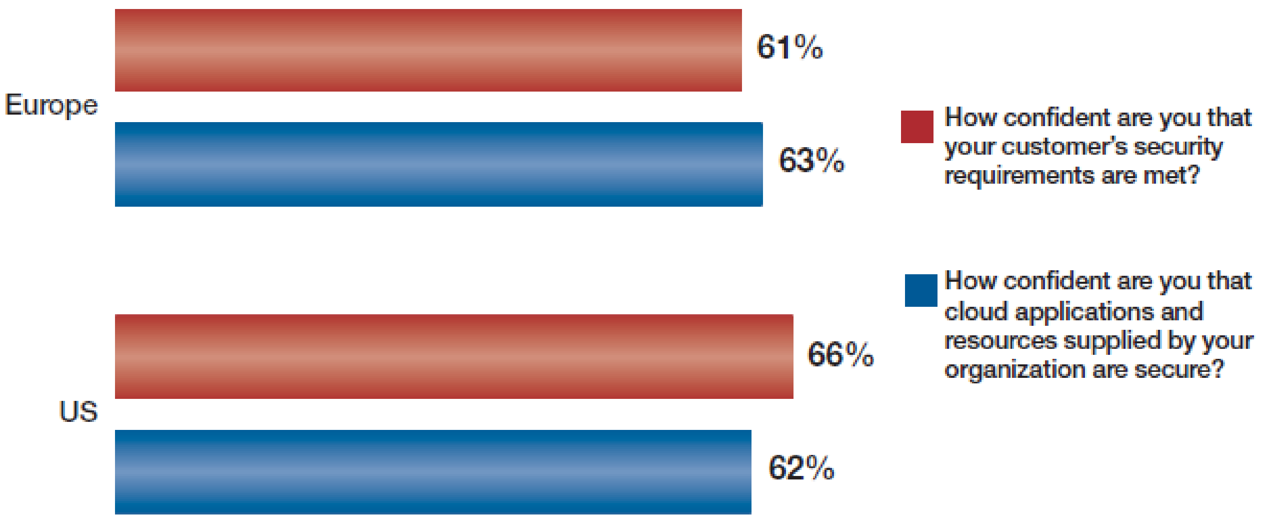
Cloud computing is growing very quickly and it concentrates big interests and investments from the entire world. Its run is of course propelled by Cloud Service Providers (CSP) who, beyond offering innovative services, produce effective marketing campaigns aimed at creating potential users, in particular in SMEs and PA. As stressed by an April 2011 survey from the Ponemon Insitute ("Service of cloud computing providers study"), Cloud Service Consumers (CSC) are attracted by the advantages that cloud services can give, both in terms of expense restraint and overall complexity.

Bar Chart 5: Reasons customers migrateto the cloud computing environment
US & Europe results combined



The same survey points out that the main obstacles of cloud services usage stem from the possibility of CSP to guarantee adequate security levels to CSC. CPS and CSC's expectations entail, if possibile, a greater concentration on cloud service security, beginning from the definition or the prerequirements and the usage's contexts.

Bar Chart 6: Lack of confidence in the security of cloud resources provided
Not confident & unsure response combined



The best way to approach and profit from cloud services and to reduce risks is to identify user requirements and analyse the risks by considering the features of CSP.

The main security issues for CSC are general and have a more significant impact on most contexts and cloud services. The so-called *Multi-tenant model* (a service is helpful for many clients at the same time using the same architecture, but working and interacting as if it was created for a single client), for instance, opens the door to privacy problems that have to be considered. Different clients separation is usually virtual and it makes attacks -or configuration errors- theoretically possible and they can be transmitted to other clients of the same CSP. Other "open matters" are: difficulties to maintain an adequate cloud services governance and to obtain warranties on CSP service approaches, "lock-in" problems (problems in changing CSP because of low interoperability and portability of the supplied services) and, above all for European countries, the low respect of personal data protection laws. Moreover, an issue whose importance has yet to be clarified is how complicated it is to manage security incidents in the cloud. When an incident is occurring, it is vital to have the information to make a deep analysis and collect evidence of what happened. In the cloud, this information belong to more subjects, cooperation and information exchange is therefore essential between the CSC and the CSP. At the moment, these information exchanges are infrequent and rarely regulated. In Italy, these issues have to be summed up with the difficulties in creating facilities for the spread of symmetric broadband (with the same upload and download speeds) and these limits are an obstacle for the spread cloud services.

Due to the global interest in cloud security, during 2011 the media gave attention to security incidents. "Cloud" and "hacker" have become buzzwords with a high impact on the public and by consequence, the media talked profusely about various incidents, sometimes even emphasising them in order to have a scoop.

Main 2011 security incidents

Via search engines we can chance upon many articles or comments on real or presumed security incidents in the cloud. Among the different events, there are two incidents with a paradigmatic value: the Epsilon data theft and the poor functioning of one of the two American Amazon datacentres.

On March 30th 2011, the American company Epsilon, an important direct marketing CSP that sends over 40 billion emails a year on behalf of its clients, detected unauthorised access to its systems and serious violation of information confidentiality by unknown hackers. Given the nature of the services provided by Epsilon, the compromised information was essentially the user data of its client companies, which Epsilon was conducting promotional and loyalty building campaigns for. The list of the companies involved is made up of important businesses and includes, among others, financial, fashion and technology companies. This is certainly one of the most serious hacking events for the sheer amount of compromised data and it showed that the security of cloud services is a key-issue for CSCs that may suffer the direct and even of considerable consequences of incidents involving CSPs.

The second event is about cloud service reliability and involves an internationally important player: Amazon. In mid-April 2011, the Amazon Web Services (AWS) offered by one of the two major datacentres, had technical problems that knocked down the website of a subscriber CSC. Beyond the 36 hours needed to go back to normality, a lot of websites were darkened. Quora, Reddit and Foursquare had to wait that Amazon restarted to deliver its services to restore their websites. Not all the websites that were basing their activity on the damaged datacentre went offline. Netflix, a video streaming website, escaped unharmed thanks to the shrewdness and caution it displayed when projecting service redundancy measures. Hence, this service black-out underlined both service availability problems and the possible solutions.

The main episodes on international and national level

The growth of the cloud in 2011 was characterised by the refining of market proposals and by the definition of technical examinations and best practices on the international level that met CSC security needs. Literally pushed by these needs, the great market players, organisms that interface with security players and many governmental authorities produced many documents to create trust between CSP and CSC. Among those who actively move to develop a sense of trust in cloud services, we have to nominate the **Cloud Security Alliance** (CSA), an international association that wants to promote best practices for secure cloud computing and education in the use of cloud for the IT security sector. CSA has fifty national chapters in the world and more than 29,000 associates, and has generated a cloud security approach that is by now considered “de-facto” an international standard. The “Security Guidance for Critical Areas of Focus in Cloud Computing” reached its final version ,3.0, released in November 2011. It further deepened security concerns and added a topical issue of “Security as a Service” (SecaaS.)

Throughout 2011, CSA started new research and development projects that will be released in 2012. We should remember “CSA Security Trust & Assurance Registry” (CSA-STAR) a public registry of security controls in the various cloud offers. The registry helps whoever is attempting to verify and evaluates market offers on security.

CSA STAR™ Security, Trust & Assurance Registry

It is also worh remebering the CloudSIRT project, whose mission is to develop cloud community skills and to be ready to face vulnerabilites, threats and incidents to preserve trust in cloud computing.

As we move towards the improvement of cloud service security, every cloud end-user (public or private) must identify policies to better understand cloud services in their context, taking into account both features, and potential limitations or pitfalls.

United States

At the beginning of 2011 the US "**Federal Cloud Strategy**" was disclosed, a stategy that traces the guidelines for govermental agencies that are adopting cloud services. This document contains the **"Cloud First Policy"**, which force federal structures to give priority to cloud services when starting new projects. In addition, many activities were put forward that intended to make the ambitious targets set by the Federal Cloud Strategy possible. In particular, we have to mention the certification program **"Federal Risk and Authorization Management Program"** (FedRAMP) elaborated by US General Service Administration and published in December 2011, which gives a standard approach to cloud products and service security tests and monitoring. FedRAMP uses a *do once, use many times* kind of approach that wants to curb costs and certification efforts for the benefit of efficiency and transparency. Finally, the documents from the NIST, the American standardisation corporation are noteworthy as they contributed sound scientific and methodological bases to the analysis of cloud services and helped create a common awareness of problems and their solutions

European Union

Europe dedicated many efforts to create an environment where cloud services can be developed and to give spaces to think within the **Digital Agenda** and, with popular consultation, the redaction of the "European Cloud Computing Strategy". The European Commision's vice-president Neelie Kroes established three guidelines for the European strategy:

- define the legal contexts which can positive for the development of cloud services, particularly related to personal data protection and their treatment abroad;
- research support to find effective solutions in the field of security, cloud service resiliency and the development of proper technical standards for APIs and data formats;
- support pilot projects for cloud services deployment, especially for the public sector, SLA development and contracts based on shared ideas.

Finally, the contribution that the CSA has openly given for the development of the European strategy with a document that suggests that the priorities on which the European Commission should direct their efforts. Among these, the main are represented by: portability and interoperability, trust and security, and finally innovations in cloud security.

Italy

At the end of May, the Authority for Personal Data Protection published a document entitled "Cloud Computing: Instructions for the Aware Use of Services" (*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi.*) The interesting document sought to give indications and useful information to users with small dimensions and limited economic sources (individuals, SMEs, local administrations like small municipalities) that are the recipients of increasing offers of cloud computing services (public or hybrid.) This information is directed chiefly with personal data protection in mind and wants to promote the proper use of information services via the cloud (public clouds in particular) and the data sharing it entails.

At the end of July 2011, Consip published: **“Cloud security: una sfida per il futuro”** (*Cloud Security: a Challenge for the Future*) oriented to PA and SMEs. The “Consip Notebook” focuses on security aspects and unsolved issues and wants to give useful suggestions on how to improve data security and within cloud computing. There is also an analysis of the ten major risks for Italian CSC (with the different service suppliers) and indications for an aware service approach.

DigitPa also launched an ambitious program of collecting and publishing documents on cloud that range from security to privacy. A large group of public corporations and private entities joined the program, some of whom are the main international cloud computing players. The final release is expected in 2012.

Moreover, at the end of 2011 the Italian chapter of CSA (CSA-Italy) was born and started the production of the document, “Portabilità, Interoperabilità e Sicurezza delle applicazioni” (*Applications Portability, Interoperability and Security)* that has been presented during the Security Summit of 2012, in Milan. The document offers guidelines for the associated research over the upcoming years and aims at offering an efficient contribution to develop greater awareness in Italy.

In conclusion, the cloud is moving toward a rapid growth of offered services and to a global deployment of them. The union of the service supply appeals to efficient technologies and economies of scale through resources sharing. The limits between CSPs are slowly fading, and CSP's responsibilities are more interconnected to CSC’s. Security turns to a crucial junction within this growth, and can create the pre-requirements to transfer *core* and similar applications and services into the cloud.
As we progress towards a common security model and possible solutions, the choices made on the governmental levels are crucial. Our hope is that Italy will devote the proper attention to these topics to guarantee future growth and development.

Personal Data Treatment Regulations, Updates over the last 12 Months

By Gabriele Faggioli

The European Commission recently presented a proposal to harmonize personal data protection within the EU.
In particular, it proposes a regulation that will replace the 95/46/CE directive that will be self-executed in every Member state, thus in Italy as well.
If it will be approved, the Privacy Code will be affected, but privacy protection will finally have common rules within the Member states.
In this frame, the Italian lawmaker has definitely not been inactive. With a series of measures the Italian legal framework in the field has been radically changed.

At first, on May 13th 2011 the Decree law no. 70/2011 *"European Semester – First Urgent Instructions for the Economy*" *(Semestre Europeo - Prime disposizioni urgenti per l'economia)* was approved and then converted into the law no. 106/2011. The article no. 6, paragraph 1, foresaw legal compliance simplifications and reductions particularly important for the matter of privacy.

Then, on December 6th 2011 the Decree law no. 201/2011, known as "Save Italy" (*Decreto Salva Italia)* was approved and contained the "*Urgent Provisions for the Growth, Equity and Consolidation of public accounts*", converted into the law no. 214 on December 22nd 2011. The Decree brought reductions to the administrative fulfilment on privacy to reduce the burden driving from the current regulation on businesses. At last, with the Simplifications Decree approved on January 1st 2012 and published in the *Official Gazette (Gazzetta Ufficiale, the official journal of record of the Italian government)* in February, we should see more changes simplifying the legal obligations for personal data protection within businesses.

In chronological order:

- *Decree law no. 70/2011* "*European Semester– First urgent provisions for the economy" converted into law no.106/2011.* To reduce the burdens of the regulation that weighed particularly heavy on small and medium enterprises, changes have also been made to decree no. 196/03 to, according to the lawmaker, allow the "proper enforcement of the European regulations" ("*corretta applicazione della normative europea")*, with a focus on regulation of data protection for natural persons. The law maker introduced a new principle ("*il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo-contabili non è soggetto all'applicazione del Codice per la protezione dei dati personali*"). Between May and July, in fact, the lawmaker established that it was useless to subject natural persons' personal data to regulation when treated for administrative purposes and, in particular, when the data treatment is related to organisational, administrative and financial activities, leaving aside the nature of the treated data (even sensible data). The lawmaker (art. no. 34 paragraph 1-ter legislative decree 196/03) believes that this is followed by the internal organisational activities for the contractual and precontractual fulfilment of obligations, to manage the working relationship in every phase, for bookkeeping, for tax purposes, trade union, welfare, health, hygiene and work security law enforcement. Between May and July, the lawmaker wanted to create a clear distinction between data of natural persons and legal persons, as in Table 1 below; the regime is to be enforced from May to December 2011.

Table 1. Applicable Regime from May to December 2011

Natural persons data		**Legal persons data**	
Data treatment for accounting or administrative purposes	Simplifications	Data treatment for accounting or administrative purposes	Non-application of the *d.lgs 196/03* and related provisions
Data treatment without administrative or accounting purposes	Legislative decree application (*d.lgs 196/03*)	Data treatment without administrative or accounting purposes	Legislative decree application (*d.lgs 196/03*)

- *Decree Law no. 201/2011 with "Urgent Provisions for the Growth, Equity and Consolidation of public accounts" converted with the law December 22nd 2011, no. 214.* With the article 40, paragraph 2, letter a) of the Decree law 201/2011 the definition of *"personal data"* changed and now does not include data on legal persons, corporations and associations. The definition of personal data is part of the art. 4, paragraph 1, letter b) of the legislative decree 196/2003, which says that personal data is any information related to a natural person that can be identified through any other information reference, personal identification number included (*"dato personale, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"*). After only six months, the lawmaker changes the whole coverage that was introduced in May and then confirmed in July the deletion of data on legal persons, corporations and associations (subscribers aside – marketing and data retention) from the law enforcement field. Companies are no longer "interested" in data treatment and they cannot therefore exercise the rights according to art. 7 and following legislative decree 196/03. Today's situation is shown in Table2.

Table 2. Applicable Regime from end December 2011

Natural persons data		**Legal persons data**	
Data treatment for accounting or administrative purposes	Simplifications	Data treatment for accounting or administrative purposes	Non-application of the *d.lgs 196/03* and connected provisions
Data treatment without administrative or accounting purposes	Legislative decree application (*d.lgs 196/03*)	Data treatment without administrative or accounting purposes	Non-application of the *d.lgs 196/03* and connected provisions
		Subscribers	Marketing and data retention rules application

- *Simplification Decree.* At last, with an order published in the *Official Gazette* on February 9th 2012 and at the moment under conversion process into law, the lawmaker has intervened with a change which overturns a cornerstone that up to today was considered essential in the information systems security legislation and, in particular, security measures required by Attachment B of legislative decree 196/03.
The policy document on security has been abolished. The lawmaker claims that:

➢ in article 34 the letter g) of paragraph 1 on the keeping of an updated policy document on security is suppressed and the paragraph 1-bis abrogated;

➢ in the technical specifications on the minimum security measures, part of the Attachment B, paragraphs from 19 to 19.8 are deleted (security policy document contents, and therefore the education plan of those who will deal with data treatment) and 26 ("*In his accompanying report on the annual financial statements, the owner refers, if applicable, the preparation or the updating the security policy document*".)

It is interesting to note that in May, with the Decree law no. 70/2011 "European Semester–

First urgent provisions for the economy" converted into law no.106/2011, the lawmaker modified the rules of the Security Policy Document with the change of art. 34 paragraph 1 bis, which was introduced in 2008. Table 3 shows the change introduce by the law maker:

Table 1. Applicable Regime from end December 2011

Year	Provision
2003 - August 2008	No exceptions to the obligation to present a Security Policy Document
August 2008 – July 2011	Article 34 paragraph 1 bis *d.lgs* 196/03. Subjects who treat personal data and not sensitive data, and **who treat as sensitive data concerning the health of their own employees or co-workers, without indicating the diagnosis, or their joining to trade union organisations or similar,** the update of a security policy document is substituted by the obligation of self-certification and to treat only those data according to other security measures. (Omitted)
July 2011 – January 2012	Article 34 paragraph 1 bis *d.lgs* 196/03. Subjects who treat personal data and not sensitive data, and **that treat as sensitive and judicial data those related to their own employees or co-workers, non-EU citizens as well, including the data on the spouse and other relatives,** the update of a security policy document is substituted by the obligation of self-certification to treat only those data according to the minimum security measures set by this code and by the content of Attachment B). (Omitted)
January 2012 - ?	Entire abrogation of the Security Policy Document

It should be emphasized that in front of this series of simplifications introduced by lawmakers, the Authority for personal data protection intervened, sector by sector, with measures that introduced new and significant obligations. On May 12th 2011, a provision for banks was introduced, "*requirements in the information circulation in the bank field and banking transactions tracking*", which established rules, exclusively limited to the banking sector, related to the circulation of personal data and bank transaction tracking.

On the tracking field, the Authority realised that in the absence of laws obligating banks to track transactions, determining the details of file conservation, to guarantee the control on activities performed on clients or potential clients' data from anyone in charge of their treatment (his/her qualifications, competence, operative fields and purposes) banks have to adopt suitable information solutions and measures that allow an effective control, even in the treatment of data for every single information stored in the databases. These solutions have to include a detailed registration, in a dedicated log, of the information of bank transactions. In particular, the log files have to track every access operation to bank data by someone in charge, at least following information:

- identification code of the subject in charge that accessed the information,
- data and time of the operation;
- workspace code;
- code of the client on whose name the operation of bank data access has been performed;
- type of contractual relation of the client for whom the operation has been performed (i.e. current accounts number, bank credits/mortgage, stock deposit.)

This provision is extremely important and has a high impact on the banking sector, chiefly due to the complexity of implementing these policies for system administrators.

It is, at last, necessary to indicate the Legislative Decree no. 61 that entered into law on April 11th 2011 (on May 4th 2011 in the *Official Gazette*, no. 102 – Implementation of the directive 2008/114/CE on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection). Its aim is to set the procedures to identify and designate European critical infrastructures (ICE) in the fields of energy and transportation, and assessment methods for the security of facilities, the protection requirements from human, accidental, intentional, technology and natural disaster threats (article 1.) These procedures regard infrastructures on the national territory and those infrastructures, even if based in Member states of the EU, that Italy is willing to designate as ICE.

ICT Security Situation in the Italian Public Administration

By Giovanni Manca

General aspects

The general perception on the ICT security situation in the Italian public administration (PA) is not positive at all, but. an objective analysis cannot be only based on perceptions, but on objective data.

As we will see shortly, what we miss is global and up-to-date analytic data on how central and local PAs invest on ICT security. Instead we must satisfy ourselves with general analysis, indirect deductions and a bit of common sense.

In the past, the Ministry for Innovation and Technologies Institution had multiple funding plans for e-government projects and developed a unification and rationalisation methodology of ICT innovation that involved security.

Within e-government security, an ICT security directive was issued as part of the January 16th 2011 directive of the President of the Council of Ministers. The directive contains the minimum requirement that the administrations have to fulfil after self-evaluations on their ICT security level.

The National Technical Committee on ICT Security was born and its task are the fulfilment of security objectives through a route with the following steps:

- analysis of the PA's situation from a security perspective;
- creating and spreading guidelines;
- project planning to fulfil the objectives;
- consultancy and support services.

In October 2003 a national model to certify ICT systems and product security was established according to ITSEC and Common Criteria standards, as long as they do not deal with secret state information.

It seems that everything is going on quickly and smoothly in the right direction. The route continues with the funds allocation for two initiatives:

- a CERT project for PA;
- an “education and awareness centre for PA personnel”

In summary we also remember the National Plan for Public Administration’s technologies, information and communication security (*Piano nazionale della sicurezza delle tecnologie dell’informazione e comunicazione della pubblica amministrazione*) and the National Organisation Pattern for ICT Security (*Modello organizzativo nazionale di sicurezza ICT.*) These documents were published on March 2006 as book no. 23 of the CNIPA, National Centre for Computer Science in the Public Administration (*Centro Nazionale per l’Informatica nella Pubblica Amministrazione*.) But what happened over the past six years?

What does ICT security in the PA mean?

To analyse the current state of ICT security we need to understand what is means in organisation and implementation terms for the PA itself.

The PA works respecting the law and ICT security must be therefore analysed in its public management. Furthermore, the PA has a response time appropriate to its large size, which does not fit with the reality of rapidly developing technologies and methodologies. These brief preliminary remarks introduce the fact that the PA began to be adjusted to the National Plan and Organisation Patterns rules in 2006. The complicated Connectivity Public System (SPC) gathers these rules so that the PA can handle the process with comfort and support. SPC security laws are in compliance with regulation documents, product and services providers that comply with SPC rules are subjected to tests and audits and this should not leave room for doubts on their evolution. CNIPA (today DigitPA) has a leading role in the SPC project and considering the current information, a usual part of the report on the situation of PAs, the first pieces of structural data are emerging.

These pieces of data have been released after specific disclosures within the “Report on ICT Security Situation in the PAC”, where PAC stands for Central Public Administration.

Of the reports, three of them were produced but the third seems not to have been published yet. The two first are available at DigitPA (not on the institutional website).

In short, we can affirm that the reports are important for their data but also because:

- they introduce a standard pattern of data disclosure;
- they present the collected data according to the standard patterns classification.

The indicators are:

- logical security;
- facility security;
- organisational security;

The evolution from CNIPA to DigitPA introduced some delays and so it is necessary to underline that the latest data are from 2007 (published on March 2009) and only regards central public administrations.

Data are collected via a survey that 61 administrations accepted to respond to. We will not delve too deeply into the results but by analysing the middle values of the data collected through the surveys, we can see the following results:

- "satisfying" for the logical protection;
- "very satisfying" for the facility security;
- "sufficient" for services security;
- "to be improved" as regards organisational security.

This is in league with our expectations: the security efforts for logical and facility security are high, since they have been active for many years now, while online services are still growing and consolidating. The situation is better overall, apart from the organisational security. The bigger administrations are in line with the Organisation Pattern, whereas the smaller ones are struggling to organise themselves and sometimes they cannot satisfy the legal requirements on internal security, in particular the laws on personal data protection. There are SPC “interface” rules, but they do not act inside a single administration even if they state, for example, the nomination of a CERT (Computer Emergency Response Team) manager.

Before discussing the current state, we can end the analysis of the intermediate phase of security evolution underlining the great effort that DigitPA is doing to check the security situation in the central PA. It is also important to point out that in this phase the security education process organised in the Higher Institute for Communications by the Communications Department of the Ministry of Economic Development for PA personnel is coming to an end, on the basis of what the specific project of the National Committee foresees.

What about the last three years?

Where are we now?

From mid-2009 SPC became DigitPA and developed a security coordination with the CERT-SPC office. The administrations increased their security awareness and their organisational efficiency, but an adequate regulation that force them to apply security is still missing.

A series of specific articles on the Decree Law no. 235 of December 30th 2010 which bring changes to the CAD (Digital Administration Code) gives the right stimulus in this direction. These articles are 50-bis (Operative continuity) and 51 (Data, systems, facilities security of the public administrations).

From the two articles emerge some legal innovations in terms of ICT security.

The first innovation is the concept of operative continuity that forces the public administrations to arrange beforehand emergency plans that can guarantee the restore of the normal activity after a variety of pre-defined security incidents.

This aspect is very important for a central or local PA because, as it is obliged to eliminate paper materials from the administrative procedure, digital data protection becomes crucial. Even an Excel file with, for example, medical records on the organs that can be transplanted and stored on hard disks has the same value as the giant filing cabinets of the Italian tax record offices or social security institutes. The latter had already arranged operative continuity and disaster recovery plans before the current legal constraints to confirm that big administrations can act more rapidly that the other public administrations.

With this in mind and due to the lack of common standards, DigitPA produced guidelines in order to help PAs and to avoid the possible hard work of going through thousands of difficult questions. The guidelines were published on the DigitPA websites under the "*Continuità operativa*" section and they have been made official on the *Gazzetta Ufficiale* (*the official journal of record of the Italian government*) no. 295 on December 20th 2011.

Article no. 51 is also very important. It establishes that specific technical rules have to be set declaring the modalities that guarantee data, systems and facilities accuracy, availability, integrity and confidentiality.

This is noteworthy in that specific security rules are set, going beyond the old privacy laws part of attachment "B" of the Privacy Code. ICT security must also be extended to the general data treatment not only limited to personal data. DigitPA has to inform the competent Ministry in case of unfulfilling administration via specific reports, assuming the role of the supervisor.

Conclusions

We saw that ICT security in the PAs is rather opaque, in particular when concerning local corporations. But it does not mean that PAs are unsecure. Every more or less complete disclosure seems to indicate the opposite, even with its acceptable flaws. The new CAD laws can positively change the situation as they set obligations and indicate who has to respect them.

Not all that glitters is gold and the operative continuity will be thoroughly examined by DigitPA, but the question is, will laws be properly applied in every PA, especially in the smallest and under-equipped in terms of manpower and tools?

With regard to the application of Article 51, DigitPA will only collect disclosures based on surveys and no PA will be so sincere to denigrate itself if something goes wrong. The previous disclosures were anonymous, while the new failings are reported to the competent Minister. DigitPA acquires then a ICT security supervisory role (because it is actually supervision.) Despite the institutional professionalism of DigitPA, a degree of scepticism is permitted regarding the effectiveness of such supervision.

It is worth reiterating that, in the national set of rules, a National Security Agency (equivalent to the BSI of the Federal Republic of Germany) would be much appreciated and provide a strong and independent coordination of the initiatives in the ICT security field. This agency, more than once discussed in political circles, has never been created because everyone in the PA wants to mind its own business, and does not want accept intrusions except from the providers in charge.

However, we do not accept it, because a factional approach to ICT security is never a good thing.

Internet and Control Systems Protection in Industrial Environments (and Infrastructures)

By Enzo M. Tieghi

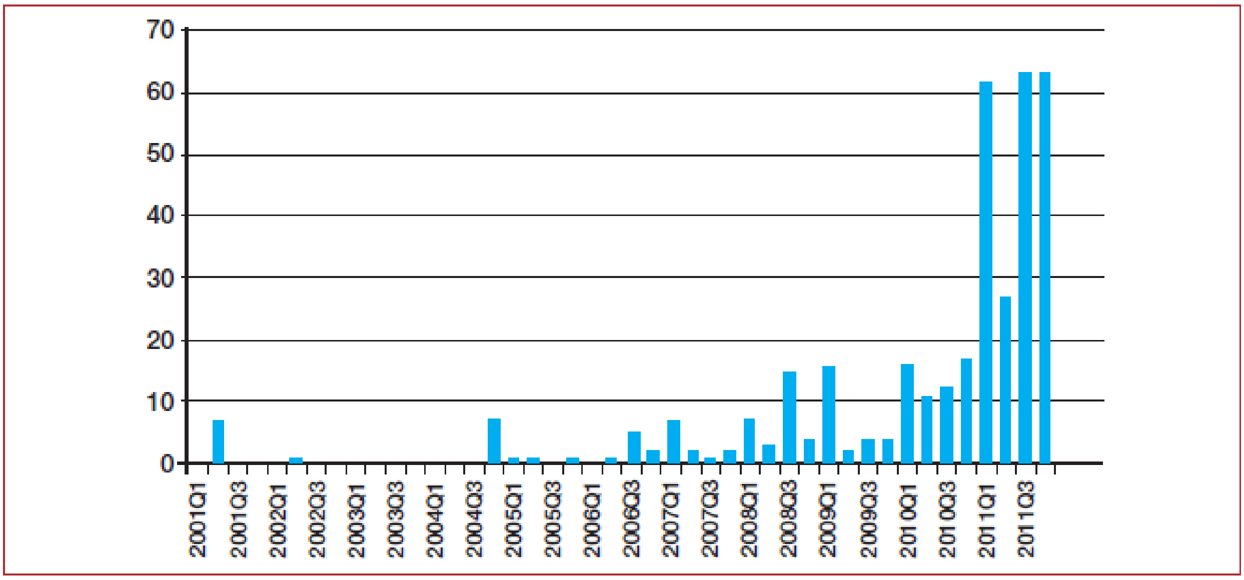
2011: the year of awareness?

For many people involved in the development, the maintenance and the operation of control and remote control systems used in industrial and infrastructural sectors, 2011 was, perhaps, the year of awareness. However, it is now necessary to take into consideration the information security risk. This will ensure proper and continuous functioning of control and supervision systems, the monitoring and the management of installations, beyond simply being able to ensure production and service continuity. Automation and control systems are now everywhere: from production and equipment areas in industries, to buildings (shopping centres, hospitals, offices, museums, airports, warehouses, prisons, laboratories, etc.), to networks and all kind of infrastructures (aqueducts, highways, railways, tunnels, bridges, harbours, telecommunication networks, radar, traffic lights, gas and oil pipelines, etc.),. More and more (is this globalisation?), systems and devices with the same technologies, architectures and models are used in applications that are completely different one from the other. Configurations and protocols (now based on IP) are similar everywhere and they are adopted as standards: what follows is that the vulnerabilities of each of these systems component and their threats can open large gaps in a steel establishment or in a hospital, and the ubiquitous role of networks will cause these problems to spread faster than usual.

Stuxnet "awoke us" from lethargy

Born in 2010, Stuxnet immediately appeared as something new and disruptive. For the first time, newspapers[1] and TV news talked about this APT (Advanced Persistent Threat), a malware “specially designed and developed” by targeting a certain type, a certain brand and a certain model of the control system. Incidentally, it was exactly the same equipment used by the Iranians to control equipment and machinery in their controversial nuclear centres. The main objective was the technology control system made in Germany, since the Americans had long put Iran on the blacklist, not allowing the sale of USA technological systems.

[1] http://www.corriere.it/esteri/10_settembre_26/iran-attacco-informatico-guido-olimpio_25e66fea-c99411df-9f01-00144f02aabe.shtml



ICS vulnerabilities since 2001 by Sean McBride[2]

We all know that cyberspace’s borders are no longer well defined and Stuxnet was soon started spreading outside the perimeter of Iranian equipment and national borders. In mid-2011 more than 100,000 infected systems were counted in the world[2], that were starting to damage other equipment around the world, causing interruptions and faults even not far from us: impacts that were also felt throughout 2011, as many infections went unnoticed and probably still do - the operators are entirely ignorant that this "sleeping" APT may be in their system, waiting to be awakened and to cause unexpected and, hopefully, fairly benign displeasures.

And Duqu, is it Stuxnet’s “son”?

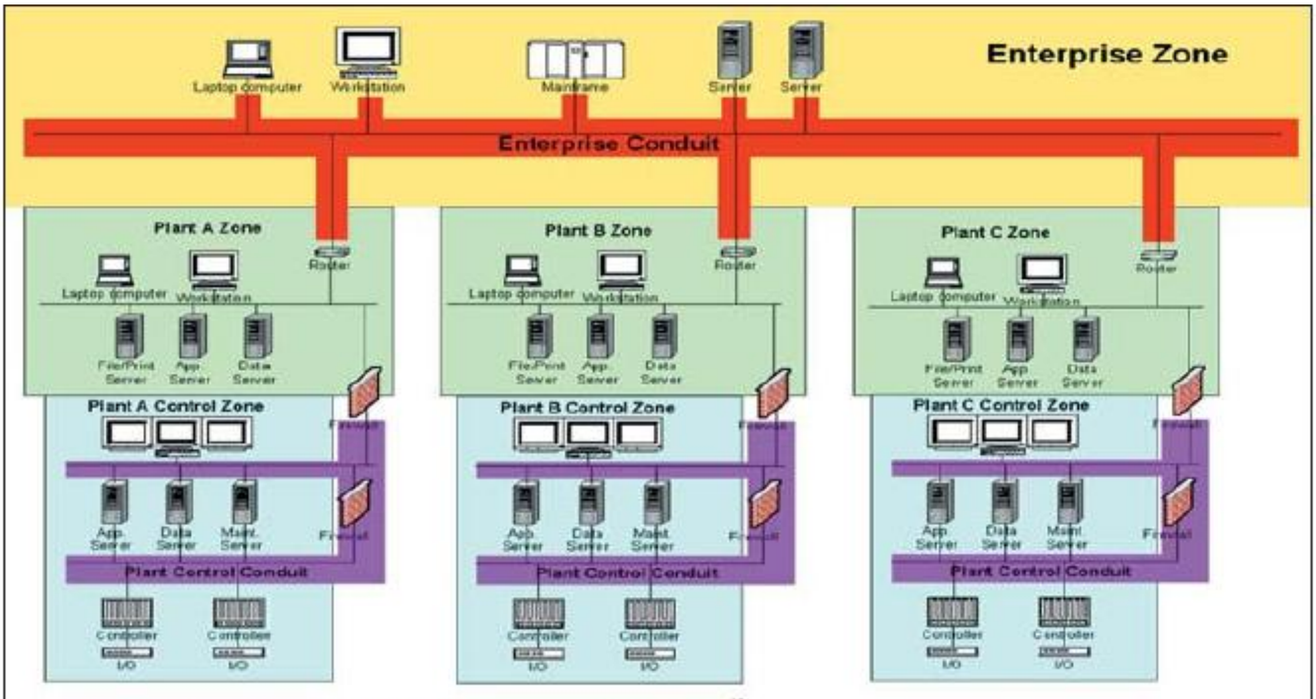
“In the new threat discovered in 2011, called Duqu, the components are nearly identical to Stuxnet’s ones, but the purpose is completely different. As a matter of fact, Stuxnet’s main goal is to affect the logic in the PLC in order to cause damage to the system, while Duqu’s purpose is to gather and steal information that could be useful for aggressors to arrange a future attack against systems, industrial establishments and infrastructures,” said the expert Eric Byres, during a meeting that was held in October 2011 [3]in Milan. What is Duqu’s aim? It is to prepare future cyber-attacks. “It is like Arsène Lupin who wants to understand the model of the safe and of the alarm systems before acting» says Antonio Forzieri, security expert and professor at the University Politecnico di Milano. Aggressors are looking for information such as planning documents that could help them mount a future attack on an industrial structure. This is why Duqu is regarded as the precursor of a possible Stuxnet-alike attack.” (from Corriere.it)[4]

From here, the ultimate awareness that now even control and remote control systems, that have been long ignored from a cybersecurity perspective, could be a desirable target that, if disrupted, could cause large damage, sometimes even bigger than any large data breach of credit card processors. They can stop industrial companies and manufacturing facilities, logistical centres and even aqueducts or operating systems in hospitals.

[2] https://www.critical-intelligence.com/

[3] http://www.tofinosecurity.com/eric_byres

[4] http://www.corriere.it/scienze_e_tecnologie/11_ottobre_19/virus-malware-duqu-nuovo-stuxnet_f7c0c9bcfa52-11e0-81c3-3aee3ebb3883.shtml

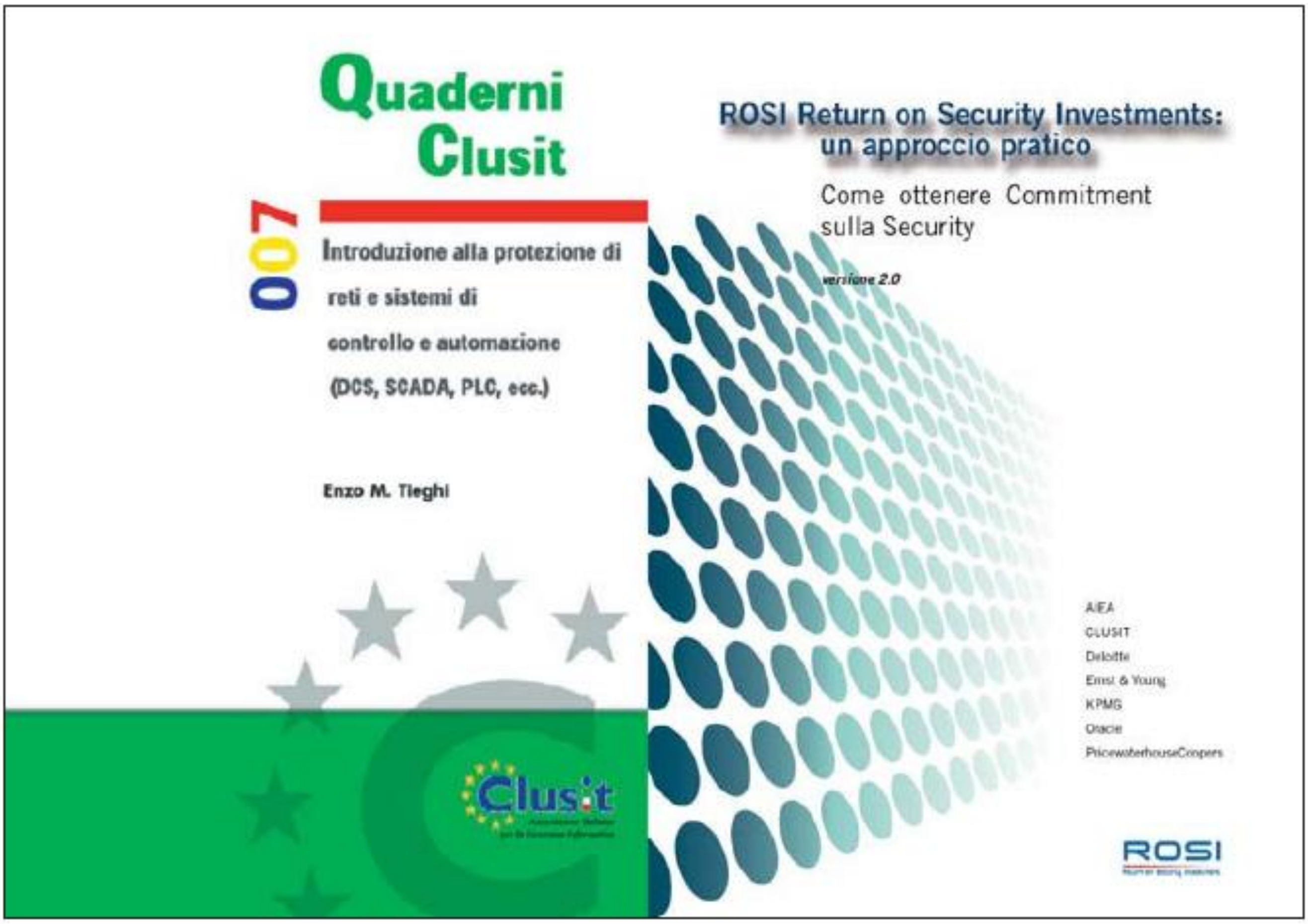


ISA99 Zone & Conduit Model (www.isa.org/ ISA99[5]

How can we protect our systems (and our facilities), then?

In the very conservative industrial world and in control systems, ICT methodologies and technologies are traditionally “ratified” with a few years of delay. People in the world of industrial systems have started discussing cybersecurity at the threshold of 2000 (it is significant to notice that the committee and the relevant standard for the control systems security is called ISA99, the year when it all began[5]). It has now been also released the first IEC62443 standard. There are numerous research and working groups in many parts of the world and in many different sectors that have started new activities to try to identify the best, the most effective and the least expensive way to apply common principles for protecting control and remote control systems.

[5] http://www.isa.org/isa99



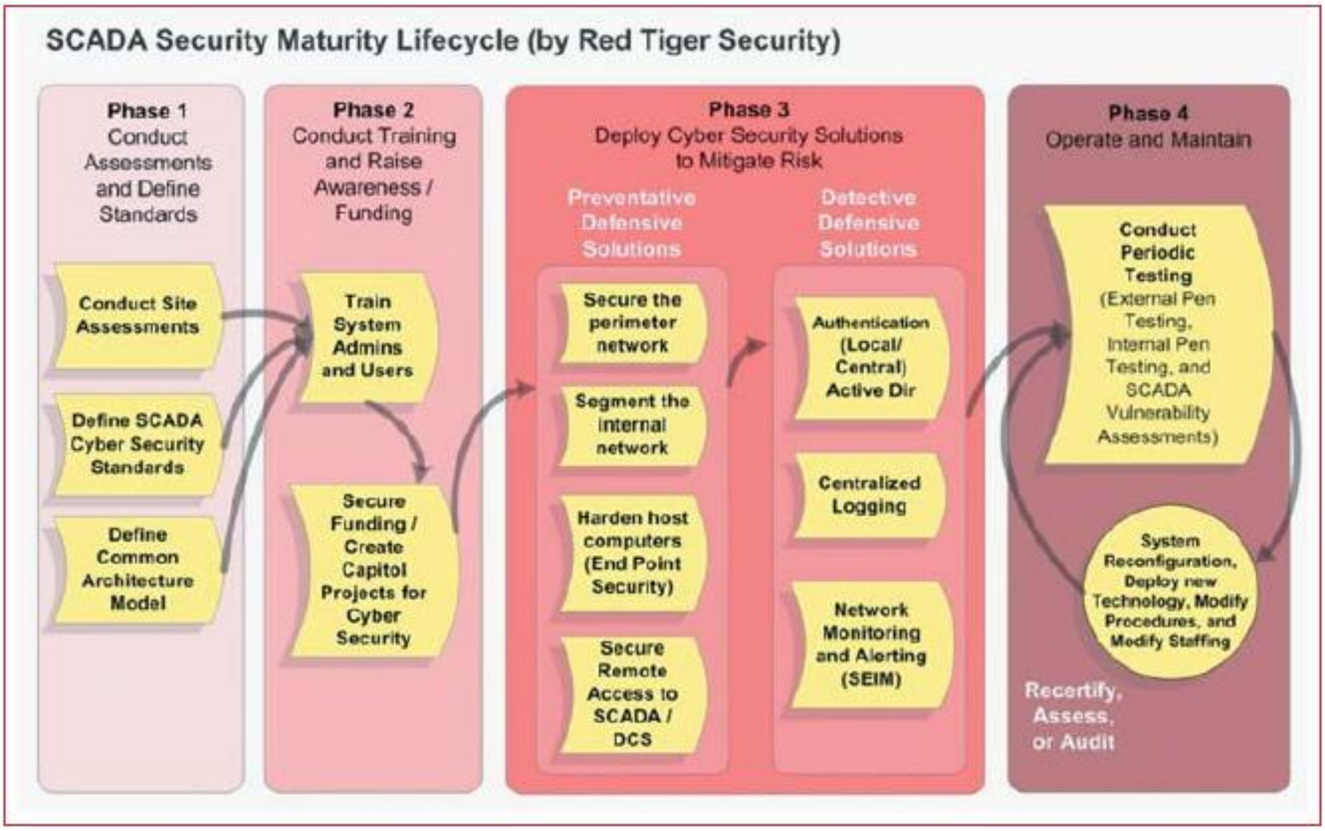
CLUSIT confirmed its institutional sensitivity and its presence in the community even on the issue of industrial systems security, publishing one of its Notebooks (the first one was released in 2007) entitled “Introduction to Network Security and Control and Automation Systems (DCS, SCADA, PLC, etc.)”, available on the CLUSIT website[6]. In 2011, while writing the second edition of the ROSI (Return on Security Investments: a practical approach - How to get Commitment[7]) document, CLUSIT’s working group did not want to evade the issue, including the a chapter on “Industrial Security Assessment”. There are two effective and ready-to-use tools to tackle cybersecurity’s deficiencies in industry and infrastructure, extending the traditional field of IT security systems also to manufacturing systems and control networks of establishments that are useful to the community.

Once we've identified the issues and the potential damage, how can we proceed?

How many times have we heard, were we told or have we said that "security is not a product, is it a process"?
This is even more real when there is not simply “data" to protect, but also "controlled processes" by systems used in factories and other sectors. The purpose of the assessment (including the one suggested by ROSI) and the activity of any remediation is not just about the network, systems and the ICT infrastructure, but it is also about the risks that, as we have already mentioned, may causes production and service delivery interruption, taking into account all the interdependencies that there may be: without electricity computers and communications do not work, but without computers and communications we are unable to produce and distribute electricity, we cannot have water, trains, planes, hospitals and traffic lights do not work.

[6] http://www.clusit.it/download/index.htm
[7] http://rosi.clusit.it/

This is why there is now the need for new professional figures, with specific expertise, and for new technologies and products that are specifically designed and produced for the "hostile" environment where these systems must work, in hot, cold, dusty, humid, vibrating, and low-maintenance environments, that are not "normal" conditions in traditional datacentres. Where systems cannot be stopped for an upgrade of the operating system or the antivirus, for a reboot, to install a patch, to change a configuration parameter, because the system must carry on operating and producing until a scheduled downtime planned well in advance, scheduled for next summer or between Christmas and New Year; in any case, never soon enough.


SCADA Security Maturity Lifecycle (by Red Tiger Security)

Phase 1
Conduct Assessments and Define Standards
Conduct Site Assessments
Define SCADA Cyber Security Standards
Define Common Architecture Model
Phase 2
Conduct Training and Raise Awareness / Funding
Train System Admins and Users
Secure Funding / Create Capitol Projects for Cyber Security
Phase 3
Deploy Cyber Security Solutions to Mitigate Risk
Preventative Defensive Solutions
Secure the perimeter network
Segment the internal network
Harden host computers (End Point Security)
Secure Remote Access to SCADA / DCS
Detective Defensive Solutions
Authentication (Local/ Central) Active Dir
Centralized Logging
Network Monitoring and Alerting (SEIM)
Phase 4
Operate and Maintain
Conduct Periodic Testing (External Pen Testing, Internal Pen Testing, and SCADA Vulnerability Assessments)
System Reconfiguration, Deploy new Technology, Modify Procedures, and Modify Staffing
Recertify, Assess, or Audit

Awareness of these issues brings us to a model of "SCADA Security", which evolved according to the Maturity Model, with all the steps that have to be done at the level of policy, personnel, training, procedures, countermeasures, architectures, testing and verifications: the one shown here, for example[8], was thought up by the international expert Jonathan Pollet, of Red Tiger Security, who held a crowded conference in Rome in 2011, as well as giving an advanced course that explained how to protect control systems in order to deal with the most violent and sophisticated techniques designed to damage networks, systems and the controlled establishments.

What will be the answer of the Italian market in 2012?

As we have already seen, there is still much to do. If 2011 was the year of awakening and awareness, what we expect from 2012 is the begin of new specific activities to protect networks and security systems in factories and infrastructures. Uncoordinated investments in the IT Security field or a prompt installation of firewall between the "Process Control Network" and the "Enterprise Network" with adjoining DMZ as suggested by ISA99 (7) model are not enough. We need real initiatives (and financial support) to address any issues that could generate accidents to networks or control and remote control systems. Skills, methods, technologies and products are available, as they are used in many countries, also in Europe, that are already expert on industrial cybersecurity.

[8] http://www.redtigersecurity.com/scada-security-lifecyle/

We expect a sharp increase in interest not only by industries, where the product costs money, but by those charged with the protection of people and of the environment who may be the most effective drivers also considering the coming into effect of sector and implementation standards in Italy – for example the EU directive 2008/114/EC[9] that lays down conditions and obligations for operators of the European critical facilities, in the sector of energy, communications, transport, and soon in many other areas that affect our everyday lives.

[9] http://www.infrastrutturecritiche.it/aiic/index.php?option=com_content&view=article&id=249:workshop- aiic-considerazioni-sulla-applicazione-operativa-della-direttiva-2008114ce&catid=122:convegni&Itemid= 118

ICT Security Situation in the Italian Small and Medium Enterprises

By Claudio Telmon

Preliminary remarks

Talking about the ICT security situation in the Italian small and medium enterprises is not trivial, as many businesses belong to this category. They range from craftsmen, professionals, brokerage firms, the pharmaceutical industry, fashion industry, medical laboratories and ICT service industries. They are all too different to be analysed homogeneously, and it would not even be useful in this context. Some of these SMEs look more like households and they use the Internet for little more than bookkeeping. Others work in such a context where security is a critical aspect of their industrial culture and subjected to a set of rules. These extreme contrasts, that for better or for worse merge in the Italian scenario, are not considered in this analysis unless expressly said. The company took as example has at least four or five employees, tens of systems distributed in no more than three branches/offices and with regular security requirements. It does not mean that there is no need for protecting intellectual property or that possible violation would create huge damage: the companies analysed need to use information security tools extensively and on an advanced level, like the insurance or pharmaceutical industries, but do not work for ICT security firms.

General comments

The ICT security situation in the Italian SMEs is often perceived as poor, because the businessman often has a disinterested and ignorant attitude towards security. This idea, which has been powered by clichés and comparisons with other realities in the insurance or banking sectors, does not give enough credit to the improvements and countermeasures seen in recent years. Recent analyses, for example the Assintel study of the e-security project, talks of enterprises with heightened awareness that are beginning to realise how important information and systems are. Awareness which implies more care for some IT security aspects, such as the possible drawbacks of connectivity and data loss. Compliance with the laws on personal data treatment, which recently led a great deal of security markets and not only for SMEs. However, SMEs seldom chose the right countermeasures, though, nor pay enough attention to the offers of the market.

Risk awareness

Italian SMEs are slowly becoming aware of the role of information systems and tools in support of their business activities. If this awareness is still far from being obvious and strengthened, it is however true that fewer companies feel they you can still work without a computer, a common idea until a few years ago. Companies know well that data or system disruption can lead to unease and significant damage. Regarding malware, the attention appears to be more focused on disruptions rather than on more dangerous consequences, such as the theft of credentials or access to confidential data. The focus on external threats is modest, whereas, on average, the risk awareness related to internal threats is higher. This last point is justified by the fact that when the personnel is perceived as a source of potential threats, the problem is not limited to the information systems, and the attention to ICT risk stems here from the risk awareness in more "physical" areas. In these cases, indeed, the information problem is often seen as marginal if compared to the overall staff reliability.
The result is a framework in which information tools are more seen in a "traditional" risk perspective that comes from physical damage (poor functioning, data loss etc.), whereas information risks, such as industrial espionage and others related to unauthorised access to systems, are not generally perceived. The most common reason is that there is no evidence of significant impacts or events associated with this type of risk. There are little to no statistics on damages to Italian SMEs after abusive access, in fact there are often foreign studies on big American enterprises, not entirely relevant to the Italian SME context. Nevertheless, Italian SMEs do not

appear to be concerned with frauds as they trust in procedural controls, such as authorisation processes for economic transactions, and they generally believe that a prowler would not bother following so many steps to access their sources via an information attack. They often do not know about similar attacks performed to fellow businesses. This is an evaluation of risk that can remind us of the concept “if it hasn’t happened to anybody yet, I don’t think I’ll be the first”, a very common thought whose application justified the delay in the adoption of security measures for personal data treatment until the threat of conformity audits on business. In front of the objection that information attacks may not be attributed- as in cases of intellectual property theft, the answer is that it is an exaggerating precautionary actions as no data on SMEs is available. Such idea do not stem from the an accurate analysis of the issue but it is part of the process in which unperceived risks are not taken into account.

A separate discussion regards personal data treatment. As already said, personal data treatment is the driving force that brought information security to SMEs and not only, if we think that when talking about security the attention moves to personal data and minimum measures and not on the industrial information archives.

Finally, SMEs count on outsourcing services, even cloud for e-mail accounts and websites, and often rely on providers located outside Italy or the EU to find offers. The use of large international e-mail hosts is common and when choosing vendors, even in case of personal data or e-commerce websites, cost analysis and service quality prevail over security and conformity.

The result is that SMEs consider ICT risk as marginal because they have no evidence of significant impacts and therefore they do not understand the issue. There are exceptions in those areas where the chance of damage is supported by negative events that happened to their peers, like data loss, malware in the systems or no conformity to the personal data treatment regulations.

Security management

Most SMEs do not have IT systems managers, they rely on professionals or small specialised businesses which often correspond to the hardware or software supplier, or they simply turn to the shop or retailer where they buy their PC. Sometimes, when a person inside the company has IT skills, he deals with ordinary tasks, and the more complex activities are carried out by external providers. ICT security is generally delegated to the suppliers that generally choose the method of risk assessment we talked about in the previous section.

Considering the high number of SMEs in Italy, we rely on these small providers. The businessman can hardly give assessments and, since there is no law that sets specific skills or qualifications to practice this activity, everybody can work in the sector even with limited abilities, the current common skills are various but limited. Competition is often a matter of costs and perceived quality, in terms of time of intervention and prices. The results from an IT systems management point of view is that security capacities in particular, are varied but poor.

In addition to this, we must add that the products offered to small enterprises are often low-quality because they have to be affordable, especially regarding software. For instance, small businesses programs often requires simple features and yet they are restrained by shoddy software limited functionality. At the same time, outsourced online services can have vulnerabilities only because security was not managed by skilled personnel.

To complete the framework, the bad relationship between businessman/personnel and information has to be considered as it seems that on the one side there is a refusal to understand the fundamentals of the topic, on the other side a common resignation that problems just “happen” and nothing can be done to avoid them.

Security is adequately managed when a company luckily has a skilled and aware supplier; in the other cases, security is confronted in the limits of what is needed to avoid enormous problems or management difficulties.

There is a glaring difference between the businessman's risk awareness on how the risk is handled and the current security management situation. This data also emerge from the above-cited Assintel study.

Despite this, the security situation of Italian SMEs has improved over the past few years, thanks to the imposition of regulations on the treatment of personal data. Antivirus solutions are commonly used, though not evenly or frequently kept updated. Passwords and centralised data storage on business servers is also widespread, even if the habit of storing information on laptops or any other mobile systems remains, and the same is true of the installation of security updates to the operating systems. Backup systems are often activated, for servers especially, but inadequate overall with copies being made too infrequently or stored insecurely without testing the restoration possibilities ahead of time. Finally, wireless access to the business network are mostly protected, but this comes from default secure configurations of the machines distributed by suppliers and not because of an aware choice from the business.

These security measures originates from two main requirements, mentioned above: the conformity to regulations on personal data treatment and protection against major issues such as data loss or system breakdown and service interruption.

Alongside these improvements, there are still uncertainties due to a general feeling of comfort and not poor choices made by decision makers, and not due to a lack of investments. Common examples are the resources shared on the local network with no reasons, which can make authentication mechanisms redundantly useless and facilitate the spread of malware, or the fact that operating system's elements are not regularly updated. Smaller enterprises usually use NAT or automatically configured mechanisms to protect their systems against unauthorised access, whereas firewalls are rare and can be found in big firms with more pressing requirements.

Security policies, the core of personal data treatment rules, are often carried out through open requests from the privacy consultant, a very common profession by now. Outside what is strictly asked by the regulations, the attention of system usage is widespread only for business purposes.

The reason is twofold: on one hand, the attempt to avoid legal problems, for example, when there is the need to access to data on the PC or to an employee's e-mail account. On the other hand, and this is an interesting point, awareness that systems used only for business purposes are, on average, less prone to malware, and thus more reliable and require less maintenance is becoming common knowledge. Security policies, however, are rarely written, except when required by legislation, and, as the Assintel study confirms again, often they are not very clear even to employees.

Security tools

As can be imagined from the explanations above, the use of security products or the request of specialised skills are limited in the Italian SMEs. From the product point of view, the only widespread exception are antivirus solutions. If, today, it is common to find updated antivirus solutions in small enterprises, we should not forget that until a few years ago it was the exception. Firewalls are way behind. The remaining security products and services have a low circulation and SMEs are not interested in them at all, except in the larger SMEs or in case of very specific needs. The activation or configuration of security measures embedded in commonly used tools, like authentication features at the operating system level , the security options of connection systems, or the activation of antivirus and antispam mechanisms offered by the e-mail account provider is more common. Even in this context, if we dismiss those mechanisms with evident effects like antispam, activation and configuration depend on the awareness of the personnel that manage the information systems, as the businessman himself can hardly evaluate the management quality and the trust relationship that is necessary between who handles the system and the company.

Conclusions

Slowly but surely, ICT security management in the Italian SMEs is getting better. In the past years, the driving force was a desire to conform to Italian regulations on the treatment of personal data. But the awareness of the role of information security tools is increasing as well in order to provide the continuity of business activities. The risks perceived by SMEs are primarily inefficiencies due to system breakdowns and malware. This risk awareness is confirmed, or better, is not denied, by the absence of studies that show the importance of other security information risks for Italian SMEs.

The low request for ICT security professionals in Italian SMEs means security management is still far from adequate, except where specific needs or the "chance" availability of major in-house competence, leading to better system management and, consequently, better security.

CLUSIT Report 2012, the Authors

Mr. Luca Bechelli – He has been an independent consultant in the information security field since 2000, a subject that he also teaches at the University of Pisa, for the Master in Internet Technologies. Together with partner companies, he runs an advisory service for national and international projects on topics such as Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling, as well as taking part in the planning stage and in project management for system integration activities. He also practices R&D activities with companies in the field of security and through collaborations with research institutions. He is co-author of scientific and technical/popular publications. Since 2011 he has been a CLUSIT associate and since 2007 a member of its Board of Directors, as well as of the Technical and Scientific Committee. He also took part, as a professor, in many CLUSIT Education workshops during the Security Summit.

Mr. Matteo Cavallini – He has been working in the field of information security for more than 15 years for both private companies and governmental institutions. He is currently Head of the MEF/Consip Security Local Unit's Operating Structure, Ministry of Economy and Consip's internal CERT, as well as being vice president of the Cloud Security Alliance. In the past, he also worked on Gov-CERT.it (now CERT-SPC) projects at CNIPA and he was in charge of the parametric security at Consip. While working at CNIPA, he also served as security senior expert for the Testing Commission of the Public Connectivity System's security services. From 2000 to 2004, he had been IT Security Manager in Consip, realizing some of the most critical projects from an information security point of view. He is certified as EUCIP Security Adviser and Lead Auditor BS7799.

Mr. Raoul Chiesa – He discovered the TLC world in 1986 and since 1997 he has started operating professionally in the ICT Security sector. Raoul has been the first Italian ethical hacker and, together with Daniele Poma of @Mediaservice.net, he is a charter member of the vendor-independent company specialized in performing security tests. In 2000, at the request of professor Danilo Bruschi, he became a charter member of CLUSIT and has since also joined the Board of Directors. In 2003, he also became a member of ISECOM's (Institute for Security and Open Methodologies) Board of Directors. During the same year, Raoul also started his collaboration with the United Nations agency, UNICRI, where he is currently an "Independent Senior Advisor on Cybercrime". Since February 2010 he has been a member of ENISA Permanent Stakeholders Group, the European Agency for information and networks' Security. Raoul is also author of many publications and supervisor during important national and international events. More recently, he joined Cyberdefcon Ltd. and Jart Armin's team at HostExploit, and established a new think-tank, "The Security Brokers", working globally as an InfoSec facilitator.

Mr. Mauro Cicognini – In 1995 he got his degree in Electronic Engineering at the Politecnico University of Milan (major in Biomedical Engineering, from a personal passion for neuroscience). He then worked for a long period in the technical field, first as an expert and consequently as manager in different companies, operating in the sectors of services and high technology (software system integration, telecommunication, industrial automation). Between 2001 and 2006 he built up a team of advisors for Siosistemi S.p.A., expert on legal compliance and international standards (Privacy, ISO 9000, ISO 27000). After having worked as a manager in the commercial and marketing field at I.NET S.p.A. and at BT Italia S.p.A., he is now dedicating to executive advisory. He is member of CLUSIT's Board of Directors, of its Technical and Scientific Committee, as well as being coordinator of CLUSIT's Educational workshops.

Mr. Gabriele Faggioli – He is a lawyer and a partner at ISL, a company specialized in legal, contractual and management advice. He is a Counsel at the ISL law firm ad member of Politecnico University of Milan's faculty –. His main areas of specialization are computer and telematic contracts, information & telecommunication law, intellectual and industrial property law, as well as legal aspects concerning information security, publishing and marketing law. He is member of CLUSIT's Board of Directors. He published several books and many articles on these topics and he was supervisor at many workshops and conventions.

Mr. Paolo Giudice – He is the Secretary General of CLUSIT. During the 80’s and the 90’s he did some advisory activities as an expert in business management and financial risks. The evolution of the IT sector which highlighted the existing shortcomings in the field of Security, pushed him into the information security world and in July 2000, together with a group of friends and colleagues, he founded CLUSIT. From 2001 to 2008, he coordinated the Committee of Infosecurity Program Italy and since 2009 he has been coordinating the Scientific Committee of the Security Summit event. Paolo is also a partner of C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) of Geneva and a member of CLUSIT Switzerland Board of Directors.

Mr. Antonio Ieranò – He is a European Security Consulting Systems Engineer at Cisco Systems. Having a passion for blogging, he has been dealing with information security for more than 10 years. In particular, at Cisco he analyses the European landscape concerning information security and threats. Antonio has a wide knowledge of IT technologies and of products or issues linked to security, from both technical and legal points of view. Before working for Cisco, which he joined via Cisco's acquisition of IronPort in January 2007, he was in charge of various European offices of Symantec.

Mr. Giovanni Manca – He has a degree in Electronic Engineering and in 1985 he started dealing with issues linked to ICT security and with the deployment of the first telematic services in Italy. Since 1999 he has been working in the public administration of the structures created for technological innovation that, later on, became DigitPA. In this context, he dealt with the sector of digital identification technologies (at the international level), such as the electronic ID cards, the Italian health insurance card, the digital signature and, generally, for ICT security.

Mr. Paolo Passeri – He has been dealing with information security for more than 10 years. His interest in this subject began after his degree in Physics at the University of Milan and it was fulfilled thanks to numerous experiences as advisor and in project management for different system integrators. He is currently CTO and Business Developer at Business-e, an Itway Group company, where he performed some advisory services and realized security projects for TLC operators, Public Administrations and important bank groups. His area of expertise covers the entire matrix of information security, focusing on security problems generated by new technologies and concentrated on mobile security and social networks.

Mr. Mario Salvatori – He is editor-in-chief of the monthly magazines *AziendaBanca* and *Assicura*. He is married with one daughter and holds a degree in Political Science. He is a journalist since 1980 and has a passion for distributive, organizational and technology innovation in the financial sector and he is curious to discover new forms of media.

Mr. Claudio Telmon – He has been a freelance consultant in the field of security for nearly 15 years. He managed the security laboratory of the IT department of the University of Pisa. Later, he continued to work with the department for activities such as teaching and research, focusing on the field of risk management. He has worked as a professional in varied technological and organizational aspects, working for companies in the financial sector, in the telecommunication sector and with public administrations. He is a member of CLUSIT's Board of Directors, of its Technical and Scientific Committee, as well as being founding member and member of AIPSI Board of Directors.

Mr. Enzo Maria Tieghi – For more than 25 years, he has been taking care of software for automation and control systems, security and compliance to standards and regulations across different industrial sectors in which he operates. He is CEO at Servi Tecno srl. He gives lectures and takes part as a speaker at specialist events both in Italy and abroad, and contributes with articles and experiences to trade magazines and international conferences. He is author of the CLUSIT Notebook "Introduction to network security and to control and automation systems (DCS, SCA-DA, PLC, etc.)”. He edited the Italian edition of the book "SCADA Security Good Practices for the drinkable water sector" for AMGA Foundation and Franco Angeli Editions. He is member of AIIC's Board of Directors, of the Sistemi Informativi Study Group in AFI, as well as an ISA Information member of the ISA99 Committee and of ISPE-Gamp Italy.

Mr. Alessandro Vallega – He has been working for Oracle Italy since 1997 as Project Manager in ERP and in the information technology sector since 1984. He is Business Development Manager and responsible for Governance Risk and Compliance, Database Security and Identity & Access Management. In addition, he is coordinator of the Oracle Security Community, as well as an editor or team leader of multiple books, such as: "ROSI Return on Security Investments: a practical approach", "Electronic Health Record: the role of technology in data protection and security", "Privacy in the Cloud: the challenges of technology and personal data protection for an Italian company" and "Mobile Privacy: formal performances and security measures for the processing of personal data compliance within the company". He also contributed to the first 2012 CLUSIT Report on ICT Security in Italy. He is member of IAEA, CSA Italy and of CLUSIT'S Board of Directors.

Mr. Andrea Zapparoli Mazoni – Since 1997, he has been dealing with ICT Security, Cybercrime and Cyber warfare, taking advantage of his multi-disciplinary background in both Political Science and Computer Science. Over the years he has been involved in GRC, Identity Management, Data Loss Prevention, Security Intelligence and Vulnerability Management in Enterprise, Industrial and Public Administration environments. Andrea is CEO of iDialoghi and a trusted advisor for national and international organizations. He works closely with CLUSIT, holding workshops (SCADA and Social Business Security), taking part in Security Summits and in the editing of documents (FSE, ROSI v2). For the 2012 CLUSIT Report, he is the author of Focus On "Social Media Security", as well as the editor of the sections relating to trends and the analysis of major international incidents. He recently founded, along with Mr. Raoul Chiesa “The Security Brokers”, a global think-tank and high-level security consulting company.

ACKNOWLEDGMENTS

CLUSIT and Security Summit would like to thank the authors, the organizations and everyone who contributed to 2012 Clusit Report publication.

In particular, thanks to: @Mediaservice.net, ACE European Group, ADP Italia, ADS, Akamay Technologies, Alba, Almaviva, Assintel, Business-e, Cisco Systems, Cleis Security, Clusif, Colt Telecom, CRAG Partners, Deloitte, Euro Informatica, Future Time, iDialoghi, IBM, IFOA, Innovery, Ireth, Italia Lavoro, McAfee, Neonevis, Net 1 di Fornaro Natale, Omnitech, Oracle Italia, Oracle Community For Security, Panta Ray, P.D.C.A., PrivateWave, Programatic, Safenet Italy, Selex Elsag, Sonic-Wall, Spike Reply, Systemeng, TAI Software Solutions, Trend Micro, VEM Sistemi, Xech, Zeropiù.

But also to: Carlo Junior Accettella, Davide Alaimo, Stefano Amadori, Gianluigi Angotti, Maria Antonietta Aniballi, Davide Aprea, Andrea Ardizzone, Orlando Arena, Marco Babbei, Mario Ballerini, Giuseppe Bartone, Luca Bechelli, Giovanni Besozzi, Paolo Borghesi, Nicola Bressan, Danilo Bruschi, Marco Bubani, Fabrizio Bugli, Giancarlo Butti, Francesco Buzzoni, Cristiano Cafferata, Matteo Cavallini, Aldo Ceccarelli, Daniela Cembi, Amedeo Chiappini, Raoul Chiesa, Marco Ciampi, Mauro Cicognini, Fabrizio Cirili, Ombretta Comi, Corradino Corradi, Franco Corsetti, Maurizio Corti, Claudio De Paoli, Gianna Detoni, Lisa Dolcini, Elenio Dursi, Cinzia Ercolano, Cristian Ercolano, Gabriele Faggioli, Mariangela Fagnani, Valentina Falcioni, Alessandro Feltrin, Tiziano Feraco, Sergio Fumagalli, Ivano Gabrielli, Cesare Gallotti, Domenico Garbarino, Loredana Gazzaniga, Lorenzo Grillo, Antonio Ieranò, Alessandro Lega, Pascal Lointier, Vito Losacco, Matteo Maino, Wilmana Malatesta, Gianluca Manariti, Giovanni Manca, Alberto Manfredi, Massimiliano Manzetti, Stefano Marsani, Raffaele Mazzitelli, Stefano Mele, Lorenzo Migliorino, Matteo Meucci, Francesco Miraglia, Marco Misitano, Mattia Monga, Annalisa Morandin, Roberto Obialero, Roberto Pachì, Paolo Passeri, Alessio Pennasilico, Fabio Pietrosanti, Daniele Poma, Isabelle Poncet, Stefano Quintarelli, Stefano Rosso, Andrea Rui, Mario Salvatori, Luca Sambucci, Roberto Sarra, Giampaolo Scafuro, Riccardo Scalici, Sofia Scozzari, Maurizio Spelta, Valentino Squilloni, Walter Summonte, Gigi Tagliapietra, Paola Tamburini, Carla Targa, Claudio Telmon, Enzo M. Tieghi, Francesca Tolimieri, Maurizio Tosti, Alessandro Vallega, Giovanni Battista Vassallo, Francesco Vecchione, Maria Gaia Vinciguerra Frezza, Francesco Maria Vizzani, Silvio Zaina, Giovanni Zanetti, Paolo Zanotti, Andrea Zapparoli Manzoni.

A special thanks goes to the Postal and Communications Police and to its director, Mr. Antonio Apruzzese.

CLUSIT was born in 2000 at the Department of Information and Communications of the University of Milan. It is the most numerous and influential Italian association in the field of information security. Today, it represents more than 500 organizations from all sectors of the country.

Aims

- Raise the computer security culture among Companies, Public Administrations and common citizens
- Participate and contribute to the development of laws, practical codes, and correct behaviours in computer security both at the national and European levels
- Contribute to the definition of learning programs and of certifications for computer security experts
- Promote the adoption of methodologies and technologies which can contribute to the improvement of the security level of the information infrastructure at all levels.

Activities and ongoing projects

- Specialized training: CLUSIT workshops
- Professional certifications: CISSP and CSSLP courses and exams
- Research and studies: “Information Security Innovation” award for the best University thesis
- Specialized conferences: Security Summit (Milan, Rome and Verona)
- Technical-scientific documents: CLUSIT Notebooks
- ROSI: a method for assessing the return on investment in information security
- “IT risk and small businesses” project, dedicated to all small and microenterprises
- YouTube CLUSIT channel: ICT security in short videos
- School Project: on-site Training
- CLUSIT Reports: annual report on damaging events (Cybercrime and information accidents) in Italy; the analysis of the ICT Security market in Italy; labour market analysis.

CLUSIT institutional role

At a national level, CLUSIT collaborates with: Presidency of the Council of Ministers, Ministry of Interior, Ministry of Justice, Ministry of Defence, Ministry of Economics and Finance, Ministry of Economic Development, Postal and Communication Police, *Arma dei Carabinieri*[10] and *Guardia di Finanza*[11], Authority for personal data protection, The Communications Authority, Universities and Research Centres, Professional and Consumers Associations, *Confindustria*[12] and *Confcommercio*[13].

[10] The national military police of Italy

[11] The Italian law enforcement agency under the authority of the Minister of Economy and Finance and part of the Italian armed forces

[12] The Italian employers' federation

CLUSIT international relations

At an international level CLUSIT takes part in numerous initiatives in collaboration with: CERT, CLUSI, Universities and Research Centres in more than 20 countries, DG Information Society of the European Commission, ENISA (European Network and Information Security Agency), ITU (International Telecommunication Union), OCSE (Organisation for Economic Co-operation and Development), UNICRI (United Nations Interregional Crime and Justice Research Institute), Professional Associations (ISACA, ASIS, CSA, ISCC, ISSA SANS) and Consumers Associations.

[13] The Italian federation of all actors in the field of trade, tourism, services and professions

The Security Summit is the most important Italian appointment for people with a keen interest in information system, network security, and information security.

Organised in response to today's professionals needs, the Security Summit is a convention that offers participants the opportunities of examination, knowledge sharing and education.

Open to international experiences and to trends coming from within industry, university and research, the Security Summit turns to security professionals and people dealing with organisational and legal pertaining to ICT security.

Admission is free, after online registration.

The Security Summit is managed by CLUSIT and CEventi, the conference division of the publishing house Cardi Editore that organises events on finance and ICT.

Teachers and speakers

Over 250 teachers, speakers, lectures, businessmen and professionals took part in the past Security Summit editions.

Attendees

During the first three editions of the Secuirty Summit over 5,000 people joined us and about 3,000 certificates of attendance were released providing CPE and 350 diplomas.

Edition 2012

The following edition of the Securtiy Summit 2012 will be held in Verona on October 4th, 2012.

Information

Website: https://www.securitysummit.it/

Agenda and contents: info@clusit.it, +39 349 776 8882

Other information: ceventi@cardieditore.com, +39 02 6710 1088