Funded by the European Commission

Seventh Framework Programme

CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D5.3 - Best Practices Analysis Document

Date of deliverable: 30 / 09 / 2015
Actual submission date: 30 / 09 / 2015

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.0

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	no
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	✓

Revision history

Version	Object	Date	Author(s)
0.1	Creation	23 Jan 2015	MELANI
0.2	Revision	4 March 2015	MELANI, SM
0.3	Revision	23 April 2013	MELANI, SUPSI
0.4	Revision	4 May 2015	MELANI, SM, SUPSI
0.5	Revision	11 May 2015	NASK, MELANI
0.6	Preliminary review	20 May 2015	SUPSI
0.7	Revision	26 May 2015	NASK, CYBERDEFCON
0.8	Review	28 May 2015	MCAFEE
1.0	Final preliminary document submitted	30 May 2015	CYBERDEFCON
1.1	Additions	14 August 2015	MELANI, PosteIT, CERT Poland, Vitrociset
1.2	Additions	22 September 2015	MELANI, INOV
V11	Prelim edit	23 September 2015	CYBERDEFCON
FINAL	Review & final doc		INOV, CYBERDEFCON

D5.3 Best Practices Analysis Document

Responsible
MELANI

Contributor(s)
INDRA
SM
INOV
NASK
PJ
CEFRIEL
SUPSI
CYBERDEFCON
HMoD

Reviewer
INOV

Summary:

‘Best practices’, within the realm of cyber security, can be interpreted in a multitude of ways. In the preliminary report for D5.2, a review of the methodological problems was carried out. Now, for D5.3, the research focus concentrates on three different approaches to the issue: organisation, technical, and people/consumers. Beside the extensive literature review to be found in each section, the report makes two notable original contributions about ‘people-centred’ best practices. It does so via newly collected data. Firstly, a survey carried out exclusively in one European participating country shows the perception of cybercrime there, and how this compares to other statistics in general. This analysis highlights the need for heeding cultural differences when designing ‘best practices’. Secondly, the project investigates, via a survey, how the cyber security professionals currently implement ‘best practices’. Results tended to confirm the view that the organisations, which perceive that cyber-attacks present substantial threat, are most likely to invest heavily in cyber security solutions and to implement a wide range of solutions across a greater range of possibilities. The project concludes by investigating a few possible future developments for the ‘best practices’ in cyber security.

Keywords: best practices, methodology, critical infrastructure, SWOT, cybercrime, current and future practices, survey

TABLE OF CONTENTS

Introductory Remarks

1 Research Question

‘Best practices’ is a term which, although often branded around, is difficult to be narrowly defined. To some, it may come as a straight truth, almost as part of common sense, which — when this common sense is patently not being applied — brings about the question: how was this practice left unchanged for so long? A case in point is with a bank fraud happening in late 1978 – probably one of the earliest cases involving computers:

At that time, the Security Pacific National Bank was issuing every day a new code to its bank officers. The bank officers would have to give the code to the wire room in order for their transaction to perform successfully. Mark Rifkin, a then 32-year-old computer consultant, was passing almost every day by the wire room to check on their systems. And during his coming-and-going, he noticed that the clerks in the wire room would merely write the new verification code on notices. On 25 October 1978, he read the daily password while making other operational procedures due for the day. He then exited the building, phoned the wire room pretending to be a bank officer, gave the clerk the correct code, and proceeded to wire $10.3 million.[1] The bank did not even notice the fraudulent transaction before the Federal Bureau of Investigation contacted them to verify their books on suspicions that they had had based on an unrelated large purchase of diamonds.[2] Rifkin was eventually arrested on 6 November 1978, and sentenced on 26 March 1979 to eight years in prison.[3]

It is nowadays a common sense that writing a password on a notice is bad practice. Informed by many similar cases, our collective conscience seems to have evolved to the point where we now judge this idiosyncrasy as plainly ‘stupid’. But it was not always the case, and this incident fleshes out a few important questions to consider:

How can we define the ‘best practices’? How do they evolve and are they really such ‘universal’ truth? Can we assess what will the ‘best practices’ look like in the future?

Reviewing all ‘best practices’ in the field of cyber security is a large-scale research activity that for sure goes far beyond the framework of the CyberROAD project. From here on we will restrict ourselves to particular points of interest or concern. The limitations of the report stem mainly from the wide variety of meanings that the term ‘best practices’ in cyber security can imply. This alone suggests that even an overview of this topic may point to several research gaps in this area.

Operators of industrial control systems, banks or even social media websites all cherish different aspects of security (e.g. the confidentiality of personal information is perhaps more important to a bank than to Facebook) and have a different understanding of the term ‘best practice’. A crucial viewpoint, too, should belong to the consumer, which is sometimes hidden beneath the need for entities to attain compliance. Best practice, after all, should be of benefit to the end-users, as well as the organisation implementing the process — via a top-down approach which, in terms of cyber security, contributes to the protection of the consumer from products or services that are not fit-for-purpose.

[1] Bill Gardner, 'AM cycle', *The Associated Press*, 3 November 1978.

[2] The Washington Post, 'Bank Was Unaware of Swindle', *The Washington Post*, 11 November 1978.

[3] Facts on File World News Digest, 'Rifkin Sentenced in Bank Theft', *Facts on File World News Digest*, 30 March 1979.

This report is split into three parts, each with subsections.

The first part covers organisations and is split between critical and non-critical organisations. It concerns different initiatives launched within these domains.

The second part delves into two technical approaches, also for organisations (mainly businesses) to tackle with 'best practices' of cyber security.

The third part considers the human as the central point which the 'best practices' need to affect. More specifically, it will review a specific and practical example of what 'best practices' mean for cybercrime in Poland – a country represented in this consortium by CERT. Furthermore, based on a conducted survey, the report will also investigate what different types of organisations currently apply and regard as 'best practices'. It will notably focus on interpreting what may have influenced their choices.

This research report is concluded by forecasting the direction in which the 'best practices' seem to be heading.

2 Methodological considerations: what constitutes ‘best practices’?

There are plenty of standardisation agencies in the field of cyber security and related issues, publishing what they brand as ‘best practices’.[4] Yet there has been little critical reflection on definitional and methodological issues the term may raise.[5] From a cursory look, it is uncertain if they constitute opinions (even concerted ones), or have a proper scientific value to account for. ‘At best, “best practices” are best guesses’ as an academic article unrelated to cyber security suggests.[6] If this view is taken as being an accurate reflection, the practical value of identifying ‘best practices’ can be next to zero. However, the way research is conducted can have important implications as to whether the outcome is only a ‘best guess’ or is supported by evidences.

Generally conceived, “best practices” aim at improving performance (e.g. the cyber security posture of an organisation) by identifying and codifying factors which have achieved the sought results in another environment. A more formal definition can be put as such: it is ‘the selective observation of a set of exemplars across different contexts in order to derive more generalisable principles and theories of management’.[7] Often, documents showcasing ‘best practices’ are rather in the form of a checklist of points to comply with, and detail what has been implemented and proved to work somewhere else without much thought given to the process of translating case specific conclusions to general theory.[8] But ‘best practices’ have an undeniable particular appeal, and this is twofold: it provides a practical and seemingly straightforward solution with the implied promise that the solution will apply to many different situations; and it has a rather simple methodology. However, this simplicity comes with a set of flaws. The methodology comprehends elements of generalisation and of comparison, and both present their own set of issues.

Before generalising, it is necessary to have a well-defined and comprehensive set of cases to study. For instance, if a research seeks to investigate the ‘best practice’ for Swiss banks to protect their computer systems from malware, one has to look at *all* the banks in Switzerland. The outcome of the research would then be applicable only to the elements of the set. Often however, the outcome will be interpreted to imply that the best practice can also work for a case outside the original data set. In the above example, this would mean wrongly applying the solution that worked for a Swiss bank to any bank outside Switzerland. This is a logical misconception. Universality cannot be derived from empirical observations. One of the reasons beyond logic is that the environment and the social constructs associated with a case are inherent to one case and cannot be simply translated onto another one. Norms regulating the banking industry in Switzerland and in the rest of the world differ as well as, for instance, the working culture within organisations.

Defining what and how to compare represents the second challenge. Identifying comparison criteria as well as attributing a value to the criteria relies on human judgement, which is biased, if not

[4] For an extensive list, see: ITU, 'Part 5: Security best practices', http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part05.aspx [1 May 2015].

[5] This is also the case for ‘best practices’ in other fields, see for instance Stuart Bretschneider, Frederick J. Marc-Aurele Jr., and Jiannan Wu, '“Best Practices” Research: A Methodological Guide for the Perplexed', *Journal of Public Administration Research and Theory* 15, no. 2 (2004).

[6] Alexandra Kalev, Frank Dobbin, and Erin Kelly, 'Best Practices or Best Guesses? Assessing the Efficacy of Corporate Affirmative Action and Diversity Policies', *American Sociological Review* 71, no. August (2006): p.590.

[7] E. Sam Overman and Kathy J. Boyd, 'Best Practice Research and Postbureaucratic Reform', *Journal of Public Administration Research and Theory* 4, no. 1 (1994): p.69.

[8] Arnošt Veselý, 'Theory and Methodology of Best Practice Research: A Critical Review of the Current State', *Central European Journal of Public Policy* 5, no. 2 (2011): p.99.

fallible. Judgement is particularly needed when we encounter a serious lack of information, and when action needs to be taken as a consequence of the judgement.[9] Going back to the example from above, the lack of information is the motive for undertaking the research in the first place, due to the fact that one does not know how to protect the bank's computer system. On the other hand, as a result of the research, the action that will have to be taken is to implement specific measures. But when looking at other banks' implemented solutions, one will invariably fall to biases. Biases are inevitable because human beings' observations are made on the basis of judgements.[10] Several psychological studies have shown the saliency of expectation biases at the level of individuals and organisations.[11] 'We tend to perceive what we expect to perceive', writes Richard Heuer, an intelligence study scholar.[12]

Further to these two fundamental methodological flaws, often comes another avoidable one: the internal validity of the results even within the chosen set.[13] Alternative hypotheses explaining the success of a case need to be thoroughly tested, using yet another methodology than that utilised in the case study. Process tracing, presently very popular methodology within the social science, would come handy in many research settings.[14] Process tracing aims at looking at 'the decision process by which various initial conditions are translated into outcomes'.[15] It garners the different variables that may have led to the outcome, considers them as dependent, and then looks carefully for evidence linking the variable to the outcome of the process. Conscientiously fleshing out the process, the variable, and the evidence helps to alleviate biases and to contribute to a more robust and, importantly, reproducible analysis. In other words, the research acquires a scientific character.

Similarly, another remedy to the generalisation problem is to understand and explicitly spell out how organisations differ. This does not remove the logical fallacy, but may tame the problem. It is to be noted that 'any "best practice" [research] design will be, by its very nature, less generalisable than standard social science research design'.[16] One of the very reasons is that the method focuses on extremes ('best practices') and not on mean values applicable to most cases.

By following a strict methodological approach, it is however possible to gain from discerning 'best practices' in cyber security. Specifically to this field, there seems to be a prevailing assumption that an organisation that applies 'best practices' will avoid turning into an easy prey to attackers, especially to the opportunistic ones. Any organisation can become the victim of a cyber attack. There is nothing substantial an organisation can do against well-resourced and persistent adversary, such as certain intelligence agencies (e.g. NSA or the Russian FSB) – and even applying any 'best practices'

[9] Raymond Geuss, 'What is political judgement?', in *Political Judgement : Essays for John Dunn*, ed. Richard Bourke and Raymond Geuss (Cambridge: Cambridge University Press, 2009), p.40.

[10] Ronald Beiner, *Political Judgement* (Illinois: Univeristy of Chicago Press, 1984), p.148.

[11] See for instance: Peter C. Wason, 'On the Failure to Eliminate Hypotheses in a Conceptual Task', *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960); Richards J. Heuer, 'Limits of Intelligence Analysis', *Orbis* 49, no. 1 (2005).

[12] 'Limits of Intelligence Analysis', p.79.

[13] Bretschneider, Jr., and Wu, '"Best Practices" Research: A Methodological Guide for the Perplexed', p.309.

[14] See for instance Gary King, Robert O. Keohane, and Sidney Verba, *Designing Social Inquiry* (Princeton, New Jersey: Princeton University Press, 1994).

[15] Timothy J. McKeown and Alexander L. George, 'Case Studies and The- ories of Organizational Decision Making', *Advances in Information Processing in Organizations* 2(1985): p.35.

[16] Bretschneider, Jr., and Wu, '"Best Practices" Research: A Methodological Guide for the Perplexed', p.312.

will not help.[17] Incentives for organisations to apply 'best practices' reside more in avoiding embarrassment by opportunistic hackers, which tend notably to be more vocal about their exploits than state sponsored hackers would. Counter-intuitively, this also implies that organisations, which apply 'best practices' can use them as a way to deflect responsibility when successfully attacked. The underlying message seems to be: 'there is nothing else that we could have done to prevent the attack from happening'.

Another issue inherent to the field of cyber security is what 'best practices' can possibly mean for each sector. For operators of a critical infrastructure, applying guidelines for 'best practices' are part of a risk mitigation strategy to avoid the worst-case scenario. Notably, one of the challenges important to them is to bring together the variety of different existing standards. For law enforcement agencies, on the other hand, the 'best practices' are more about enhancing information sharing processes and meandering through at-times unnecessary lengthy bureaucratic processes. For an intelligence agency like the NSA, 'best practices' in cyber security may rather concern information assurance. Tackling the problem of insider threats may be their priority of 'best practices' – especially after the leak they experienced with Edward Snowden. For instance, only a month after the first Snowden's revelation, the NSA decided to implement a two-person rule to access or move information.[18]

For owners of small-and-medium enterprises, the 'best practices' can represent first indications of what to do, if anything at all. A set of such guidelines can look as following: not only technical measures, but also organisational ones should be in place, making it clear for the employees whom they have to approach when they receive a mere suspicious looking e-mail; guaranteeing that each computer has an up-to-date antivirus, firewall, and anti-spam filter; carrying out regular backup of the data (preferably not with a cloud solution); logging the network activity; setting the access rights to the minimum and segmenting the network; automatically filtering out emails with specific extensions; conducting efficient password policy; and, lastly, encrypting the sensitive data.[19]

Although the 'best practices' may be well pertinent for small-and-medium enterprises, they may not be of much value to experts working in protecting the systems of an intelligence agency or a critical infrastructure. This research report focuses on the latter to offer an in-depth example of what 'best practices' can look like, and how they are actor-centred.

[17] Bluntly, this is captured by how the FBI director puts it: 'There are two kinds of big companies in the United States: There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese'. Dexter Roberts, 'Chinese Hackers Like a 'Drunk Burglar,' 'Kicking Down the Door,' Says FBI Director', *Bloomberg*, 6 October 2014.

[18] AP, 'Officials say new anti-leak measures set at NSA', *CBS News*, 18 July 2013.

[19] MELANI and GovCERT, 'Sécurité informatique: aide-mémoire pour les PME [IT security: a help for SMEs]',(Bern: MELANI, 2015).

Part 1: Organisational Approaches

3 CRITICAL INFRASTRUCTURES

Control and monitoring systems are essential operational processes used in today's critical infrastructures such as power plants, transportation systems, and manufacturing facilities. The generic term, Industrial control systems (ICS), includes many different control and monitoring systems, including SCADA (Supervisory Control and Data Acquisition), programmable logic controllers (PLC), Distributed Control Systems (DCS) and embedded control systems that eliminate or reduce the need for human interaction.

For IDCs, it is today's common practice to make use of standard embedded system platforms, often commercial off-the shelf software that helps to reduce cost and promotes ease of use but, at the same time, introduces additional risk from computer network-based attacks on inherent vulnerabilities found in standardised systems.

The potential for significant disruption to critical infrastructures and services from cyber-attacks was highlighted after deliberate attempts to infiltrate these systems. Successful intrusion could lead to uncountable consequences for the general public and national security.

As a result of bringing this subject to widespread attention, cyber security experts, governments, academics, critical infrastructure operators and other interested parties have formed working groups and launched initiatives to research into associated issues. ENISA (European Union Agency for Network and Information Security) is proactive in this area supporting research via a survey that investigates industrial control systems security-related working groups, standard bodies and initiatives.[20] This study provides useful information on standards and guidelines aimed at protecting critical infrastructures in different countries.

The working groups identified by the survey are summarised in *Table 1*. The information provided here suggests that the European Union may be lacking leadership regarding the creation and implementation of standards and guidelines. The US and international bodies appear to be further advanced in this area.[21] As a result, the European companies are tending to gravitate towards international standards for guidance and direction. This observation is of importance for deliverable and should be a topic for further investigation.

[20] ENISA, 'ICS Security Related Working Groups, Standards and Initiatives',(Heraklion: ENISA, 2013).

[21] 'Protecting Industrial Control Systems - Recommendations for Europe and Member States',(Heraklion: ENISA, 2011).

	Name	Acronym
International Working Groups	UCA International Users Group	UCAIUG
	Department of Energy	DOE
	ISA and ISA99 committee	ISA and ISA99
	National Institute for Standards and Technology	NIST
	NIST Smart Grid Interoperability Panel & Cyber Security Working Group	SGIP/CSWG
	Smart Grid Testing & Certification Committee	SGTCC WG
	Critical Infrastructure Security Working Group	CISSWG
	DETER Enabled Federated Testbeds consortium	DEFT
	Information Trust Institute	ITI
	ISA Security Compliance Institute	ISCI
	Anerican Gas Association Task Group	AGA 12
European Working Groups	Deutsches Institut für Normung	DIN

Table 1: ICS Security Related Working Groups

3.1 INITIATIVES FOR CRITICAL INFRASTRUCTURE PROTECTION

Improving critical infrastructure protection and resilience is of outmost importance in order to be able to withstand potential emerging cyber threat scenarios. In this section, a sample set of initiatives is analysed to give an overview of the current landscape.

The European Programme for Critical Infrastructure Protection is a specific action that aims at identifying and protecting the critical infrastructures of the European member states. The Programme defines the main activities that are necessary to maintain a safe environment for each of the EU States and across all relevant sectors of economic activity.

One of the main goals is identified as the need to improve protection from major threats such as cyber terrorism which per se is difficult to define.[22] In 2012, a review of the first version of the Programme was issued, analysing the extent to which the program has been adopted.[23] Based on the results of this review, the Commission approved and adopted a new approach, which sets a more

[22] European Commission, 'European Programme for Critical Infrastructure Protection',(Brussels: European Commission, 2006).

[23] 'Review of the European Programme for Critical Infrastructure] Protection (EPCIP)',(Brussels: European Commission, 2012).

practical implementation of the first version of the programme.[24] In this new approach, the interdependencies between critical infrastructures, industry, and state actors are observed. When a single critical infrastructure becomes the target for attack, the impact on a wide range of actors in a number of diverse infrastructures can be considerable. Another outcome of the review was finding that there was a lack of attention to and understanding of the connections between critical infrastructures and different sectors, which may extend across national boundaries. In order to appropriately protect the European critical infrastructures and enhance their resilience, this mismatch needs to be tackled. This is a finding that indicates a gap where improved practices guided through a best practices scenario may be of benefit and is a topic of note for this deliverable.

Figure 1 shows how different sectors in the critical infrastructure industry depend on each other. For example, the electric power (or power grids) infrastructure is central to numerous other sectors including telecommunication, water, natural gas, oil, etc.

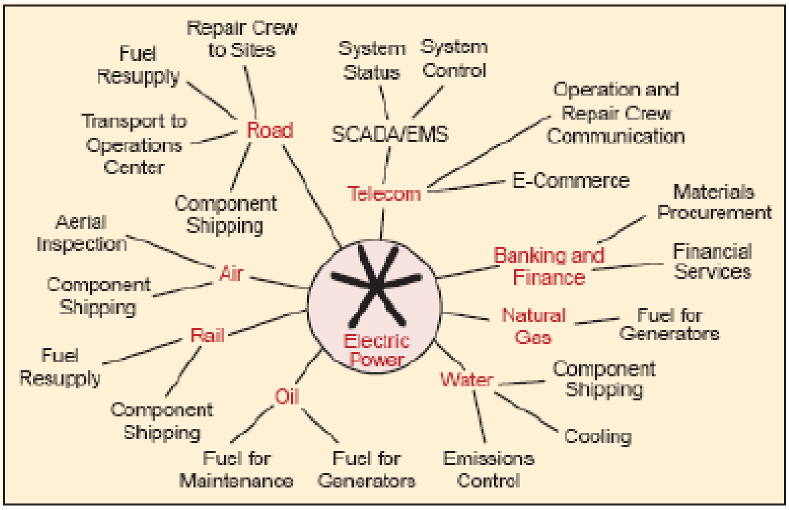

Figure 1: Interdependence between different critical infrastructures[25]

On March 30 2009, the European Commission also adopted a Communication on critical information infrastructure protection with the aim of introducing a plan that would involve both the private and the public sector.[26] The plan proposes five categories of support: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for European Critical Infrastructures in the field of information and communication technology. The plan was revisited in 2011, when the Commission concluded that there was insufficient support at the pure national level and that a joint effort across the European Union was needed. The requirement was for a system to adopt integrated cooperation between member states, which would enhance the

[24] 'A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure',(Brussels: European Commission, 2013).
[25] Ibid.
[26] 'Protecting Europe from large scale cyber-attacks and] disruptions: enhancing preparedness, security and resilience (COM(2009) 149 final)',(Brussels: European Commission, 2009).

resilience and security of information systems and networks and improve the level of protection from all manner of disruptions, deliberate or accidental.[27]

These considerations led to the establishment of the Critical Information Infrastructure Protection (CIIP) and Resilience Unit within the European Union Agency for Network and Information Security (ENISA). The main goals of this unit are to:

- Collaborate with the EU to enhance understanding of the threat landscape that networks such as Smart Grids and ICS-SCADA have to face;
- Develop good practices in the area of cyber security strategies and national cyber exercise;
- Offer training and seminars to individual members of European Union States on areas of their expertise, such as national exercises, contingency plans, incident reporting;
- Aid National Telecom Regulatory Authorities in the implementation of a coordinated exercise in mandatory incident reporting;
- Co-manage with the Commission for the Pan European Public Private Partnership for Resilience (EP3R) the process of combating fragmentation of the public and private stakeholders on emerging critical information infrastructure protection issues.

An important influence in this programme is the 2008 Directive on European Critical Infrastructures.[28] The aim of the program is to establish a standard approach towards determining if there is a need for better protection of European Critical Infrastructures. Directive 2008/114/EC9 applies specifically to the energy and transport sectors and urges member states to pinpoint which critical infrastructures may be at risk. By 28 August 2013, fewer than 20 had been designated which is most likely not a comprehensive assessment, when considering the number of European critical infrastructures that exist. The conclusion of the analysis is that there are a number of very critical infrastructures, including main energy transmission networks that have not been included.

The Smart Grid Coordination Group (SG-CG), formed by three European organisations, CEN (a major provider of European Standards and technical specifications), CENELEC (the European Committee for Electrotechnical Standardization) and ETSI (the European Telecommunications Standards Institute) [29], is another important initiative that co-produced a report on standardisation across the smart grid industry.

This working group formed as a result of the Smart Grid Mandate M/490 issued by the European Commission and European Free Trade Association.[30]. This mandate remit is to recommend a framework for standard enhancement in the smart grid sector be developed that outlines the European picture within the context of global activities[31]. The brief extends from generators to households appliances, which covers wide range of apparatus and devices and, as a consequence, the

[27] 'Policy on Critical Information Infrastructure Protection (CIIP)',(Brussels: European Commission, 2013).

[28] 'Directive on European Critical Infrastructures 2008/114/EC',(Brussels: European Commission, 2008).

[29] SmartGrids, 'CEN / CENELEC / ETSI: Smart grids and standardization', http://www.smartgrids.eu/CEN-CENELEC-ETSI [1 May 2015].

[30] European Commission and European Free Trade Association, 'M/490 EN - Smart Grid] Mandate - Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment',(Brussels: EC, EFTA, 2011).

[31] CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)',(2014).

standards required would also be diverse. For this reason, the bodies involved in the working group were of industry types.

The working group carried out some important developments, such as:

- A report highlighting existing standards and verifying if and how the European standardisation fit the requirements for smart grids.[32] The report provides a selection guide for Smart Grid systems for consideration of the most relevant existing and upcoming standards, from CEN, CENELEC, ETSI and further from IEC, ISO, and ITU, including as well other bodies when needed. The report also outlines how and when these standards can be used.[33]
- The Smart Grid Architecture Model (SGAM), a reference model to analyse and visualise smart grid use cases in respect to interoperability, domains and zones.[34]
- The SGIS - Security Levels (SGIS-SL), a framework to bridge the divide between electrical grid operations and information security for the purpose of enhancing the grid resiliency and for guidance on Smart Grid information security.[35]

The work was focused exclusively on smart grids. This is a notable research gap as a similar level of analysis and detail is lacking for other kind of critical infrastructures (communications, oil, gas and water distribution networks, etc.).

By comparison, initiatives in critical infrastructure protection in the United States are part of a nationwide program to ensure uniformity of security for vulnerable and interconnected infrastructures. The Homeland Security Presidential Directive HSPD-7 for Critical Infrastructure Identification[36] was first introduced by President Bill Clinton in May 1998 and was updated by President Bush in December 2003. Specific parts of the national infrastructure were identified as critical to national and economic security and, additionally, to the well-being of US citizens.

Directive HSPD-7 lists various steps that are necessary to secure the infrastructures, which have been defined as "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety".[37]

In the same directive, the US establishes a national policy that enhances the security and protection of US critical infrastructures and the identified key resources against terrorist acts. Additionally, in the Presidential Policy Directive/PPD-21 the importance of protection from cyber threats is explicitly stated.[38]

[32] CEN/CENELEC/ETSI Joint Working Group, 'Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids',(2011).

[33] CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)'.

[34] 'Smart Grid Reference Architecture',(2012).

[35] 'Smart Grid Information Security',(2012).

[36] White House, 'Homeland Security Presidential Directive/HSPD-7', 17 December 2003.

[37] Ibid.

[38] 'Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience', 2013.

3.2 STANDARDS AND ‘BEST PRACTICES’ FOR CRITICAL INFRASTRUCTURE

Critical infrastructure vulnerability reduction and enhanced resilience to cyber-attack is a major, but complex, goal for the European Union. Securing industrial systems is in the interest of organisations and citizens, of both the EU member states and the rest of the world. This is not an easy challenge for standardisation bodies as new cyber threats constantly challenge the established procedures and processes.

Innovative solutions are needed to protect industrial and operating utility networks. Interesting approaches are those that combine the ‘best practices’ in security management and the methods of governance of enterprise IT infrastructure. Although most of the current IT security policies and methodological frameworks have been designed to prevent and protect the Internet, a few steps ahead have been done in the last ten years towards the development of security techniques and standards that are specific for critical infrastructure networks.

In the United States, for example, the North American Electric Reliability Corporation is developing a robust set of critical infrastructure reliability standards that enable the industry to adapt to continuously changing threats and vulnerabilities by emphasising security risk management.

In the European Union, there are several initiatives for the protection of critical infrastructure, as has been mentioned in the above sections. Additionally, the Cyber Atlantic 2011 exercise is an initiative of note.[39] It was carried out in Brussels, testing the responses to cyber incidents and cyber-attacks. The exercise was based on the hypothetical scenarios of SCADA system failure in a European wind turbine.

ENISA provides another example of an interesting activity promoting best practices in critical infrastructure through its recommendations for the Europe and member states concerning the protection of industrial control system.[40] As well, ENISA published a report with an in-depth analysis of existing standards, regulation and guidelines for critical infrastructure protection.[41] The study points out that the energy sector (including oil, gas and electricity subsectors) has the largest number of specific guidelines, standards and regulatory documents. On the other side, sectors like transportation and water supply or agriculture lack this information (the Annex A also contains a summary of the most important standards for security recommendation for industrial control system).[42]

[39] ENISA, 'Cyber Atlantic 2011', https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 [1 May 2015].

[40] 'Protecting Industrial Control Systems. Recommendations for Europe and Member States',(Heraklion: ENISA, 2011).

[41] 'Protecting Industrial Control Systems - Recommendations for Europe and Member States'; 'Protecting Industrial Control Systems - Annex IV. ICS Security Related Initiatives',(Heraklion: ENISA, 2011).

[42] For a more extensive list please refer to: CEN-CENELEC-ETSI Smart Grid Coordination Group, 'Smart Grid Set of Standards (Version 3.1)'; E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (Waltham: Elsevier, 2014); IEC TC57 WG15, 'List of Cybersecurity for Smart Grid Standards and Guidelines', http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf [4 March 2015].

In this section, we discuss today's landscape of best practices, standards and regulations related to cyber security for non-critical infrastructures. Non-critical infrastructures include both public and private organisations and encompasses private industry, general service corporations, banks and financial organisations, non-profit associations, educational and research institutions, logistics and retail companies, commercial sector and merchants, as well as general services provided by the public sector. This broad domain is particularly exposed to threats and cybercrime, whilst it is often poorly covered by a cyber security policy (with the exception of banks and finance), not to say about the best practices.

In the following two sections, two reviews, conducted with the objective to identify and better understand the state-of-the-art of cyber security best practices in non-critical infrastructures, are reported. The first section presents a literature review in general, while the second focuses more on the end-user.

The following matrix presents the results of a quite extensive, although not exhaustive, investigation conducted in the Internet to identify best practices for non-critical infrastructures. The data are organised so that they present the source from which information was extracted, remarks summarising the content and the intention of the document, and a list of main arguments covered by the document. Concepts and arguments represented will also be of valid support in the understanding and developing of a cybercrime and cyber security taxonomy in D5.4.

The investigation focused on four principal business fields:

1. General, private organisations, industry, standards and guidelines.
2. Data centre security.
3. Bank and finance.
4. IT and software security.

The last one, in particular, deals with the fundamental and cutting-edge aspect of designing and developing secure-based valuable software, which represents an important and prioritised security activity in counteracting cybercrime.

Table 2: List of best practices

Document/Web Site	Web link	Remarks	Main arguments covered
General, private organisations, industry, standards and guidelines			
Microsoft, Best Practices for Enterprise Security	https://msdn.microsoft.com/en-us/library/cc750076.aspx	A well-structured web site, covering systematically all the aspects related to enterprise securisation.	Security threats, security strategies and planning, security entities architecture, security considerations for End Systems and Administrative Authority, Data Security and Availability, Naming Resolution, IP security, Monitoring and Auditing
ITU, Security Best Practices	http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part05.aspx	Very well structured and all–encompassing web site dealing with IT security and best practices, guidelines and standards from both USA and Europe agencies.	Social Networks, Business and IT continuity for SMEs, standards of good practices, National (USA) standards, security awareness (European agency), cyber security and networking, routing and network best practices, data encryption, electronic signature, e-mail security, payment cards, Incident Management, Monitoring and Response, Media and End User Device Security, Mobile Device Security, Information Exchange, Operating System and Server Security, Planning, Testing and Security Management, Radio Frequency Identification (RFID) Security, Risk Management, Security Metrics, Security Policy, Spam Spyware and Malicious Code, Web security, Wireless networks, Network Interoperability and Reliability Council.
ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance	https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en	The ISO/IEC 27003 standard on-line, dealing with guidance in developing the implementation plan for an	Information Security Management Systems (ISMS), ISMS scope boundaries and policy, information security requirements analysis, risk assessment and risk treatment planning, ISMS

		Information Security Management System (ISMS) within an organisation.	design guidelines.
BSI, ISO27001 Features and Benefits	http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISOIEC27001-Features-and-Benefits-UK-EN.pdf	A grid showing how to manage IT security with a ISO/IEC 27001 standard management system	Legislative requirements, reputation damage, availability of vital information, lack of confidence in the organisation, ability to manage IT security risks, difficulty in responding to rising customer expectations in relation to the security of their information, no awareness of information security within the organisation.
Google for Work Security and Compliance Whitepaper	https://static.googleusercontent.com/media/www.google.com/it/US/work/apps/business/files/google-apps-security-and-compliance-whitepaper.pdf	Security guidance for Google Apps for Work, Education, Government, Nonprofit, Drive for Work, and Google Apps Unlimited	Employee background checks, security training, internal security and privacy team, internal audit specialists, vulnerability management, malware prevention and monitoring, incident management, data centre security, network and data transmission security, service availability, third-parts standards and certification, data usage, data access and restrictions, law enforcements, EU and US regulatory compliance, user authentication, email, eDiscovery, securing endpoints, data recovery, security reports.
The Hartford Financial Services Group, Managing Security to Protect Data, 2009	http://www.thehartford.com/sites/thehartford/files/managing-security.pdf	A recommendation of security methods to safeguard sensitive or confidential data in technology and life science businesses.	Laptop security protocols, physical security procedures for backup media, electronic encryption, sensitive data protection

GIAC-Tim King, Best Practices for Securing Office Facilities: An Introduction to Physical Security, 2004	http://www.giac.org/paper/gsec/3597/practices-securing-office-facilities-introduction-physical-security/105843	Practical guide to best practices for physically securing remote offices and corporate branch buildings and facilities	Alarm systems, building security for building design planners and architects, access limitation and authorization, dual key entry systems, network connectivity and safety, doors one-way peepholes, physical security penetration testing
TREND Micro, Best Practices for Security and Compliance with Amazon Web Services, 2013	http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_best-practices-security-and-compliance-with-amazon-web-services.pdf	Cloud computing security best practices, concerning in particular with the Amazon Web Services (AWS) cloud system.	Cloud computing security , Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) security concerns, deployment model issues, security responsibilities in the cloud model, shared security responsibility with Cloud Service Providers, steps towards securising clouds strong passwords adoption, multi- factors authentication, operating system protection, firewall policy, host-based intrusion prevention system, file integrity monitoring, sensitive data encryption, conducting vulnerability assessment and penetration testing, customers involvement.
Data CentreSecurity			
GFI Blog, Goggi Cristina, The Ultimate Network Security Checklist	http://www.gfi.com/blog/the-ultimate-network-security-checklist	A concise but far-reaching pragmatic Web page presenting network security best practices, covering a wide range of aspects.	Security policies, servers provisioning and management, workstation deployment, network equipment, vulnerability scans planning, backups, remote access authorization, wireless networks, emails, Internet access issues, file shares, log correlation, centralised time system (e.g. NTP).
SecureSafe	http://www.securesafe.com/en/security	Securised on-line data storage and cloud system for individuals, business and finance.	Offers file and password secure storage, secure shares and business collaboration, highly secure digital delivery of financial documents.

Bank and finance			
TD Bank BusinessDirect Security Awareness	http://www.tdbank.com/exc/pdf/BusinessDirectSecurityMessage.pdf	Suggestions and involvement of customers in best practices to lowering the IT fraud risks.	Online banking transactions, individual security best practices, emails, malware and spyware countermeasures, banking online security features (user credentials, transaction limits, dual control, PC security best practices, account usage and password, inform the bank on suspicious fraudulent activities.
MP Bank, Online Banking Security Best Practices	https://www.mandpbank.com/online-banking-security-best-practices.htm	Security standards and procedures in order to keep customer's financial information secure and confidential.	Bank responsibilities: Layered security model, transaction encryption, secure login, login watermarking, multi-factor authentication, timed log-out, Customer responsibilities: User ID and Password confidentiality protection, updated browser and anti-virus protection, keeping information secure, using a separate Computer for Higher Risk Transactions, inform the bank on suspicious fraudulent activities.
Iberiabank, Security Best Practices	http://www.iberiabank.com/about-us/online-security/security-best-practices.html	Document showing how Iberiabank's online banking system protects the confidentiality of customer account and personal data and comply with all applicable banking regulations relating to the safeguarding of customer data.	Bank's security best practices related to: passwords, computers, mobile devices and others.
Enterprise Bank&Trust, Internet Banking Best Practices & Controls	http://www.enterprisebank.com/about_us_security/best-practices?l=kc	Recommendations to customers about how to perform security best practices on their data and online transactions.	Risk Assessment, account controls, internet usage controls, systems (PCs,..) controls.
Security National Bank, Online Banking - Business	http://www.snbconnect.com/business-best-	List of best practices and	Online transaction policies, emails, firewalls, strong

Best Practices	practices.aspx	recommendations to customers using the online banking system.	passwords, confidentiality of credentials, administrative rights limitation, commercial security suite software, browser cache clearing, secure session (https not http) in the browser, no automatic login features, do not use public Wi-Fi access, familiarise with the institution's account agreement, develop written security procedures, immediately share with bank and other customers information on suspected fraud activity.
Flushing Bank, Security Best Practices for Businesses & Public Entities	https://www.flushingbank.com/security.html	Suggestions to customer, who must actively participate in creating a secure environment to protect his online banking accounts from unauthorised access and fraudulent activity.	Monitor account activity on a daily basis, utilise dual controls, implement transaction limits, never share access information, use different logins and passwords for each online banking system, never access from a public computer, install commercial anti-virus, anti-malware and anti-spyware software, keep computers and software updated, limit administrative rights, pop-ups awareness, limit or eliminate unnecessary web-surfing and e-mail activity by employees, educate employees to clear the Internet browser's cache, use confidentiality of personal data and secure protocols (https), type the address of the page you are browsing to in the address bar instead of clicking on a link, no automatic login features, never leave a computer unattended, never send personal or sensitive

			information by e-mail or on the Web, do not click on links or open attachments contained in suspicious emails, immediately report suspicious or fraudulent activity.
Bank of America, Fighting Fraud. Online Security Management and Fraud Prevention, 2009		White paper aiming at involving employees at all levels to effectively combat fraud in its emerging context.	Fraud prevention, workplace trends, threads and fraud trends, integrated approach in front-door and back-door security, transactional control, employee education and bank solutions, best practices guidelines.
Bank of America & Merryll Lynch, Best Practices for Fraud Prevention	http://corp.bankofamerica.com/documents/10157/67594/Best_Practices_for_Fraud_Prevention.pdf	Best practices analysis and guidance to lowering the risk for a company dealing with online financial transactions	Online activities precautions, email, system best practices, electronic payment, check payment.
Bank of America & Merryll Lynch, Best Practices for Mobile Banking Security	http://corp.bankofamerica.com/documents/16303/72084/Mobile_Banking_Security.pdf	Recommendations to customer when accessing the online banking system from a mobile device	Password hardness and safety, managing system settings, downloads and device software, physical device security concerns.
IT and Software Security			
(ISC)2, The Ten Best Practices forSecure Software Development	https://www.isc2.org/uploadedfiles/%28isc%292_public_content/certification_programs/csslp/isc2_wpiv.pdf	An educated list and explanation of ten best practices to develop secure-based software, stakeholders-centric.	Protect the brand your customers trust , know your business and support it with secure solutions, understand the technology of the software, ensure compliance to governance, regulations, and privacy, know the basic tenets of software security, ensure the protection of sensitive information, design software with secure features , develop software with secure features, deploy software with secure features, educate yourself and others on how to build secure software.
SANS Institute Security Best Practices for IT Project	http://www.sans.org/reading-	Deals with IT projects, both	Security failures (Confidentiality, Integrity,

Managers, 2013	room/whitepapers/bestprac/security-practices-project-managers-34257	software and general IT ones, incorporating security best practices into the entire development life cycle .	Availability concerns), security plans and controls, risk mitigation, quantifying losses due to threats, security stakeholders identification, communication plans, risk management, communications security, authentications and passwords, access management, encryption, wireless attacks, physical security, reports and deliverables.

From the analysis of the survey outcomes reported in Table 2 and from the content of the documents found, it is possible to concisely present some general facts about cyber security practices nowadays, as implemented in non-critical organisations:

1. **The banking and finance sectors currently are the most motivated in looking for ways to reduce the risk of cyber frauds.** This particularly applies to online banking and financial transaction practices and to the more tertiary-oriented countries like Switzerland. The quality level of planning and security policy is similar to that found in critical infrastructures. Moreover, banks pay particular attention to finding ways in which customers can be encouraged to actively participate in good security practices (see point 5).
2. **Generally, the major software and IT-related companies are proactive in the adoption of cyber security activities.** These encompass most of the security best practices known today, although still **much remains to be done in the secure-based IT and software design and development field** (see point 5).
3. **The valuable layered-approach model to cyber security is not widely practiced**. In general, with the exception of the biggest organisations, no model at all is usually implemented: in the vast majority of cases, a simple do-it-yourself approach is adopted.
4. **"Traditional" countermeasures against cybercrime like firewalls, anti-malware software, user credentials and access rights, secure communication channel, and backups, are widespread in almost all non-critical infrastructure organisations.** All of them tend to be "first-aid" interventions, which respond directly to the problem but fail to provide preventive actions as a result of insufficient planning.
5. **Less 'traditional' countermeasures requiring a higher level of intervention and prevention techniques are less commonly adopted by non-critical organisations (with the exclusion of banks and the financial sector and the biggest companies).** Standard and regulation compliance, internal security teams, risk mitigation planning, log analysis, staff and customers awareness, and physical security require additional resources not readily available to SMEs. **The vast majority of protection measures adopted are those intended to counteract current communication risks.** All activities realised via electronic communication still represent an important vector of potential damage: emails, network traffic, unsecure telecommunication links, spamming, or vulnerability in social media. The principal reason behind this attitude is the necessity to protect sensitive and personal information from robbery, and the fear to be a victim of a criminal attack resulting from this data theft.

6. **The necessity to be compliant with standards and legal regulations are mostly evident in restriction-tied branches, such as banking and the healthcare sector**, where the protection of sensitive personal data, law enforcement, and the risk of sensitive data theft are particularly perceived.
7. **Awareness of sensitive data protection and of privacy needs is gaining more importance**, so that those activities appear rather widespread and best practices related to this thematic are generally taken into consideration.
8. **Some innovative types of countermeasures and best practices are being adopted within newer IT technologies such as cloud architectures, collaborative computing and secure data centres.** New variants of security issues necessitate fit-for-purpose practices, for example, access limitation for collaborative sessions, remote distribution of documents, multi-factor authentication. **Security-by-design remains a new field despite encouragement for wider adoption by academic and industry experts.** Software development companies and other IT organisations appear to be slow to incorporate security-by-design as standard practice even though there is a general awareness within the industry that there should be greater adoption.

Finally, this has implications for the end-user to consider. The necessity of making customers aware of the risks of becoming victim of frauds due to the widespread availability of IT technology, is becoming more evident in all sectors of non-institutional business branches. Having said this, it is nevertheless apparent from the survey that a real and effective implementation of such practices is still mainly the prerogative of banks and finance institutions. The reason is that online banking exchanges and electronic financial transactions are nowadays widespread among the public community, and are constantly increasing in volume, whilst remaining particularly sensitive to the domains of data thefts, frauds and personal information violations.

For nearly the same reasons, companies increasingly understand the need to make their staff aware of cyber security problems and threats. Each time more institutions begin to integrate quality and security policy in the staff training activities, often driven by standards and regulatory guidance.

Research and academic activities about this subject abound. Some relevant research papers are presented in Table 3:

Table 3: Papers on user awareness and training

J. L. Spears, "User participation in information systems security risk management", DePaul University, Chicago, IL, USA, 2010	http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2918&context=misq&sei-redir=1&referer=http%3A%2F%2Fscholar.google.ch%2Fscholar%3Fq%3Duser%2Bawareness%2Bon%2Bsecurity%2Bpaper%26hl%3Dit%26as_sdt%3D0%26as_vis%3D1%26oi%3Dscholart%26sa%3DX%26ei%3DHkpTVYbCKIbfywOjnYGwCg%26ved%3D0CB4QgQMwAA#search=%22user%20awareness%20security%20paper%22

A. Mylonas et al., “Delegate the smartphone user? security awareness in smartphone platforms”, Athens University of Economics and Business (AUEB), Greece, 2013	http://www.sciencedirect.com/science/article/pii/S0167404812001733
Ambrocia Boitumelo Makhudu and al., “Investigating Information System Security Policy and AwarenessTraining Programs in South African Organizations”, in Innovation Vision 2020: Sustainable growth, Entrepreneurship, and Economic Development, South Africa 2010	http://www.academia.edu/2409019/Investigating_Information_System_Security_Policy_and_Awareness_Training_Programs_in_South_African_Organizations
Ron Condon, “Enforcing user awareness with IT security awareness training, policy” in ComputerWeekly.com, 2008	http://www.computerweekly.com/news/1287865/Enforcing-user-awareness-with-IT-security-awareness-training-policy
AT Stephanou, R Dagada, “The impact of information security awareness training on information security behaviour: the case for further research“, University of the Witwatersrand, South Africa	http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.1461&rep=rep1&type=pdf
J. Evers, “Security Expert: User education is pointless”, 2006	http://news.cnet.com/Security-expert-User-education-is-pointless/2100-7350_3-6125213.html?tag=item
S. Srikwan, M. Jakobsson, “Using cartoons to teach Internet Security”, 2007	http://www.informatics.indiana.edu/markus/documents/security-education.pdf
John D'Arcy and al., “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach“, University of Notre Dame, Notre Dame, Indiana, USA 2006	http://pubsonline.informs.org/doi/abs/10.1287/isre.1070.0160
M. T. Sipponen, “A conceptual foundation for organizational information security awareness”, University of Oulu, Department of Information Processing Science, Finland, 2000	http://www.emeraldinsight.com/doi/abs/10.1108/09685220010371394
S.M Furnell and al., “A prototype tool for information security awareness and training”, University of Plymouth, Plymouth, UK, 2002	http://www.emeraldinsight.com/doi/abs/10.1108/09576050210447037
S.H. (Basie) von Solms, “Information Security Governance – Compliance management vs operational management” Academy for Information Technology at	http://www.sciencedirect.com/science/article/pii/S0167404805001057

the University of Johannesburg , Johannesburg, South Africa 2005	
J.M. Stanton and al., “Analysis of end user security behaviors”, Center for Science and Technology, School of Information Studies, Syracuse University, Syracuse, NY, USA, 2004	http://www.sciencedirect.com/science/article/pii/S0167404804001841
T. Dinev, Q. Hu, “The Centrality of Awareness in the Formation of User Be havioral Intention toward Protective Information Technologies” in Journal of the Association for Information Systems, Department of Information Technology and Operations Management, Florida Atlantic University, USA, 2007	http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1325&context=jais&sei-redir=1&referer=http%3A%2F%2Fscholar.google.ch%2Fscholar%3Fstart%3D10%26q%3Duser%2Bawareness%2Bon%2Bsecurity%2Bpaper%26hl%3Dit%26as_sdt%3D0%2C5%26as_vis%3D1#search=%22user%20awareness%20security%20paper%22
A. Adams, A. Blandford, “Bridging the gap between organizational and user perspectives of security in the clinical domain”, UCL Interaction Centre, University College London, UK, 2005	http://www.sciencedirect.com/science/article/pii/S1071581905000728

Part 2: Technical Approaches

5 SWOT AND ISO 31000

In this section two examples of 'best practices', used in the context of specific technical applications, are reviewed.

5.1.1 THE STANDARD ISO 31000

ISO 31000 is a family of standards codified by International Organization for Standardization whose purpose is to offer generic guidelines for the design, execution and maintenance of risk management processes throughout an organisation. It was published in November 2009 a replacing previously acting AS/NZS 4360.

The approach of ISO31000 is to help organisations align all strategic and management operation tasks throughout projects and processes to a common set of risk management. The most important attribute of ISO 31000 is the conceptualisation of 'risk' as the effect of incertitude on objectives: in this way it refers both to positive and negative possibilities.[43]

ISO 31000 suggests dealing with risk as follows:

1. Invalidating the risk by stopping the activity which creates the risk in the first place
2. Accepting or increasing the risk in order to achieve an opportunity
3. Removing the risk source
4. Changing odds and consequences
5. Sharing the risk with other parties
6. Holding the risk by informed decision

Compliance to the guidelines can be beneficial to cyber security training programs.[44]

5.1.2 SWOT ANALYSIS: WHAT IT IS AND HOW IT IS USED

SWOT is an acronym of strength, weakness, opportunities and threats. Both existing and new businesses can use the SWOT analysis: the former to evaluate changing conditions and respond adequately, the latter as a part of their planning process. It is possible to assign the SWOT analysis to a group of people with different positions within the company (sales or customer service, for instance). This also contributes to encourage different parties to work together.

A SWOT analysis is usually conducted using the four pillars it provides, one for each letter of the acronym. There is the possibility of holding a brainstorming session to identify the factors in each category. Otherwise, it is also possible to ask team members to initially complete analysis on their own and then to meet to discuss and create a final version of the required SWOT analysis.

[43] ISO, 'ISO 31000 - Risk management', http://www.iso.org/iso/home/standards/iso31000.htm [14 August 2015].

[44] CyberPol, 'CYBERBOK© Cyber-crime Security Essential Body of Knowledge: A Competency and Functional Framework for Cyber-crime Management ', http://cyberpol.org/CYBERBOK.pdf [14 August 2015].

Paying attention to Strengths and Weaknesses within a SWOT analysis is an internal process for a company. The company can invest work to change these factors. On the other hand, Opportunities and Threats represent the external factors over which the company may have no control.

The term 'strength' describes people's positive properties (education, background, reputation) and the company's assets (e.g., capital, credit, or distribution channels). 'Weaknesses' are aspects of business that present disadvantage in situations of competition, for example, limited resources or poor location of a business. 'Opportunities' are reasons the business is likely to prosper. Notably, one of the most important reasons is the perception that people have of the business in question. Finally, there is no way to control 'threats'. Yet they are connected to competitors and to factors that can put the business at risk, such as unfavourable trend, consumer behaviour, or government regulations.

Once the SWOT results are ready, they can be used to create strategies to maximise the positive aspects of the business and to minimise the negative ones, and to organise regular review meetings.[45]

5.1.3 SWOT Analysis and ISO 31000

In ISO 31000, one of the key concepts of risk management is that it is to be driven by the strategic planning process. A good way to introduce 'risk' into strategic planning could be through the Threats and Opportunities sections of the SWOT model.

The ISO 31000 risk management standard states:

> Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organisation, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

According to the risk assessment expressed in the ISO 31000, in the 'context' and the 'environment' there are assets and policies used for that specific business. Context is, according to the SWOT matrix, the 'strength' and 'weakness', while the environment could represent the 'opportunities'. The 'threats' in the SWOT matrix are 'risks' in ISO 31000.

As an example, let us consider a scenario where the company's business is in telecommunication (services and products). Then the following elements would come out in the SWOT matrix:

[45] Ronald Quincy, Shuang Lu, and Chien-Chung Huang, 'SWOT Analysis: Raising Capacity of Your Organization',(Rutgers University, Beijing Normal University, 2012); Tim Berry, 'What Is a SWOT Analysis?', *BPlans*, 4 October 2008; Mindtools, 'SWOT Analysis: Discover New Opportunities, Manage and Eliminate Threats', 2015.

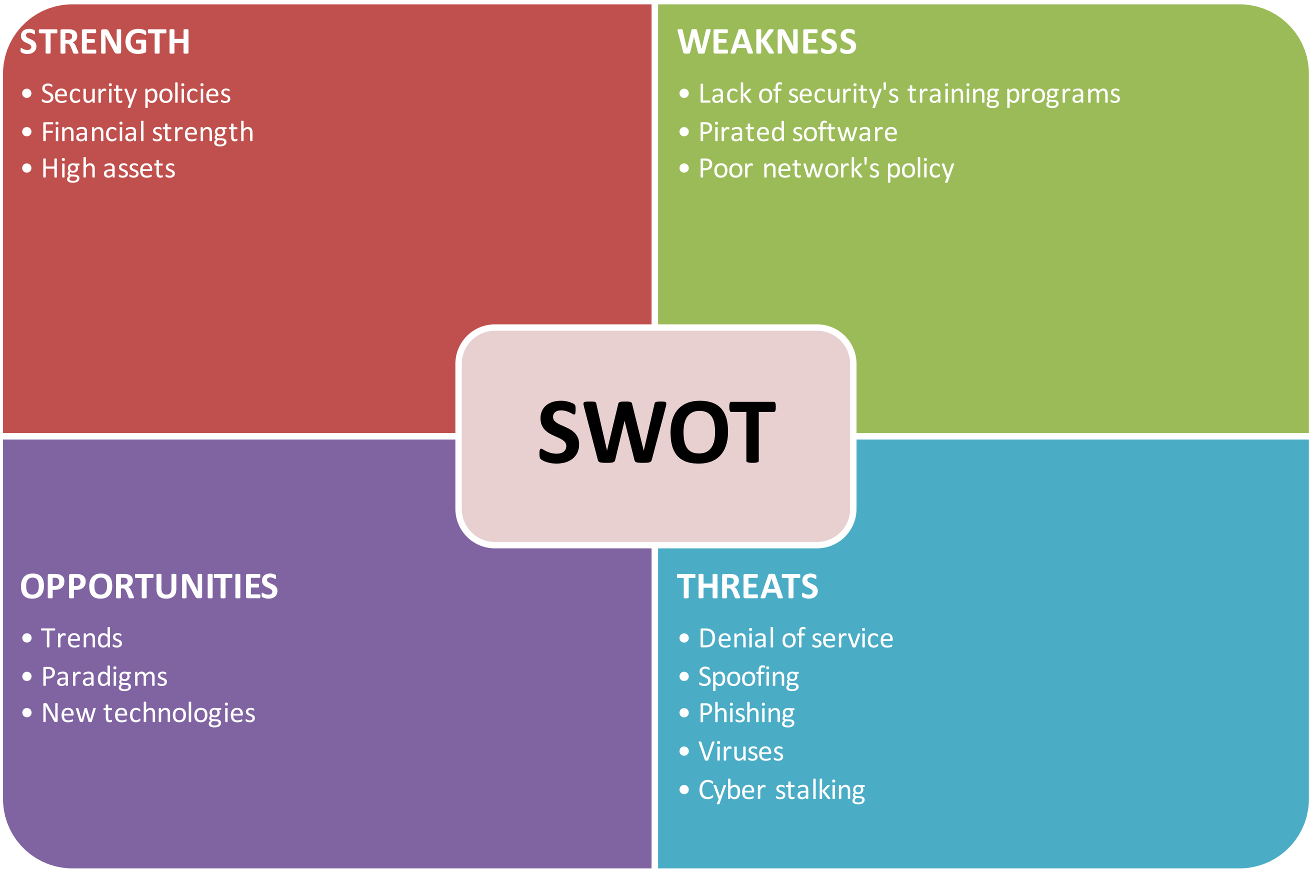

Figure 1: SWOT matrix for cybercrime

It is possible to refine the SWOT matrix with a more accurate taxonomy for cybercrime.[46]

5.1.4 SWOT and Taxonomy

Once the SWOT methodology is properly understood, it is not difficult to apply this method to each sub-category of the taxonomy for cybercrime and cyber terrorism using a scheme of Strength-Weakness-Opportunity-Threats. Each sub-category becomes a new macro-area. This way, there is a different SWOT for each (sub-) domain and, consequentially, new "Strengths-Weakness-Opportunities-Threats" for different domains.

[46] For a short online discussion, see Wolf Streider, 'Is a SWOT analysis a reasonable starting point for a risk assessment? Discuss', https://www.linkedin.com/grp/post/1834592-240204315?goback=.gmp_1834592 [14 August 2015].

Part 3: People-Centred Approaches

6 PERSPECTIVE OF SMALL-AND-MEDIUM ENTERPRISES ON PROTECTIVE MEASURES

Best practices can equally be approached from an angle that places people as the focus. In this section, small and medium-sized enterprises provide the sample set for a review of the measures taken against cybercrime in an effort to protect the economy globally.

Today cybercrime is a threat which all Europeans are exposed to. For individuals and small-and-medium enterprises (SMEs) the impacts may be great as particular importance is given to their "assets" such as money, privacy, health, family and information. However, SMEs constitute a potentially less-prepared target within Europe, as many use the Internet without knowing its security vulnerabilities.

The 2012 Data Breach Investigations Report, presented by Verizon, concludes that 75% of cyber-attack victims were opportunistic.[47] Thus, it is of paramount importance to address the existing best practices to prevent cybercrime in social networks, e-commerce, e-banking, mobile systems, public clouds, and the Internet of Things, which impacts not just ordinary European citizens but small enterprises as well, whose vulnerability to cybercrime is a growing economic concern.

In fact, it is difficult to give even a rough estimation of the losses caused by cybercrime. There are too many sources and different statistics that are not in line with each other due to significant variation within the subjects under consideration. However, these methodologies enable us to appreciate the scale of the problem being faced. For instance, in 2012 the World Economic Forum elaborated, on the basis of interviews among 250 industry experts and business executives, a report which estimated that over the next few years cyber-attacks could cause economic losses of up to 3 trillion dollars, if the fight against this threat is maintained at the same level.[48]

Notably, if we restrict ourselves only to SMEs, the projections are even more alarming. According to the Symantec Internet Security Threat Report 2014, cyber criminals will diminish their action against large companies, focusing their resources on attacks against SMEs. In addition, the report stresses that the *modi operandi* used are becoming increasingly sophisticated and are composed mainly of phishing and social engineering (often used together), as well as of ransomware.[49]

SME's, unaware of the cybercrime activities they are facing every day, adopt innovative technologies and increase their resources without realising that this may offer a wide open door to new security threats in their daily operations. SME owners might see cyber security as an important issue but, as stated by Gregory P. Keeley, 'the majority of small businesses have almost no strategy or execution

[47] Verizon, 'The 2012 Data Breach Investigations Report',(Verizon, 2013).

[48] World Economic Forum and Deloitte, 'Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience',(World Economic Forum, 2012).

[49] Symantec, 'Symantec Internet Security Threat Report 2014',(Symantec, 2014); World Economic Forum and Deloitte, 'Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience'.

plan with regards to simple issues such as Internet usage policies, privacy, and effective security solutions'.[50]

Some studies have pointed out that weak knowledge and awareness in the SME environment about cybercrime, information security, security technologies and control methods can be a reason for low cyber security practice.[51] How can SMEs be expected to protect themselves or act against threats and crime if they are not aware of potential vulnerabilities?

Lastly, SME staff, in general, lacks specialised knowledge and training, acts without specific cyber security policies, and does not know how to develop and implement a response to cybercrime threats. Therefore, cyber security is not prioritised as a fundamental issue within the SME. In addition, any reduction in ICT budgets — combined with the lack of time, training, education, and ability to establish continuous security awareness — severely decreases the extension and efficiency of countermeasures against cyber-attacks.

What are the threats SMEs are exposed to? To respond this question, *Watchguard.com* listed 10 major IT security threats that are commonly harmful to SMEs (in US):

- Insider attacks,
- Lack of contingency,
- Poor configuration leading to compromise,
- Reckless use of hotel networks and kiosks,
- Reckless use of Wi-Fi hot spots,
- Data lost on a portable device,
- Web server compromise,
- Reckless web surfing by employees,
- Malicious HTML email,
- Automated exploit of a known vulnerability.

Watchguard.com also presented some prevention measures (see table below) that can be considered as best practices, or 'practical techniques and defences'.[52] In terms of methodology, Cobb suggests a 6-step plan for SMEs to protect their data and systems from cyber-attacks:[53]

- Assess your assets, risks and resources,
- Build your policy,
- Choose your controls,

[50] Gregory P. Keeley, *Cybersecurity in Small Businesses and Nonprofits, Chapter 9 "Protecting Our Future: Educating a Cybersecurity Workforce"*, vol. 2 (Hudson Whitman/Excelsior College Press, 2013).

[51] S. Dojkovski, Sharman Lichtenstein, and Matthew J. Warren, 'Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia' (paper presented at the European Conference on Information Systems, St. Gallen, 2007).

[52] S. Pinzon, 'Top 10 Threats to SME Data Security',(WatchGuard Technologies, 2008).

[53] Stephen Cobb, 'Cyber Security Road Map for Businesses', *We Live Security*, 14 May 2013.

- Deploy your controls,
- Educate employees, executives and vendors, and
- Further assess, audit and test.

There exist a number of policies and guidelines for organisations that provide directions for information security, such as the ISO-27000 series of standards that instruct how to improve some areas of security policy for example ISO-270002 (security controls), ISO-270031 (business continuity) and ISO-270032 (cyber security).[54] However, the high cost of implementation of these guidelines restrains SME adoption.

A fundamental question to be considered in relation to SMEs is: should the focus be on the latest mitigation technology or on a managed plan of policies and practices that can effectively provide protection for an SME through risk reduction? A balance between both lines of action may be the way forward. Information security cannot rely solely upon technical solutions, especially considering high costs of cybercrime prevention and poor availability of qualified cyber security professionals in the market, most of which are employed by large corporations and public entities.

On the other hand, information security has to rely as well upon a suitable IT security culture that can be implemented by cautious and good actions of employees, by enforcing training and education. In this context, knowledge is the major key to leverage employee's behaviour and their understanding of the value of security. Thus, recommendations for SME and best practices have to be based on knowledge and cultural transformation.

Both of the above mentioned modalities of fighting cybercrime have information sharing as the principle cornerstone, providing support to the following assertions recently formulated by Zappa:

> The real frontier that needs to be demolished is the cultural one. Many defensive strategies could be put in place, and at a low cost. Beyond internal security policies, there is a need to incentivise information sharing at the highest levels. As a preventive measure, before an attack, all the best practices and information concerning cyber threats could be shared between companies of the same network, trade associations and law enforcement agencies; this could help in putting counter measures in place.[55]

Table: Top 10 Threats to SME Data Security

Nr.	Threat	SME's Practical techniques and best practices for preventive measures
1	Automated exploit of a known vulnerability	**Mitigating automated exploits** • Invest in patch management • Build an inexpensive test network. • Train the employees to comply with the updated software • Implement prevention policy

[54] International Organization for Standardization, 'An Introduction to ISO 27001, ISO 27002....ISO 27008',(International Organization for Standardization, 2015).

[55] F. Zappa, 'Cyber-crime: Risks for the Economy and Enterprises at the EU and Italian Level',(Unicri, 2014).

2	Malicious HTML email	**Mitigating malicious HTML email** • Implement an outbound web proxy. • Implement spam filtering • Raise employee awareness • Implement prevention policy
3	Reckless web surfing by employees	Mitigating reckless web surfing • Implement web content filtering • Web filtering solutions to block URLs • Use a firewall
4	Web server compromise	**Mitigating web server compromise** • Audit your web app code. • Audit the web application code to fix all the security holes • Use firewall for malicious traffic
5	Data lost on a portable device	**Mitigating data lost on portable devices** • Manage mobile devices centrally • Encrypt data on the devices, • Use of Mobile Device Management (MDM) software
6	Reckless use of Wi-Fi hot spots	**Mitigating reckless use of Wi-Fi** • Teach users to always choose encrypted connections
7	Reckless use of hotel networks and kiosks	**Mitigating reckless use of hotel networks** • Set and enforce a policy, forbidding employees to turn off defences. • Use updated anti-virus/spyware/malware • Use a firewall
8	Poor configuration leading to compromise	**Mitigation for poor configuration choices** • Perform an automated vulnerability audit scan • Change the default username and password of electronic devices • Implement prevention policy
9	Lack of contingency	**Mitigation for lack of planning** • Develop policy based on the company's needs • Implement prevention policy
10	Insider attacks	**Implement the principle of dual control** • Check the basic background of employees • Not concentrate authority over IT asset in one employee • Implement prevention policy

7 Combating cybercrime in Poland: state of current practice

As the previous contribution made clear, cybercrime is damaging and important to consider when looking at the negative effects of cyber-attacks on a country's economy. In order to delve deeper into the topic, this contribution focuses on a specific country which is also an active participating member of the CyberRoad project, Poland.

A specific approach to cyber security 'best practices' is illustrated by using Poland as an explicit example. There are few technical or academic Polish articles that deal with cybercrime as a detailed subject. The academic papers written in Polish or by Polish authors that exist on the topic tend to focus on the relevant laws that can be applied to cases that involve cybercrime. They do not, however, provide any context or analysis of actual cases that have been handled and constraints faced.[56] Non-security vendor driven research, on the other hand, tends to focus on compliance with EU regulation, usually in the broader cyber security context (a list of such research is presented below).

Foreign – and often vendor driven - research tends to focus on technical observations (for example, malware infection levels in the Microsoft Security Intelligence Report) or makes assumptions about the cost of cybercrime in a specific given country.[57] Especially in the latter case, it is very unclear how accurate this is, and an issue that does not only apply to Poland.[58]

7.1 CERT statistics

CERT Polska - operating as a part of the NASK Institute (Naukowa i Akademicka Sieć Komputerowa, a CyberROAD project partner) provides a broad number of security statistics based on actual observation of security incidents in Poland in its annual 2014 report.[59] For instance, it estimated that on an average day in 2014, there were 280,000 computers infected with malicious bots. Over 50,000 of them were infected with a type of a banking Trojan written to facilitate financial fraud. As a part of its mission, CERT Polska regularly publishes information on specific mechanisms of cybercrime, including statistics regarding malware on Polish networks, malicious URLs, phishing, spam, distributed denial-of-service attacks and their associated and command & control servers.[60] Other similar reports – specifically focused on government administration in Poland – are published by the Polish Internal Security Agency (ABW), which operates the CERT.GOV.PL.[61] Other Polish entities exits that publish cybercrime related statistics, but from an Internet safety aspect (such as child safety online, child pornography and hate material).[62]

[56] Nicolaus Copernicus University, 'Cyber-crime Research Centre: Publications', http://www.cyber-crime.umk.pl/publications,7,en.html [12 May 2015].

[57] Microsoft, 'Microsoft Security Intelligence Report ', http://www.microsoft.com/sir [12 May 2015]; Norton, 'Norton Cyber-crime Report 2012', http://us.norton.com/cyber-crimereport [12 May 2015].

[58] Andy Greenberg, 'McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim', *Forbes*, 3 August 2012.

[59] NASK, 'Cert Polska: Rapport 2014',(Warszawa: CERT Polska, NASK, 2014).

[60] See for a full list of publications: 'Papers', http://www.cert.pl/raporty/langswitch_lang/en [12 May 2015].

[61] CERT.GOV.PL, 'Publikacje', http://www.cert.gov.pl/cer/publikacje [12 May 2015].

[62] Polish Safer Internet Centre, 'saferinternet.pl: Keeping children and young people safe online', http://www.saferinternet.pl/en/ [12 May 2015]; Dyzurnet.pl, 'Dyzurnet', http://www.dyzurnet.pl [12 May 2015]; Fundacja Dzieci Niczyje, 'The Nobody's Children Foundation', [12 May 2015].

7.2 *POLICE & GOVERNMENT STATISTICS*

The Polish Police does not provide detailed statistics relating to cybercrime in their public reports.[63] More information can be gained from the MSW (Ministry of the Interior) reports that include general statistics in terms of the amount of cases and (selected) laws applied.[64] This also includes data from other parties, such as the Ministry of Justice.

The Polish Ministry of the Interior Report lists 19 articles of the penal code that specifically concern cybercrime and attacks against computer systems, and lists another 19 that can also be committed in cyberspace. It also enumerates 11 different crimes understood as cybercrime:

1. Online fraud
2. Phishing and other financial crime
3. Paedophilia and child pornography
4. Copyright and intellectual property infringement
5. Trading in unlicensed or illegal goods
6. Human and human organ trafficking
7. Illicit trade in excise goods
8. Trade of artefacts coming from crime and illegal trade of goods of national heritage
9. Extortion or threats by organised crime
10. Hacking, sniffing, breaking into systems and malware
11. Illegal gambling online

The report also summarises police statistics regarding specific violations of articles of the penal code. However, apart from the fact that there is an increase in these selected violations, numbers are difficult to perceive. It is not always clear if the statistic really concerns cybercrime, as it is not mandatory to specify whether a crime was committed on a computer network or the Internet when reporting it. For those that clearly fall within cybercrime, the larger numbers of offenses were 'computer fraud' (26,945 cases) and 'paedophilia and child pornography' (1,648 cases). In terms of cybercrime, the number of cases that actually ended up in court is much smaller. The top two categories concerned the destruction or damage of computer data (57 persons tried, 47 sentenced) and 'computer fraud' (33 persons tried, 18 sentenced). The only two other categories in the report 'interference in the functioning of computers or networks' and 'production, acquisition, selling, sharing, devices or computer programs to commit crimes' were at 9 (5) and 6 (4) respectively.

As part of the CyberROAD, Cert Poland submitted two requests for public information. One request was sent to the Polish police and another one to the Ministry of Justice. The request asked the police for the number of initiated investigations concerning crimes against information security and other crimes committed with the use of Internet, as well as numbers of cases where investigations were discontinued and reasons for the decision. The results showed that an overwhelming majority of investigations is discontinued due to an impossibility of establishing the perpetrator. Most crimes against information security are related to unauthorised access to information (Art. 267 of Polish

[63] Policja, 'Statystyka', http://www.statystyka.policja.pl/ [12 May 2015].

[64] Ministerstwo Spraw Wewnetrznych, 'Raport MSW o stanie bezpieczeństwa [Polish Ministry of the Interior reports on security in Poland]', [12 May 2015].

Penal Code, which unfortunately does not differentiate between physical and electronic access). Other crimes in which the Internet was used are mostly frauds, in particular during online transactions. These findings are in line with statistics of the Ministry of Justice. Only one in about fifty crimes identified by the police resulted in a final conviction, with an average sentence of less than 9 months (using the same Art. 267 as an example).

7.3 NATIONAL CYBERSECURITY STRATEGY WITH REGARDS TO CYBERCRIME

Two major documents exist in regard to Poland's approach to cyber security. The first document is the "Cybersecurity Doctrine of the Republic of Poland 2015" (currently only available in Polish).[65] While the document is broad in terms of discussing different cyber security issues, it essentially glosses over the topic of cybercrime, referencing it only twice and mentioning that it should be addressed, failing to state the role of the police in doing so. The second document, the 'Cyberspace Protection Policy', introduces the concept of cybercrime, even provides a definition as 'an offence committed in cyberspace', but fails to elaborate on the topic.[66]

It should be noted that none of these documents is legally binding. It is expected that official legal acts in this area will be implemented once a directive from the European Union called the 'Network and Information Security' is established. Globally, it can be said that Poland currently lacks a comprehensive programme in combating the cybercrime.

7.4 A COMPARISON OF STATISTICS

Reports in the statistics published by different parties signal a large disparity between the numbers of observed security incidents (including cybercrime) by CERT Polska and government statics regarding cybercrime cases. Based on the surveys carried out in the CyberROAD project (more in the next section), it would appear that most cases are simply not reported to the police. Subsequent police investigations into cases appear not to be very effective, with only few going to court. The situation is best summed up in the words of Jerzy Kosinski, a researcher at a Polish police school:

> "It can be said, that computer piracy has become one of a few areas of computer crime where the police are effective."[67]

This may be because the affected companies are determined to fight with this problem, and have the resources to hire law firms and push cases. The conference paper also makes another point in the paper worth noting:

> Computer frauds such as interfering with input data, program or output are often a black number. Afraid of having their reputation undermined, banks, offices and companies often fail to inform the police and the public about them.[68]

[65] Biuro Bezpieczeństwa Narodowego [National Security Bureau], 'Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej [Cybersecurity Doctrine of the Republic of Poland]',(Warszawa: BBN, 2015).

[66] Internal Security Agency Ministry of Administration and Digitisation, 'Cyberspace Protection Policy of the Republic of Poland',(Warsaw: MAIC, 2013).

[67] Jerzy Kosinki, 'Cybercrime in Poland 2011-2012', in *International Scientific Conference Archibald Reiss Days III*(Belgrade2015), p.1.

[68] Ibid., p.2.

The Eurobarometer survey conducted in October 2014 on cyber security highlights another aspect of the problem:

> Whilst the value of the cybercriminal economy as a whole is not precisely known, the losses are thought to represent billions of euros per year. The scale of the problem is itself a threat to law enforcement response capability – with more than 150,000 viruses and other types of malicious code in circulation and a million people victims of cybercrime every day.[69]

7.5 THE CYBERROAD SURVEY

As part of the CyberROAD project, the project consortium decided to carry out a three-step survey into cybercrime to get a better understanding of the phenomenon and end user perceptions.[70] This survey was aimed at respondents from the entire world with an English language version and specifically at Poland with a Polish language version. The consortium members decided to pick Poland as a specific example country to compare with others. Poland was selected because it is one of large EU countries and is also represented by a national CERT team (CERT Polska) in the CyberROAD consortium. The initial results of the first survey are summarised below with an attempt to highlight the main differences between Polish and English speaking respondents (data based on responses collected until May 11, 2015):

- Polish respondents stated that cybercrime was a lesser concern for their organisation compared to the English language respondents (39.2% of the respondents said that cybercrime was only a slight concern or none at all while this represented 16% of the respondents of the English survey). This is despite that fact that individually, respondent concern was at similar, if not slightly higher levels.
- Security training levels of respondents were slightly lower than the English language survey respondents, with 73.1% of respondents receiving no training or only after a problem is identified in comparison to 63,2% for the English survey.[71]
- Education was pointed out as the main area of improvement (74.6% of respondents with a similar number of English survey respondents, 72.3%, stated that it was a 'very important' element to improve).

Also notable was that there was:

- A higher percentage of Polish respondents had experience cybercrime in the last 5 years in a personal capacity (43% vs. for 26.7% English language survey respondents).
- A low impact of cybercrime for Polish respondents as victims: 'inconvenience' or 'no effect' of cybercrime obtained the most responses (41% and 42.6% respectively). The English survey responses were 46.8% and 33.3% respectively.
- A low reporting rate of cybercrime cases to the Police (31%), similar to the English survey responses (30.4).

[69] European Commission, 'Special Eurobarometer 423: Cyber Security',(Brussels: European Commission, 2015), p.2.

[70] CERT.PL, 'CyberROAD – Invitation to participate in the project survey', http://www.cert.pl/news/9671/langswitch_lang/en [12 May 2015].

[71] A 'Don't know' as a de facto no training answer was included here as well

- A low successful Police action and prosecution rate (5.3%), similar to the English survey responses (7.2%).

- Low reporting rates to CERTs - similar to English survey respondents (not reported by 84.4% of Polish survey respondents and by 80.3% English survey responses).

- A low tendency to share information on attacks with other organisations – lower than that of respondents of the English language survey (21.1% vs 35.4%)

It is of note that Polish survey respondents tended to come from a younger group, more consumer oriented or involved in a commercial business than their English language counterparts who included more academics and security specialists.

7.6 THE EUROBAROMETER SURVEY ON CYBER SECURITY

The aforementioned Eurobarometer survey on Cyber Security for the European Commission gives much insight into perceptions and experiences of EU citizen with cybercrime. It is also very useful in providing a more in-depth comparison of Poland versus the rest of Europe.

- The most basic conclusion is that the average Pole is not very concerned with cybercrime. Responses to concerns regarding online banking payments were the second lowest in Poland out of all the EU countries surveyed (29% of respondents) and lowest when it came to potential misuse of personal data (25% of respondents).

- Polish respondents were least likely to say that they have changed the way they use the Internet due to security concerns.

- Polish respondents were among the least likely to say that they have installed anti-virus software (only 43%), least concerned about opening emails from people they do not know (29%), least regularly changing their passwords (14%) and one of the least likely to use different passwords for different sites (17%) or to change settings (8%).

- Despite these not very positive statistics, there was a general improvement of security issues, at least declared by the respondents, up 21% compared to a similar study in 2011.

In terms of cybercrime concerns, there are also some different perceptions compared to other EU countries:

- Poland declared one of the highest concerns of online fraud.[72]

- Encounters with online child pornography was the second highest in the EU, concerns with hatred materials were also above average.

- Denial of access to services is an area of concern for respondents, but not experienced by most.

- Personal data security concerns (having their e-mail account or social account hacked) was an area of lower concern and personal experience than in most other EU countries.

- Banking fraud was slightly less personally experienced by Polish respondents compared to the EU average, as well as slightly less an area of concern.

[72] Defined as ‘goods purchased were not delivered, counterfeit or not as advertised’

The authors of the survey made an interesting observation: 'the survey findings suggest that a greater knowledge of cybercrime leads to a preference to contact organisations such as the website or vendor rather than the police'.[73] Polish respondents often quoted the Police as appropriate contact for cyber security issues, although compared to police statistics, it appears that there is little reporting actually carried out. On the other hand, a PwC Crime Survey 2014 study noted a drop in cybercrime as a problem for survey respondents from 24% in 2011 to 19% in 2014.[74] This is below worldwide average (24%), and also contrary to CERT Polska reports and statistics.

7.7 BSA REPORT ON LEGISLATION

In comparison once more with another survey, a recent 'EU Cybersecurity Dashboard' study by a software non-commercial group called BSA released in March 2015 provides an overview of the cyber security landscape in Europe. The survey takes a legal and policy perspective, covers particularly aspects such as: legal foundations for cyber security, operational capabilities, public-partner partnerships, sector-specific cyber security plans and education.[75] Poland was found to have a 'comprehensive cybersecurity strategy with clear goals' but many were viewed as not yet implemented, and the legal cyber security framework not fully developed.

A few missing elements to the current framework, according to the BSA studies, included that:

- There is no legislation or policy in place in Poland that requires the establishment of a written information security plan.
- There is no legislation or policy in place in Poland that requires an annual cyber security audit.
- There is no legislation or policy in place in Poland that requires each agency to have a chief information officer or chief security officer.
- There is no defined public-private partnership for cyber security in Poland.
- There are no new public-private partnerships being planned in Poland.
- Poland does not have sector-specific joint public-private plans in place.
- Sector-specific security priorities have not been defined.
- Sector-specific risk assessments have not been released.

7.8 OBSERVED GAPS

In terms of the overall conclusions regarding cybercrime in Poland, the following gaps have been observed as part of this study:

[73] European Commission, 'Special Eurobarometer 423: Cyber Security', p.94.

[74] PwC, 'Economic Crime Survey Poland 2014',(Warsaw: PwC, 2014), p.6.

[75] BSA, 'Country: Poland',(BSA, 2014).

- There are sufficient cybercrime penal laws in place, but there appears to be a lack of adequate enforcement. Even if cases are reported, most of them do not lead to prosecution or sentencing.

- Reporting rates of cybercrime incidents to authorities appear to be low. Most Polish users report cybercrime effects as a mere 'inconvenience', which may also result in the relative absence of Police reports.

- There is no national plan to tackle cybercrime. Existing documents that attempt to establish cyber security policies at the national level do not devote sufficient attention to the problem or recognise the complexity of the problem.

- There is a lack of good statistics and metrics to measure cybercrime levels and costs resulting from cybercrime - a problem that applies not only to Poland but also almost everywhere else. There is a need to move beyond the technical observations of the tools used to commit the crime (like malware or malicious pages) in order to focus more on cybercrime itself.

- There is no established link between cases reported to the Police, successful prosecution in court and technical measurements and statistics from CERT reports.

Work on exploring these gaps and looking for possible solutions will be the subject of further research under the CyberROAD Project.

8 Current practices and their influences (*survey*)

Critical infrastructures and cybercrime are only one part of how 'best practices' for cyber security are being considered by various international agencies and national governments. As the initial research question did not focus on any specific industry for cyber security, there was an interest in trying to obtain a broader picture. As part of the CyberRoad WP5.1, a survey was designed and made available on the CyberROAD website with the target being professionals working in the field of cyber security and other interested parties which included policy makers, academics and consumers. The survey was offered to participants worldwide but with a specific focus towards Europe which would provide a macro viewpoint as a base for further analysis. The survey was also translated into Polish to garner a micro perspective. Poland was chosen as the survey could be pushed via CERT (Computer Emergency Response Team) Polska, a participant of the CyberROAD project.

Several questions within the survey pertained to 'best practices', the theme of WP5.2. The survey provides a snapshot of the current best practices landscape, through assessment of the practices companies are applying. The survey included questions pertaining to personal and organisational cyber security practices as well; only the organisational ones have been taken into consideration here. By looking at specific correlations, it is possible to extract interesting information.

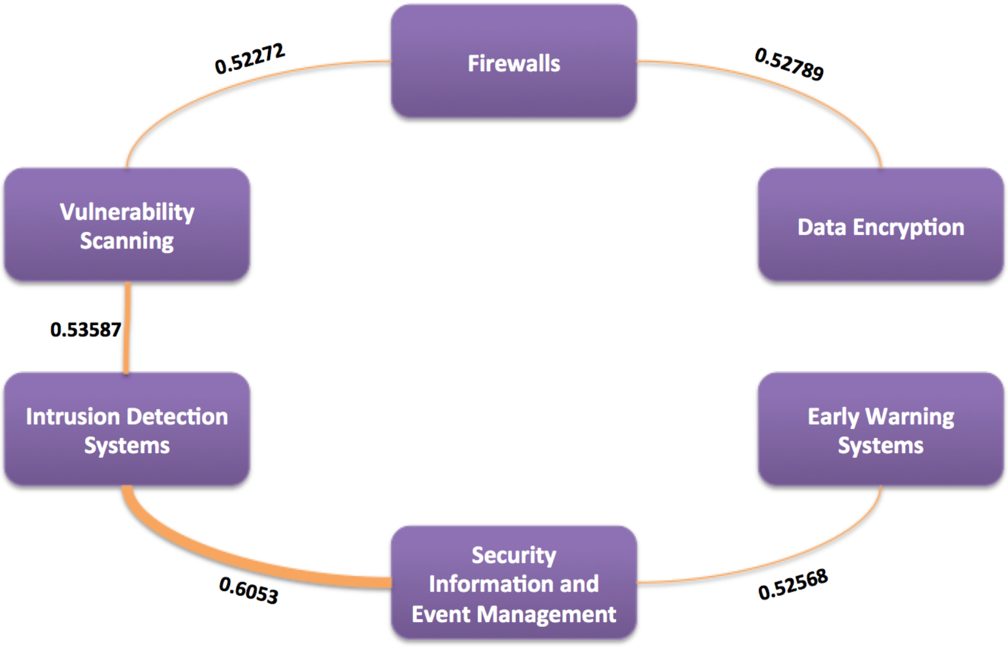

Figure 2 Relevant correlations from the survey (1/2)

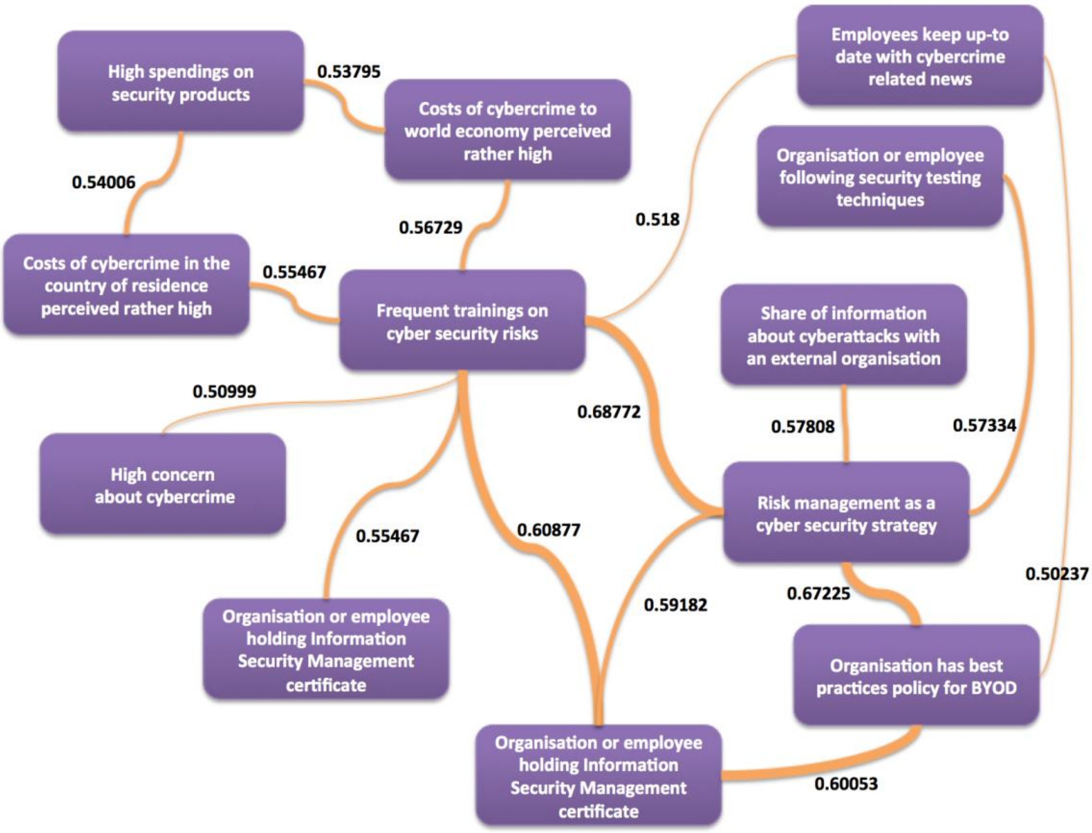
High spendings on security products
0.53795
Costs of cybercrime to world economy perceived rather high
Employees keep up-to date with cybercrime related news
0.54006
Organisation or employee following security testing techniques
0.56729
0.518
Costs of cybercrime in the country of residence perceived rather high
0.55467
Frequent trainings on cyber security risks
Share of information about cyberattacks with an external organisation
0.50999
0.68772
0.57808
0.57334
High concern about cybercrime
Risk management as a cyber security strategy
0.55467
0.60877
0.50237
0.67225
0.59182
Organisation or employee holding Information Security Management certificate
Organisation has best practices policy for BYOD
Organisation or employee holding Information Security Management certificate
0.60053

Figure 3 Relevant correlations from the survey (2/2)

The number of respondents obtained was N=679, and the survey questions can be consulted in Annex B. Correlations values and p-values were computed using the 'Data Analysis Tool Pack' from Excel. More specifically, the p-values are computed following a two-tail Student t-distribution. Only p-values inferior to 0.05 have been considered. The significant correlations, which made sense regarding the context of the research questions, are presented below. Note, however, that some of the correlations were rather doubtful and did not provide definitive outcomes.

The survey shows that roughly the same number of respondents who have risk management policies also have policies about Bring-Your-Own-Devices (BYOD) best practices. The latter is often comprised within the former, such a result is to be expected. However, as only approximately half of the sample audience affirmed that such policies were in place, there is a large number of organisations without any sort of appropriate policy. Similarly, having risk management policies and having certifications in information security management also showed correlation – again, the two being often associated with one another. Having a risk management policy also strongly correlated, on the one hand, with concerns the respondents had about cybercrime and, on the other hand, with how often the organisation decided to give to its staff some training on the cyber security.

In turn, organisations which often give security trainings also appeared to be the ones that have best practices policies for BYOD. But giving security training is not a best practice for cyber security that comes on its own. Noteworthy, those who give regular security trainings to their employees also appear to have in place a range of other security measures: they use firewalls, antivirus software, share information about cyber-attacks with other organisations, and some of their staff hold information security management certificates. Participation in security trainings is also strongly correlated with the perception of high costs of cybercrime to the local and the global economy.

These points make intuitive sense, and the survey provides evidence to support this. The conclusions derived from the majority of correlations can be summarised in two statements. Firstly, the more an entity perceives cybercrime as being a salient problem to be wary of, the more it will invest in solutions to tackle the problem. Training is one of these solutions. However, the correlation between spending on cyber security and perception of cybercrime also comes up in other places. For instance, the more prominent companies are concerned about cybercrime in their country or even in the world, the more financial resources they are allocating for it. The second takeaway is that companies, which apply at least one security measure, have a strong tendency to apply many others. There are therefore noticeable cross-correlations between having in place the following security instruments: firewalls, antivirus, spam blockers, secure email gateways, data encryption, and back-up systems.

Concluding Remarks

9 A QUICK LOOK INTO THE FUTURE

Predicting the future is not only often ends up with failure, but also lacks a scientific and academic basis to do so. Yet it is a predominant question of interest for policy makers to know where to expect future threats and to direct accordingly the state security apparatus. It is similarly of interest to many companies' executives looking ahead at the risks they may soon face and at how they can adapt their strategies to best tackle them. This interest explains the recurrence of the theme and its own importance for cyber security.

At least two viewpoints, almost opposite to each other, exist on the topic. On the one hand, some scholars insist that it is possible for certain people to garner enough knowledge to be able to make certain predictions correctly. More precisely, the psychology researcher Philip Tetlock put forward a two-pronged empirically tested argument that "how you think matters more than what you think", which in turn implies that generalists fare better at predictions than experts. The type of knowledge to acquire would hence rather have to be broad than in-depth.[76] On the other hand, the much-publicised 'theory of the Black Swan' holds that the most impactful events in our society are outliers and cannot be predicted.[77] This holds true for 9/11, the success of Harry Potter, or the invention of Google and Facebook.

With this in mind, a middle ground would have to be considered, while staying very modest: What would best practices look like in the near future? What will be the questions to arise in the near future?

Tetlock's theory, and even less so with the 'Black Swan' one, does not lend a very workable methodology to approach these questions. But Google's chief economist, Hal Varian, puts forward an elegant solution. According to him, 'to predict the future, we just have to look at what rich people already have and assume that the middle classes will have it in five years and poor people will have it in 10'.[78] Applying this rule, which best practices can the richest companies of the moment afford that others cannot?

Firstly, there are concerns within the field of intelligence. With good intelligence on cyber threats, companies are able to know what they need to focus on to prevent adversaries getting into their network. Acquiring intelligence feeds does not come cheap, especially if one wants to acquire very specific intelligence about sophisticated and persistent threat actors. An intelligence feed from one provider can cost hundreds of thousands of dollars per year. Regarding that each provider can have

[76] Philip E. Tetlock, *Expert Political Judgement: How Good Is It? How Can we Know?* (Princeton: Princeton University Press, 2005).

[77] Nassim Nicholas Taleb, *The Black Swan: the impact of the highly improbable* (New York: Random House, 2007).

[78] Evgeny Morozov, 'Facebook isn't a charity. The poor will pay by surrendering their data', *The Guardian*, 26 April 2015.

an area of specialisation with specific sensors in a part of the world able to catch interesting pieces of malware, a well-off company is able to acquire several of them and have a very specific picture of the threats.

This leads to the second point. Intelligence feeds represent only one source of information. Ideally, many sources must be brought together in order to one being able to see patterns and reveal correlations. To do so, one also needs a specific product. And products in the field of 'big data' — which are able to draw correlations between different data sources (for example what the company Palantir does) — also can easily involve costs of one million of dollars or more per year.

Thirdly, once a company is able to receive functional intelligence to defend its network, a next step may be to elaborate a strategy to completely take the adversaries out by incapacitating them – this would mean putting instigators of attacks behind bars. And this requires working closely with law enforcement agencies. Arguably, only large companies forward cases (and possibly receive intelligence back from authorities) to the law enforcement agencies. Smaller companies or those with fewer resources may still think that it may not be worth the trouble, and that the reputational damage coming out of such a procedure could be greater than the return. With time, as processes develop, companies may be increasingly comfortable in coming out about attacks they have undergone, and in working hands-in-hands with authorities to try to work out the diplomatic challenges foreign-based attackers can represent.

Taking this view, it means that in the short-run, technology making sense of 'big data' will become more and more available, while technical data on cyber-threat may become less politicised, and henceforth more easily exchanged between entities. This would ensure a better flow of information between different organisations guaranteeing that attacks are detected and thwarted early. The legal basis for this type of exchange as well as the bureaucratic hurdles would have been mostly overcome. People would then know what the process looked like and would follow it timely, for instance, when an intelligence agency detects that a company could be a potential victim.

Intelligence as a best practice is a long shot from the current situation. As showed the result of the survey presented in the earlier section, the current focus is rather on 'bring-your-own-devices' or applying at times conflicting standards issued by international organisations. However, the approach to cyber security may be slowly moving to that direction – given that no other revolutionary breakthrough of 'Black Swan'-type occurs.

Observations of the issues highlighted in the present work provide insights on the possible research gaps in this area. For example, can best practice implementation in consumer services be used as an effective control mechanism to reign in errant organisations? Is this a neglected option to ensure that end-users are kept safe from cybercrime? Imposing heavy fines on service providers, device designers, etc., who failed to provide a service or product that was fit for service can act as a stimulus to make certain that all possible loopholes have been closed, i.e., that hosting providers are not allowing cybercriminals to host malicious traffic from their networks.

One of the challenges is how to bring about the different existing standards in diverse sectors within a large industry area, for example, critical infrastructures. Standardised best practices need to be flexible enough to be appropriate without being so generic to render them practically useless. Again, what works for large multi-national corporations with large resources may tie down SMEs.

Best practices can be applied to technical measures as well as organisational ones. As the CyberROAD survey shows, there is a mismatch between the number of organisations who allow BYOD and those with best practice policies for these devices. This may be more than a purely technical problem but also an organisational one too? How can the uptake fo r best practices be further improved?

One potential problem area requiring more research is the apparent mismatch between the creation and implementation of standards and guidelines in the EU and the US as the latter has a more established track record in this area. One possible reason is an historic preference in the US for consumer rights groups which are self-regulating whereas in Europe the tendency is for governmental regulatory consumer support systems. Or it could simply be that strong leadership has lacking on the European side to push these concepts forward.

Understanding the connectivity between critical infrastructures and related sectors is crucial if vital national and international services are to be protected from cyber attacks. These calls for collaboration and a great deal of transparency, if we want the initiatives in this area to be successful. More research here is needed.

There exists a functioning working group overseeing the processes that are need to keep smart grids safe but this is not the case in all other sectors (e.g. communication, oil and gas, water). This indicates that there may exist a research gap that requires due attention.

Annexes

10 Annex A: Important security standards for industrial control systems

Name	Type	Brief Description
IEC 62351 Parts 1-8 Information Security for Power System Control Operations	(Family of) Standard(s)	It defines security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation and protection.
IEC 62210 Power system control and associated communications.	Technical Report	It applies to computerised supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems.
IEC 62443 (formerly ISA 99) Security for industrial process measurement and control: network and system security	Standard and Guidelines	A series of standards, technical reports, and related information for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.
IEC 62357 Power system control and associated communications	Technical Report	It is a technical report describing all the existing object models, services, and protocols developed in technical committee 57 and showing how they relate to each other. It also presents a strategy showing where common models are needed, and if possible, recommending how to achieve a common model. This publication is of core relevance for Smart Grid.
IEEE 1686-2007 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Standard	It defines the functions and features to be provided in substation intelligent electronic devices (lEDs) to accommodate critical infrastructure protection programs. The standard also addresses security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED.
IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security	Standard	It identifies and discusses security issues related to human intrusion upon electric power supply substations. It also presents various methods and techniques that are currently used to mitigate human intrusions.
IEEE 1711 Trial-Use Standard for a Cryptographic Protocol for Cyber Security Substation Serial Links	Standard	It defines a cryptographic protocol to provide integrity and optional confidentiality for cyber security of serial links. This standard is independent of the underlying communications protocol.
ISO/IEC 27000 Information security standards	(Family of) Standard(s)	The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system. The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues

NISTIR 7628 Guidelines for Smart Grid Cyber Security	Guidelines	It presents an analytical framework that organisations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.[79]
NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	Guidelines	It provides a catalog of security and privacy controls for federal information systems and organisations and a process for selecting controls to protect organisational operations (including mission, functions, image, and reputation), organisational assets, individuals, other organisations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.[80]
NIST SP 800-82 Guide to Industrial Control System (ICS) security	Guidelines	The purpose of this document is to provide guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions.[81]
NERC CIP-002-1/009-2	Standard	NERC Standards CIP-002 through CIP-009 provide a cyber-security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognise the differing roles of each entity in the operation of the Bulk Electric System as well as the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.[82]
Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendation for standards developer	Guidelines	This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. This catalog is not limited for use by a specific industry sector. All sectors can use it to develop a framework needed to produce a sound cybersecurity program.[83]

[79] Smart Grid Interoperability Panel (SGIP), 'Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security',(2010).

[80] National Institute of Standards and Technology, 'Security and Privacy Controls for Federal Information Systems and Organizations',(2013).

[81] 'Guide to Industrial Control Systems (ICS) Security',(2011).

[82] North American Electric Reliability Corporation (NERC), 'Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification',(2006).

[83] Department of Homeland Security, 'Catalog of Control Systems Security: Recommendation for standards developer',(2011).

11 Annex B: A copy of the survey for questions pertaining to 'best practices'

(This corresponds to questions 6 to 9, which are the only questions pertaining to best practices; see next page)

6. What risks are you exposed to?

i. Does your organisation (or do you) apply risk management as part of a cyber security strategy?

○ Yes ○ No ○ Don't know

ii. Does someone in the company (or do you) formally and regularly keep up-to-date with cybercrime related news via…?

○ Generic newspapers and news broadcaster
○ Specialized news sources
○ Consulting companies
○ Activities outsourced to external company/ies
○ Social network contacts
○ No time allocated to do this

iii. How often are staff given training about cyber security risks?

○ Weekly
○ Monthly
○ Yearly
○ Never
○ Only if there is a problem
○ Don't know

iv. Does your organisation allow the use of Bring Your Own Devices (BYOD)?

○ Yes ○ No

v. Does your organisation have a best practices policy for BYOD?

○ Yes ○ No ○ Don't know

7. The effects of cybercrime

i. Have you experienced a cybercriminal action in the last 5 years in a...?

□ Personal capacity □ Through work □ Never

ii. If you have been a victim of cybercrime in the last 5 years, what was the effect of the action?

□ Loss of money □ Inconvenience □ Loss of reputation

□ Down time □ Psychologically harmful □ No effect

iii. As a direct result of a cybercriminal attack or threat, did you/your work make any changes to the cyber security strategy?

○ Yes ○ Don't know

○ No ○ N/A

iv. If you have experienced a cyber attack, do you think it posed a systemic risk to you or your organisation?

○ Yes ○ No ○ Don't know

v. If you have been a victim of cybercrime, what action followed?

○ Reported to the police with no further action

○ Reported to the police, who contacted me/my organisation but no further action took place

○ Reported to the police, who followed it through but no prosecution took place

○ Reported to the police, who followed it through to successful prosecution

○ Not reported to police

○ Didn’t know how to report to the police

○ Other

vi. If you have been a victim of cybercrime, did you contact your national or government CERT for assistance?

○ Reported to national or government CERT, with no further action

○ Reported to national or government CERT, with action on their part

○ Did not contact CERT but I know the police did

○ Did not contact my national or government CERT because I thought it was irrelevant

○ Did not know I could report to a CERT

○ Do not know what a CERT is or how to contact them

8. Security Management

i. Which of the following security applications do you use on your own computing devices?

□ Firewalls
□ Antivirus
□ Vulnerability scanning
□ Spam blocker/secure email gateway
□ Data encryption
□ Early warning system
□ VOIP encryption
□ Password manager
□ VPN
□ Hash generator
□ Back-up system (cloud or onsite)

ii. Which of the following security applications does your organisation use?

□ Firewalls
□ Antivirus
□ Vulnerability scanning
□ Spam blocker/secure email gateway
□ Data encryption
□ Other (please specify)
□ Early warning system
□ VOIP encryption
□ Password manager
□ Hash generator
□ VPN Dedicated resources
□ SIEM (Security information and event management)
□ Back-up system (cloud or onsite)
□ IDS/IPS solution
□ DLP solution

iii. How is your own/your organisation's cyber security managed?

○ In-house by someone who is in charge of (security) policies on behalf of the organisation, e.g., a sysadmin?
○ In-house CERT
○ I manage my own cyber security
○ Outsourced to a independent specialist or organisation
○ By the Internet Service Provider
○ Don't know

iv. Do you, or does someone else in your organisation, share information about cyber events/attacks with an outside organisation?

○ Yes ○ No ○ Don't know

v. Do you/your organisation hold any Information Security Management certificates, e.g., ISO 27001?

○ Yes ○ No ○ Don't know

vi. Do you/your organisation use the following security testing techniques?

○ Penetration testing
○ Vulnerability testing
○ Audits
○ Other
○ Don't know

4. Reducing risk & raising awareness

i. Survey 1 respondents indicate BYOD is now common within the workplace but rates of best practices/guidance on safe usage are low. How highly do you rate this as a potential security risk?

○ High risk ○ Medium risk ○ Low risk ○ Not a risk

ii. Do you think that there is a need for BYOD security policies to be introduced in every organization?

○ Yes ○ No

iii. Many respondents indicated a general lack of formal policies dedicated to cyber security management in their place of work. Why do you think this is?

○ Insufficient awareness within executive management

○ Insufficient resources to prepare the documents

○ Insufficient knowledge to prepare the documents

○ There is no need for such policies

iv. Benchmarking and industry best practices are used to measure performance, raise standards and develop trust. How useful could these tools be in improving the security performance of organisations?

○ Very useful ○ Useful ○ Not useful

v. For most Survey 1 respondents staff training in cyber security prevention only takes place when there is a problem or, at best, once a year. Why do you think this is?

○ There is no need to give regular security training to all staff

○ Only specific staff i.e., those in a technical environment, need regular training

○ Perceived low effectiveness of training

○ Lack of awareness in executive management

○ Lack of knowledge in the subject

○ Lack of time/human resources

○ Cost too high

AP. 'Officials say new anti-leak measures set at NSA'. *CBS News*, 18 July 2013.

Beiner, Ronald. *Political Judgement*. Illinois: Univeristy of Chicago Press, 1984.

Berry, Tim. 'What Is a SWOT Analysis?'. *BPlans*, 4 October 2008.

Biuro Bezpieczeństwa Narodowego [National Security Bureau]. 'Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej [Cybersecurity Doctrine of the Republic of Poland]'. Warszawa: BBN, 2015.

Bretschneider, Stuart, Frederick J. Marc-Aurele Jr., and Jiannan Wu. '“Best Practices” Research: A Methodological Guide for the Perplexed'. *Journal of Public Administration Research and Theory* 15, no. 2 (2004): 307–23.

BSA. 'Country: Poland'. BSA, 2014.

CEN-CENELEC-ETSI Smart Grid Coordination Group. 'Smart Grid Information Security'. 2012.

———. 'Smart Grid Reference Architecture'. 2012.

———. 'Smart Grid Set of Standards (Version 3.1)'. 2014.

CEN/CENELEC/ETSI Joint Working Group. 'Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids'. 2011.

CERT.GOV.PL. 'Publikacje'. http://www.cert.gov.pl/cer/publikacje [12 May 2015].

CERT.PL. 'CyberROAD – Invitation to participate in the project survey'. http://www.cert.pl/news/9671/langswitch_lang/en [12 May 2015].

Cobb, Stephen. 'Cyber Security Road Map for Businesses'. *We Live Security*, 14 May 2013.

CyberPol. 'CYBERBOK© Cyber Crime Security Essential Body of Knowledge: A Competency and Functional Framework for Cyber Crime Management'. http://cyberpol.org/CYBERBOK.pdf [14 August 2015].

Department of Homeland Security. 'Catalog of Control Systems Security: Recommendation for standards developer'. 2011.

Dojkovski, S., Sharman Lichtenstein, and Matthew J. Warren. 'Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia'. Paper presented at the European Conference on Information Systems, St. Gallen, 2007.

Dyzurnet.pl. 'Dyzurnet'. http://www.dyzurnet.pl [12 May 2015].

ENISA. 'Cyber Atlantic 2011'. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 [1 May 2015].

———. 'ICS Security Related Working Groups, Standards and Initiatives'. Heraklion: ENISA, 2013.

———. 'Protecting Industrial Control Systems - Annex IV. ICS Security Related Initiatives'. Heraklion: ENISA, 2011.

———. 'Protecting Industrial Control Systems - Recommendations for Europe and Member States'. Heraklion: ENISA, 2011.

———. 'Protecting Industrial Control Systems. Recommendations for Europe and Member States'. Heraklion: ENISA, 2011.

European Commission. 'Directive on European Critical Infrastructures 2008/114/EC'. Brussels: European Commission, 2008.

———. 'European Programme for Critical Infrastructure Protection'. Brussels: European Commission, 2006.

———. 'A new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure'. Brussels: European Commission, 2013.

———. 'Policy on Critical Information Infrastructure Protection (CIIP)'. Brussels: European Commission, 2013.

———. 'Protecting Europe from large scale cyber-attacks and] disruptions: enhancing preparedness, security and resilience (COM(2009) 149 final)'. Brussels: European Commission, 2009.

———. 'Review of the European Programme for Critical Infrastructure] Protection (EPCIP)'. Brussels: European Commission, 2012.

———. 'Special Eurobarometer 423: Cyber Security'. Brussels: European Commission, 2015.

European Commission, and European Free Trade Association. 'M/490 EN - Smart Grid] Mandate - Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment'. Brussels: EC, EFTA, 2011.

Facts on File World News Digest. 'Rifkin Sentenced in Bank Theft'. *Facts on File World News Digest*, 30 March 1979.

Fundacja Dzieci Niczyje. 'The Nobody's Children Foundation'. [12 May 2015].

Gardner, Bill. 'AM cycle'. *The Associated Press*, 3 November 1978.

Geuss, Raymond. 'What is political judgement?'. In *Political Judgement : Essays for John Dunn*, edited by Richard Bourke and Raymond Geuss. Cambridge: Cambridge University Press, 2009.

Greenberg, Andy. 'McAfee Explains The Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim'. *Forbes*, 3 August 2012.

Heuer, Richards J. 'Limits of Intelligence Analysis'. *Orbis* 49, no. 1 (2005): 75-94.

IEC TC57 WG15. 'List of Cybersecurity for Smart Grid Standards and Guidelines'. http://iectc57.ucaiug.org/wg15public/Public Documents/List of Smart Grid Standards with Cybersecurity.pdf [4 March 2015].

International Organization for Standardization. 'An Introduction to ISO 27001, ISO 27002....ISO 27008'. International Organization for Standardization, 2015.

ISO. 'ISO 31000 - Risk management'. http://www.iso.org/iso/home/standards/iso31000.htm [14 August 2015].

ITU. 'Part 5: Security best practices'. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part05.aspx [1 May 2015].

Kalev, Alexandra, Frank Dobbin, and Erin Kelly. 'Best Practices or Best Guesses? Assessing the Efficacy of Corporate Affirmative Action and Diversity Policies'. *American Sociological Review* 71, no. August (589-617 2006).

Keeley, Gregory P. *Cybersecurity in Small Businesses and Nonprofits, Chapter 9 "Protecting Our Future: Educating a Cybersecurity Workforce"*. Vol. 2: Hudson Whitman/Excelsior College Press, 2013.

King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry*. Princeton, New Jersey: Princeton University Press, 1994.

Knapp, E. D., and J. T. Langill. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Waltham: Elsevier, 2014.

Kosinki, Jerzy. 'Cybercrime in Poland 2011-2012'. In *International Scientific Conference Archibald Reiss Days III*. Belgrade, 2015.

McKeown, Timothy J., and Alexander L. George. 'Case Studies and The- ories of Organizational Decision Making'. *Advances in Information Processing in Organizations* 2 (1985): 21–58.

MELANI, and GovCERT. 'Sécurité informatique: aide-mémoire pour les PME [IT security: a help for SMEs]'. Bern: MELANI, 2015.

Microsoft. 'Microsoft Security Intelligence Report '. http://www.microsoft.com/sir [12 May 2015].

Mindtools. 'SWOT Analysis: Discover New Opportunities, Manage and Eliminate Threats'. 2015.

Ministerstwo Spraw Wewnetrznych. 'Raport MSW o stanie bezpieczeństwa [Polish Ministry of the Interior reports on security in Poland]'. [12 May 2015].

Ministry of Administration and Digitisation, Internal Security Agency. 'Cyberspace Protection Policy of the Republic of Poland'. Warsaw: MAIC, 2013.

Morozov, Evgeny. 'Facebook isn't a charity. The poor will pay by surrendering their data'. *The Guardian*, 26 April 2015.

NASK. 'Cert Polska: Rapport 2014'. Warszawa: CERT Polska, NASK, 2014.

———. 'Papers'. http://www.cert.pl/raporty/langswitch_lang/en [12 May 2015].

National Institute of Standards and Technology. 'Guide to Industrial Control Systems (ICS) Security'. 2011.

———. 'Security and Privacy Controls for Federal Information Systems and Organizations'. 2013.

Nicolaus Copernicus University. 'Cybercrime Research Centre: Publications'. http://www.cybercrime.umk.pl/publications,7,en.html [12 May 2015].

North American Electric Reliability Corporation (NERC). 'Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification'. 2006.

Norton. 'Norton Cybercrime Report 2012'. http://us.norton.com/cybercrimereport [12 May 2015].

Overman, E. Sam, and Kathy J. Boyd. 'Best Practice Research and Postbureaucratic Reform'. *Journal of Public Administration Research and Theory* 4, no. 1 (1994): 67-83.

Pinzon, S. 'Top 10 Threats to SME Data Security'. WatchGuard Technologies, 2008.

Policja. 'Statystyka'. http://www.statystyka.policja.pl/ [12 May 2015].

Polish Safer Internet Centre. 'saferinternet.pl: Keeping children and young people safe online'. http://www.saferinternet.pl/en/ [12 May 2015].

PwC. 'Economic Crime Survey Poland 2014'. Warsaw: PwC, 2014.

Quincy, Ronald, Shuang Lu, and Chien-Chung Huang. 'SWOT Analysis: Raising Capacity of Your Organization'. Rutgers University, Beijing Normal University, 2012.

Roberts, Dexter. 'Chinese Hackers Like a 'Drunk Burglar,' 'Kicking Down the Door,' Says FBI Director'. *Bloomberg*, 6 October 2014.

Smart Grid Interoperability Panel (SGIP). 'Introduction to NISTIR 7628 - Guidelines for Smart Grid Cyber Security'. 2010.

SmartGrids. 'CEN / CENELEC / ETSI: Smart grids and standardization'. http://www.smartgrids.eu/CEN-CENELEC-ETSI [1 May 2015].

Streider, Wolf. 'Is a SWOT analysis a reasonable starting point for a risk assessment? Discuss'. https://www.linkedin.com/grp/post/1834592-240204315?goback=.gmp_1834592 [14 August 2015].

Symantec. 'Symantec Internet Security Threat Report 2014'. Symantec, 2014.

Taleb, Nassim Nicholas. *The Black Swan: the impact of the highly improbable*. New York: Random House, 2007.

Tetlock, Philip E. *Expert Political Judgement: How Good Is It? How Can we Know?* Princeton: Princeton University Press, 2005.

The Washington Post. 'Bank Was Unaware of Swindle'. *The Washington Post*, 11 November 1978.

Verizon. 'The 2012 Data Breach Investigations Report'. Verizon, 2013.

Veselý, Arnošt. 'Theory and Methodology of Best Practice Research: A Critical Review of the Current State'. *Central European Journal of Public Policy* 5, no. 2 (2011): 98-117.

Wason, Peter C. 'On the Failure to Eliminate Hypotheses in a Conceptual Task'. *The Quarterly Journal of Experimental Psychology* 12, no. 3 (1960).

White House. 'Homeland Security Presidential Directive/HSPD-7'. 17 December 2003.

———. 'Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience'. 2013.

World Economic Forum, and Deloitte. 'Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience'. World Economic Forum, 2012.

Zappa, F. 'Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level'. Unicri, 2014.