



Funded by the European Commission

Seventh Framework Programme



CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D5.1 Stakeholder needs and threats evaluation

Date of deliverable: 31/05/2015
Actual submission date: 31/05/2015

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 under the Seventh Framework Programme		
Restriction Level		
PU	Public	Yes
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)	No



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

Revision history

Version	Object	Date	Author(s)
0.1	Creation	02/03/15	CyberDefcon
0.2	Revision	12/05/15	CyberDefcon UNICA NASK
0.2	Revision	14/05/15	CyberDefcon UNICA NASK
0.3	Revision	18/05/15	CyberDefcon CEFIEL INOV
Review	Review	18/05/15	SUPSI
0.4	Revision	19/05/15	CyberDefcon
Review	Review	26/05/15	McAfee
0.5	Revision	26/05/15	CyberDefcon NASK
1.0	Final draft (submission)	29/05/15	CyberDefcon



D5.1

Stakeholder needs and threats evaluation

Responsible
(CYBERDEFCON)

Contributor(s)
(CYBERDEFCON)
(UNICA)
(NASK)
(INOV)
(CEFIEL)
(TUD)
(POSTEIT)
(VITROCISSET)
(SBA)
(PJ)
(SUPSI)
(McAFEE)



Summary:

The viewpoint of the stakeholder provides the focal point from which the current cybercrime landscape is observed. By proactive means of observation and assessment the possible directions for the future conduct of research and development into appropriate solutions for cybercrime is explored. Crucial to these objectives is to understand what is meant by the terminology across the current landscape. Cybercrime and threats have a variety of meanings and connotations which affect attitudes, perceptions and actions. In exploring these issues from the stakeholders' perspective the aim is to highlight the need for a cohesive approach to finding solutions that are appropriate for the threats of the future. This approach brings together the views of the different stakeholders and challenges whether current solutions to cybercrime are fit-for-purpose, starting at the ground level. Without this knowledge it is not possible to know if the right course of actions are being followed. Key to understanding these topics is the ability to apply appropriate and standardised metrics such as benchmarking and best practices so that progress can be assessed and measured. Having these basic elements in place and appropriately available are crucial factors in ensuring return on investment (ROI) that is befitting the sums being spent. This study explores these topics using comparative analysis and surveys in order to unearth the current gaps so that future money is spent on productive areas of research rather than outdated or ineffectual resources.

Keywords:

Cybercrime, metrics, taxonomy, threats, measurement, survey, stakeholders, scenario, roadmap, definition, technology, privacy, cyber security, EU, Poland, intrusions, statistics, evidence-based practices



TABLE OF CONTENTS

1	INTRODUCTION.....	7
2	IDENTIFICATION OF STAKEHOLDER NEEDS & THREATS.....	8
2.1	THE CYBERROAD TRIAD OF EVIDENCE-BASED PRACTICE	9
2.1.1	<i>Galilean EBP Category.....</i>	9
2.1.2	<i>Phenomenolist EBP Category.....</i>	10
2.1.3	<i>Aristotelian EBP Category.....</i>	10
2.2	STAKEHOLDER NEEDS & CONCERNS.....	10
2.2.1	<i>Cybercrime – What is it?.....</i>	10
2.2.2	<i>Cybercrime – The Past.....</i>	11
2.2.3	<i>Cybercrime – Impacts and Effects.....</i>	12
2.2.4	<i>Cybercrime - The Future.....</i>	13
3	ASSESSING STAKEHOLDERS NEEDS & THREATS – THE CYBERROAD SURVEY	15
3.1	THE SURVEY –A DELPHI APPROACH.....	15
3.1.1	<i>Survey Aim</i>	15
3.1.2	<i>Survey Methodology</i>	15
3.1.3	<i>Target groups.....</i>	16
4	THE CURRENT SECURITY LANDSCAPE – FROM MACRO TO MICRO	17
4.1	THE STATE OF THE ART – A MACRO PERSPECTIVE.....	17
4.1.1	<i>The Economics of Privacy (Acquisti et al. 2015)</i>	18
4.1.2	<i>Statistics and Metrics</i>	18
4.2	POLAND – A MICRO PERSPECTIVE	19
4.2.1	<i>CERT statistics.....</i>	19
4.2.2	<i>Police & Government statistics</i>	20
4.2.3	<i>National Cybersecurity Strategy with regards to Cybercrime (Poland).....</i>	21
4.2.4	<i>A Comparison of Statistics</i>	21
4.3	TECHNOLOGICAL LANDSCAPE	22
4.4	SOCIAL, ECONOMIC, POLITICAL, & LEGAL LANDSCAPES.....	22
4.5	THE THREAT LANDSCAPE	22
4.6	A QUESTION OF TRUST.....	23
4.6.1	<i>What is “trusted” data?.....</i>	23
4.6.2	<i>Who can be “trusted” with data?.....</i>	24
4.6.3	<i>The role of public sector / private sector / government/ governance, in information sharing</i>	24
4.6.4	<i>Trust – Summary of the Issues.....</i>	24
4.6.5	<i>A Searchable Database or Knowledge Base</i>	25
5	SURVEY ANALYSIS.....	26
5.1	SURVEY OVERVIEW – MACRO PERSPECTIVE	26
5.1.1	<i>Organisational – Macro view</i>	27
5.1.2	<i>Technology – Macro view</i>	28
5.1.3	<i>Social – Macro view.....</i>	29
5.1.4	<i>Legal – Macro view.....</i>	30



5.1.5	<i>Ethical – Macro view</i>	31
5.1.6	<i>Political – Macro view</i>	32
5.1.7	<i>Economic – Macro view</i>	33
5.2	AN EARLY ANALYSIS FROM A MICRO PERSPECTIVE (POLAND)	33
5.2.1	<i>The Eurobarometer Survey on Cyber Security</i>	34
5.2.2	<i>BSA Report on Legislation</i>	35
5.2.3	<i>Overview from a Micro Perspective - Poland</i>	35
5.3	EARLY SURVEY ANALYSIS CONCLUSIONS	36
6	ARE STAKEHOLDER NEEDS BEING MET?	37
6.1	CURRENT SCENARIO	37
6.2	FUTURE SCENARIO.....	37
6.3	STAKEHOLDER CONCERNS.....	38
7	CONCLUSIONS & RECOMMENDATIONS FOR THE GAP ANALYSIS	39
7.1	WHERE ARE THE GAPS – CONCLUSIONS & RECOMMENDATIONS	39
7.1.1	<i>Definitions & Taxonomy</i>	39
7.1.2	<i>Metrics</i>	40
7.1.3	<i>Trusted Data</i>	40
7.1.4	<i>Standards and Benchmarks</i>	40
7.1.5	<i>Threats and Cybercrime</i>	40
7.1.6	<i>Miscellaneous</i>	41
8	SENSITIVITY COMMITTEE REPORTS	42
	ANNEX A – SURVEY #1.....	44
	ANNEX B – SURVEY #2	45
	ANNEX C – SURVEY #3	46
	ANNEX D – THE DELPHI PROCESS IN PRACTICE	47
	ANNEX E - SURVEY #1 WHOLE TO POLAND COMPARISON	48
	ANNEX F – SEARCHABLE DATABASE – THE CURRENT LANDSCAPE.....	49
	BIBLIOGRAPHY	50



1 INTRODUCTION

The objective of D5.1 is to assess the needs of stakeholders and the threats that they are facing from cybercrime. A survey explores the current security landscape of existing EU-related threats, to provide high and low-level views of the issues and of the delivery *modus operandi* of the threats. Threats may be real or perceived; the aim is to observe stakeholders viewpoints both quantitatively and qualitatively as a topic of interest. Assessment of the stakeholders and their needs is a vital focus which is undertaken using innovative techniques to facilitate enquiry of the important questions for this task and for the rest of the work package, for example:

- a) What are the key interests/concerns of each stakeholder group?
- b) What does each stakeholder want/need?
- c) Can these needs be realistically met?
- d) Who will be affected?
- e) Who/how will the findings be implemented?

The current threat situation is a product of its historic evolution. This deliverable looks at the effect on the stakeholder and any existing gaps in terms of practices currently employed and what is needed for the future if solutions to cyberrime are to become a reality.

Key to this investigation is an exploration of innovative ways in which stakeholders can be engaged across the industry so that all the sectors affected by cybercrime are represented fairly and without bias. The needs of stakeholders in the light of technological, social, legal, ethical, political, and economic trends all have a bearing on preparedness of individuals and organisations for the future. The CyberROAD surveys explore these issues through in-depth analysis and it is expected that this approach will shed light on prevalent research gaps which will form a major contribution to the CyberROAD roadmap for the future.

For this deliverable, therefore, two vital lines of enquiry around stakeholders are needed: i) assessing the current threat status, and ii) assessing the needs both now and into the future. These two areas provide the focus for this body of work from which the outcomes will provide a major contribution towards the generation of research gaps in **D5.6 Cybercrime Research Topics**. The body of work contained within this deliverable will, therefore, provide essential research and contribute towards the lasting legacy of the CyberROAD project.



The role of stakeholders in relation to cybercrime and security is a topic debated by organisations with an interest in internet governance and multi-stakeholder perspectives which may differ from the views of technical experts and politicians (Lee, 2014). Stakeholders, who they are and how best to define them, remains an area for exploration which D5.1 approaches using innovation techniques that explore the multi-stakeholder model.

An initial approach to these ideas and strategies were outlined in WP2, in D2.1 (Section 4.4.2 ‘A Proposal for the CyberROAD Roadmapping Methodology’ Phase 1: Roadmap preparation). In D5.1 this methodology is applied as **an investigative process and as a means of rationalizing stakeholder needs and threats identification**. The ‘Evidence-Based Practices’ (EBP) model is used extensively in other fields and industries and provides a good analogy for the study of cybercrime.

The theory behind EBP can be traced back to “one of the fathers of epidemiology”, John Snow (Wikipedia, 2015), whose work in 1849, traced the origin of an outbreak of cholera to a single water pump, began a seismic shift towards observational and ‘evidence-based practices’ in preventative health-care and to the development of epidemiology as a study.

Epidemiology can bring valuable precepts to the study of cybercrime and can be paralleled in several ways:

- Epidemiology studies and evaluates the patterns that occur in different groups.
- Data collection and interpretation are key areas of study along with measurement of outcomes in order to assess risk.
- A target population or study sample are subjects of evaluation although this can be problematic depending on sample size and method of selection and depend upon subjective or informed judgement.
- Decisions arising from epidemiology relate primarily to groups and not individuals. (BMJ, 2015)

The potential for correlation between epidemiology EBP and cybercrime is **an area of exploration** in D5.1 as a potential and innovative method of categorizing sources of evidences from different stakeholders and as a novel way of exploring possible contenders for inclusion in the research gaps analysis.

To further this purpose in terms of D5.1 two distinct processes were designed:

1) A searchable knowledge bank (known as ‘The Database’) of literature, papers, books, articles, journals, publically available government publications, reports, legal documents, case driven studies, etc., from various sources.

2) An in-depth survey of stakeholders in order to assess their needs now and into the future.

Throughout these processes the ‘CyberROAD EBP Triad’ is used to categorise the sources of evidence as, in following the epidemiological approach, evidence is best observed from a sample, group or category. Evidences in ‘The Database’ are fairly straightforward to categorize according to the three evidence-based groups (Artistotelian, Galilean, and Phenomenalist) but more problematic for evidences (survey results) from the stakeholders.



The solution decided upon was to design a survey question where stakeholders (respondents) were asked to select the occupation group that most appropriately fitted to their own occupation. It was not known if this type of controlled grouping would work for the survey but it could provide an avenue for further exploration of categorization of sources according to 'EBP'. The usefulness would be in the ability to assess how balanced or representative the sources are in relation to the 'EBP Triad'. This is an area recommended for escalation to D5.6 and for the roadmap of research gaps.

2.1 THE CYBERROAD TRIAD OF EVIDENCE-BASED PRACTICE

The 'CyberROAD Evidence-Based Triad' is outlined as a directional basis for this project in D2.1. For D5.1 the 3 main categories of evidence-based sources; scientific evidence (Galilean), observatory based and event-driven case study experience (Phenomenalist), and consumer, political and commercial preferences (Aristotelian) are explored as a means to rationalize sources of evidences. To fit the purpose of this deliverable, the 'CyberROAD Triad' was adapted as represented in Figure 1.

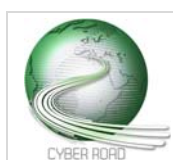


Figure 1 'The CyberROAD Triad of Evidence-Based Practice (EBP)

The approach is explained more fully in the following sections.

2.1.1 GALILEAN EBP CATEGORY

This category contains groups that contribute to knowledge on (or about) cybersecurity from a quantitative and/or research perspective, mainly guided by scientific theoretical background. Evidences from this category include international organisations e.g. Council of Europe, research



entities e.g. Ponemon Institute, educational institutions, ‘think tanks’ e.g. East West Institute, standard-setting bodies e.g. International Organisation for Standardisation (ISO), governments, etc.

2.1.2 PHENOMENOLIST EBP CATEGORY

This category contains groups that contribute to knowledge on or about cybersecurity from a practitioners’ or expert knowledge point of view. Evidences from this category include corporates and other entities that provide metrics and information on cybersecurity issues, such as Kaspersky Labs, McAfee, Trustwave, IBM (International Business Machines Corporation), etc., non-profits sharing metrics and expert knowledge such as Anti-Phishing Working Group, ENISA (European Union Agency for Network and Information Security), HostExploit, CERTs (Computer Emergency Readiness Team), service providers such as Internet Service Providers (ISPs), etc.

2.1.3 ARISTOTELIAN EBP CATEGORY

This category contains groups that do not apply the experimental scientific method, but mostly rely on intuition, pure reasoning and humanistic themes. Evidences from this category include for profit and non-profit organisations that represent the interests of consumers, end-users, businesses and humanist issues such as the Internet Corporation for Assigned Names and Numbers (ICANN), reporting entities, e.g. The Economist, regulators (government-approved or independent) e.g. The Office of Communications (OFCOM), Data Protection Authorities (DPAs), etc.

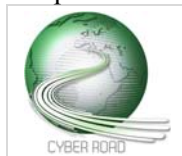
2.2 STAKEHOLDER NEEDS & CONCERNS

2.2.1 CYBERCRIME – WHAT IS IT?

Defining ‘what is cybercrime’ is an important focus of this deliverable and an area that is explored in detail in the D5.1 surveys. Currently a variety of definitions on cybercrime exist: this presents an acute problem for accurate study of the whole domain. For example, how can ‘cybercrime’ be measured or costed when cybercrime is interpreted differently by individual groups, organisations, governments, citizens, etc. The problems associated with the costing of cybercrime is discussed more fully in **D3.1 Social, Economic, Political and Legal Landscape Report, Section 3 Socioeconomic Lens of Cybercrime**) and in this deliverable in Section 4.1.1 The Economics of Privacy.

Since its inception in 2001 the Council of Europe’s **Budapest Convention on Cybercrime**¹ remains the only internationally ratified treaty. It is signed by a number of countries worldwide (55 ratifications and 8 signatures as 18.05.15). The ‘Budapest Convention’ serves to align international legislation and improve cooperation across borders by providing definitions of the types of activities recommended for criminalisation in the national law of member states, and guidance on procedures that member states are recommended to follow, for example, enabling law enforcement to gather appropriate evidences from service providers. ‘Additional Protocols’ are added when needed, for example, cyber terrorism activities as defined and entered on 1 March 2006 (Council of Europe, n.d.). A major criticism levied against the Convention, from some countries not signed up to the treaty, is that it violates a country’s own sovereign law.

¹ <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>



The difficulty in accommodating all the different stakeholder needs into a definitive statement, in terms of the objectives of the CyberROAD project, is discussed in **D2.1 Section 3 Cyber Security: Definitions and the Problem Space**. Here, cybercrime is defined as:

Cybercrime encompasses two forms of criminal activities: the use of computer systems to enable traditional forms of criminal activity (e.g., child pornography, money laundering); and the use of a computer system to launch a cyber attack (as understood by the aforementioned definition).

This description was arrived at by the CyberROAD team from an amalgamation of common conceptual distinctions found in many laws, academic articles or government reports, i.e., the Budapest Convention, United Nations Office on Drugs and Crime (UNODC, 2013). The latter document provides a reasoned argument of the need for a ‘core’ description of cybercrime while emphasising the point that an ‘aggregate’ concept may not befit ‘the art’ (Chapter 1: Connectivity and Cybercrime, pgs 1-22). The description arrived at in D2.1 was for illustrative and guidance purposes only and was further qualified by stating that definitions would be amended accordingly as the project progressed.

From D5.1’s viewpoint the emphasis is on the definition of cybercrime from the perspective of the different stakeholders and research gaps that may result from diverse perceptions, opinions and quantitative and qualitative sources. Definition is an area for survey analysis with more detail provided in [Section 3](#) and [Annexes A-E](#). It is anticipated that if major differences in stakeholder definition are exposed in the surveys these will be escalated to **D5.6 Cybercrime Research Topics** for further research gap analysis.

2.2.2 CYBERCRIME – THE PAST

The current landscape is shaped by its historical evolution which, for cybercrime, occurred over a relatively short time span. Rapid technological development and systems designed without security in mind (McGraw, et al., 2000) have enabled opportunistic cybercriminals to gain advantage over less ‘savvy’ entities. Worryingly, latest research from some quarters suggest that this situation continues into the technologies of the future, for example, application security firm Veracode found that Internet of Things (IOT) devices have “serious issues...” (Constantin, 2015).

As computerised communications spread among elite groups in the 1970s unlawful actions tended to be confined mainly to violations of privacy. Attackers then had no deliberate intention of causing harm to a victim but plied their activities as a platform for demonstration,: hackers used system intrusions and attacks as a way of testing themselves and to showcase their skills (Armin & Foti, 2015).

As the industry matured the advent of the Internet enabled communications on a global scale and facilitated a new breed of opportunistic ‘cyber’ criminal with the skills and ability to exploit flaws in the rapidly developed technologies. Users lacking the same level of knowledge and awareness of this new type of activity became easy victims. Cybercrime had arrived and with it a successful business model with excellent returns on investment (ROI). Data quickly became the new highly valued commodity which could be exploited via weaknesses in both the technology and its users.

Today, newer and more powerful technology further enhances the ability to launch, for example, bigger DDoS (Distributed Denial of Service) attacks across a wide range of industry types. Akamai Technologies, Inc observed almost a 90 percent increase in DDoS attacks in Q4 of 2014 compared to



Q4 in 2013 (Akamai Technologies, Inc, 2015). Correlation between the increase in DDoS attack traffic and unlawful intrusion attempts is illustrated in Figure 2 (CyberDefcon, 2015).

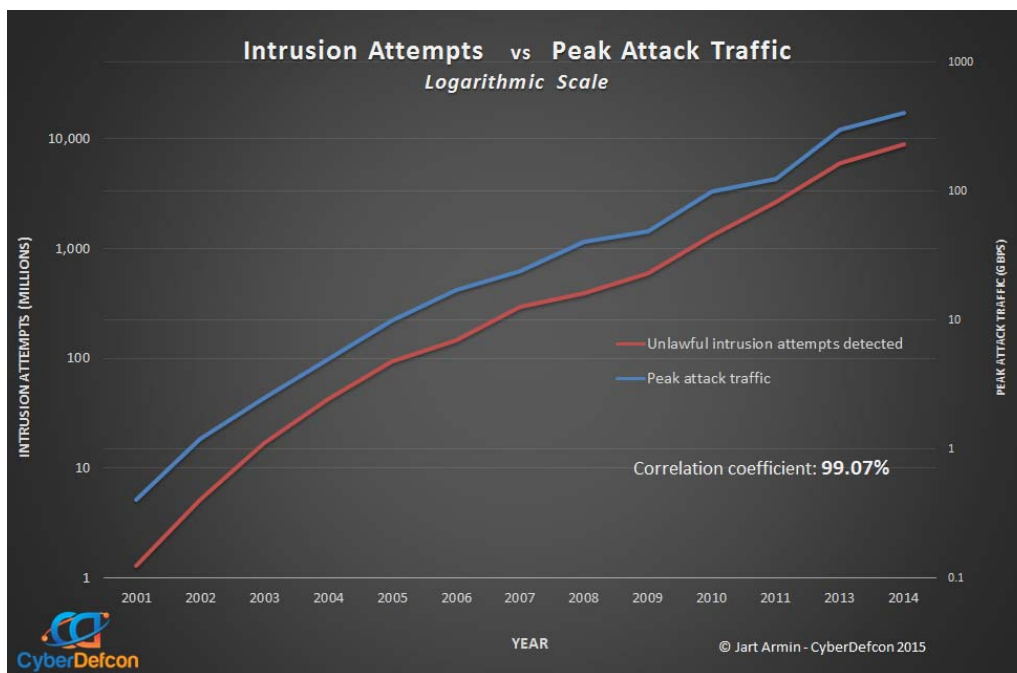


Figure 2: Intrusion Attempts vs Peak Attack Traffic 2006 – 2015

Despite the array of solutions on the market: anti-virus, firewalls, data encryption, spam blockers, etc., cybercriminal incidents continue to rise.

2.2.3 CYBERCRIME – IMPACTS AND EFFECTS

The effects and impacts of cybercrime is investigated via the stakeholder survey. These may be actual or perceived depending on the view point of the stakeholder. As well, the extent of any effect is bound up with an individual interpretation of what constitutes a cybercriminal action. The effect and impact may differ depending whether the target (perceived or real) is an individual or group/organization as may any following actions.

An act that is perceived as cybercrime by one entity may not be perceived in the same way by another and is, therefore, a subjective or intangible entity. ‘Loss of reputation’ is an example of such an effect and a domain that is difficult to quantify. There have been attempts to rationalize such costs within a framework for costing. Examples include, ‘External consequences and costs’ (Ponemon Institute, 2014), ‘damage to balance sheets’ (Ponemon Institute for Accenture, 2009) and ‘indirect cost’ (Anderson, et al., 2013) but these include different details and employ different methodologies. These labels are directed towards business costs; impacts and consequences on individuals requires a different approach. Until an effective method of measuring intangible effects is achieved there will be wide variations in any attempt to quantify the effects, consequences and costs in this area.

A regular survey on EU citizens’ ‘experiences and perceptions of cyber security issues’ is requested by The European Commission, ‘The Special Eurobarometer 423 Cyber Security’ (TNS Opinion & Social (requested by EU Commission), 2015). The latest survey conducted in October 2014 showed that, since the previous study in 2013, concern about cybercrime had increased. The CyberROAD surveys explore this area and comparisons will be useful in highlighting domains of concern.

2.2.4 CYBERCRIME - THE FUTURE

To arrive at any tangible solutions for the future, the present has to be observed and comprehended. That requires an ability to define and measure what is the current state and to project how this knowledge can be applied to the future. This is a topic that is explored throughout this deliverable using quantifiable and qualitative means to give an accurate picture of where we are, the gaps that exist in the knowledge, and how this can be resolved for the future.

Today, cybercrime is already multi-dimensional and with it sophisticated self-sufficient digital under and over ground economies have emerged, which uses data as an illicit commodity. It targets citizens, businesses and governments to obtain data, typically for financial gain. The cybercrime rate continues to increase in line with Internet adoption, mobile Internet access and deployment of broadband Internet, far too quickly for conventional law enforcement methods and particular initiatives to stop it (Global Economic Symposium, 2015) (Jeffray, 2014).

In this scenario, accurate trends and predictions for cybercrime attacks are severely difficult to draw for a distant future. However, some challenges may be pointed out that allow to deliver tangible solutions, when considering instead a near future (2-3 years) (Jeffray, 2014) (SysSec, 2013).

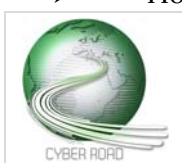
Thus, more than ever before, collaboration is a matter of utmost importance for any successful strategy to achieve the common goal of fighting cybercrime. Combined, well-coordinated and active partnerships of law enforcement, governments, academic sector, ICT industry, ICT security services, online financial services, etc., are necessary to leverage existing resources more effectively and timely, even acknowledging the fact that this cooperation between public and private sectors is by itself a challenge (SysSec, 2013).

A “mesh network” has to emerge from such a variety of stakeholders, to produce specific intelligence that should not only provide more accurate and comprehensive assessment of cyber criminality, but also to ensure that the responses are effective and prompt, especially when new clear threats and problems arise. ‘The Third Platform Innovation Stage’ (IDC, 2014) describes the anticipated explosion of new technologies and innovation predicted to arrive on the open market over the next few years. The main features of the expanding attack surface can be summed up as follows:

- As social media sites go mobile, payment mechanisms become more common, tablets and smartphones continue to penetrate the market, exploitation of specific vulnerabilities in these services and devices as well as advance of mobile malware become inevitable.
- The rise of the Internet of Things and expected boom of connected technologies as well as consumer-grade cloud services, where public and private assets are stored electronically rather than physically, will undoubtedly provide other opportunities for cybercriminals and raise additional problems for the security industry.

So, through collaboration, it is possible to make a few reliable and practical predictions on how the industry will shift over the next couple of years, pointing out the new threats and concerns, some key ones summarized in the previous paragraph. However, the challenges will be based on how this collaboration builds the intelligence capable to respond to the challenges posed by the following questions:

- How can the users control their data (for example, the process of their removal - deletion)?
- How can we enable users to have private communication in a public space?



- How shall we design compromise-tolerant systems to provide levels of liability, even if some of their components are compromised, enabling resilient services and solutions to exist?

These questions may, to some degree, be already partially fulfilled but full collaboration requires greater levels of transparency than currently exists. Transparency in the competitive environment of innovative technology is fiercely resisted by some quarters. For others it potentially means allowing access to state secrets or the ability to carry out unhindered surveillance. Communication in public spaces and privacy rights can be contentious issues and country specific. An important factor to consider is how greater integration of critical services to the digital world can be achieved without intolerable risk and fear for service users. Consideration of future impacts and effects in areas such as these would help to identify the technological gaps and address necessary research directions.



D2.1 (Section 4.2.4 Data Sources, and Information Collection and Processing) outlines the various techniques utilised to elicit knowledge. For the purpose of **D5.1** the Delphi method was chosen as the most appropriate approach for the survey component of the tasks. The Delphi methodology is particularly suited to forecasting trends in the future [Kanama 2013] and provides a **rational** approach to the collection of viewpoints and opinions. This is especially useful for D5.1 as respondent participation in further rounds of questionnaires gives the opportunity to investigate further on select questions. However, due to the time constraints within D5.1, it would be necessary to limit the number of survey rounds to an initial questionnaire, to begin the participation process and gauge interest in further rounds, followed by a second final round with the option of two surveys, each dedicated to a specialist area.

3.1 THE SURVEY – A DELPHI APPROACH

For D5.1 a broad-based Delphi approach² survey was designed by project partners with the aim of gaining an understanding of the impact of cybercrime on stakeholders and to use results to compare against other current research. This approach consists of an initial poll followed by two further surveys where participants of the first round are invited to complete at least one, or possibly two, subsequent polls (Hsu & Sandford, 2007). Participation is voluntary and further rounds of the survey are only distributed to participants who express an interest in contributing at the next stage. Answers from the first survey are used to generate more specific questions in the following rounds.

3.1.1 SURVEY AIM

The purpose of the CyberROAD survey is to explore and establish the needs of stakeholders and to find out what they see as the potential threats both now and into the future. As perceived threats may be different from real threats, it is important to try to correlate stakeholders' experiences of cybercrime with the situation as reflected in current reports and analyses. A mismatch between the two can be costly in terms of money spent on research and to stakeholders' understanding of what should or could be done to alleviate risk, i.e., are the right threats being targeted at present?, Can a blanket approach to security be taken or would a more flexible system be of more benefit?

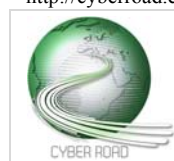
3.1.2 SURVEY METHODOLOGY

Survey 1 was prepared using specialist online software and designed along the lines of the Delphi method. The questions for this survey were of a generic nature as the intention was for Surveys 2 & 3 to explore resultant themes at a deeper level. To exploit the CyberROAD Cybercrime Survey a number of distribution methods were employed by project partners. These included the project website, a dedicated website³, announcements via social media (Facebook, Twitter, LinkedIn), and prompting by email to interested parties.

For the purposes of the CyberROAD project it was decided that the greatest value would be obtained from a comparative study using participants worldwide but with a bias towards European citizens. Using the Delphi method for the surveys made it possible to drawdown in order to probe further using selective criteria, if required. For a European project, it made sense to compare the region with others at a macro level i.e., world, and also at a micro level i.e., a specific country: Poland. Poland was selected

² http://en.wikipedia.org/wiki/Delphi_method

³ <http://cyberroad.eu/>



because it is one of the larger EU countries and is also represented by a national CERT team (CERT Polska) in the CyberROAD consortium. The participation of a national CERT allowed for easier access to various statistics on the threats affecting Poland and good potential outreach to other entities in the country as well as the general public which is especially important when disseminating surveys. The CyberROAD team decided that the surveys should be split into two versions: one for English speakers worldwide and the other translated into Polish and aimed at Polish users.

3.1.3 TARGET GROUPS

In Section 2.1, the 'CyberROAD Triad of Evidence-Based Practices' is outlined as applies to this deliverable. The model is used to example how epidemiological methods may be useful in cybercrime research areas. Respondent surveys are analysed individually and collectively according to occupation type or evidence source to introduce an element of innovation to observations.

Achieving a balanced representation across evidence source types is the ideal and it is hoped that with the varied outreach of CyberROAD partners this will be achieved. However, it is expected that interest in the surveys is most likely to be greatest from those already involved in the cyber security industry. Over representation of evidences presented from one or more sources may produce bias in the results.



To understand the current security landscape a wide range of topics need to be considered. The scale and effects of the modern phenomenon of cybercrime raises questions which has few, if any, precedents. Cybercrime is experienced around the world with few international agreements in place that adequately tackle the issues. Terminology, standards and practices are slow to mature and hinder progress towards cross-border compliance. Much of the difficulty stems from not knowing the extent of the problem which, in purely economic terms, affects budgets and forecasting from governments, to boards and to the end-user. Not knowing how big the problem is, is not exclusive to cybercrime but the industry's rapid global development has outpaced the ability to reach consensus on even rudimentary definitions. In terms of technology, and the need to take competitive advantage, the fast-paced development of concepts has been at the expense of security with the industry in a constant state of 'catch-up' with the cybercriminal.

Here, this dilemma is reviewed with views from a macro level (global) to micro level (Poland) through observations of the current security and threat landscape. The rationale for selecting Poland is explained in [Section 3.1.2. Survey Methodology](#). To review the whole security landscape is beyond the remit of the CyberROAD project but instead a snapshot of select areas is presented for observational purposes. This facilitates analysis of key areas which are further analysed via the CyberROAD surveys.

Wherever appropriate, the 'CyberROAD Triad of EBP' is used to exemplify how innovative but practical approaches can be applied to this area.

4.1 THE STATE OF THE ART – A MACRO PERSPECTIVE

There is no shortage of information to be found on any number of topics associated with cyber security. Taking the example of 'the cost of cybercrime', within the last 5 years there are 3,920 web searchable scholarly articles, papers and books on this subject alone⁴. Added to this is the wide spectrum of commercial sources collecting, collating and disseminating related information and data, some of which is not publically accessible.

The value and accuracy of the information provided in this domain is an area worthy of further research. However, an in-depth comparative study of all relevant reports is outside the remit of the CyberROAD project. Instead a sample of typical studies and reports provide the evidences for the purpose of research gap analysis. This was 'macro to micro' approach is a theme of this deliveable.

A review of a representative sample of five major studies on the theme of the "cost of cybercrime" together and one quantitative study with a focus on a specific attack type was undertaken for **D3.1 (Section 3.2 Review of the State of the Art of Metrics)**. These are not reviewed again here although observations from these reports will contribute to the overall analysis within this section. An additional study specifically explored the issue of the cost of privacy, the related cost of identity theft and data breaches relating to personal data. A review is presented here as a example of how this type of examination can provide valuable evidences for further study.

⁴ Google web browser search on 13.02.15



4.1.1 THE ECONOMICS OF PRIVACY (ACQUISTI ET AL. 2015)

'The Economics of Privacy' study (Acquisti, et al., 2015) provides an updated survey on the economics of privacy. The main focus is not on the abuse of personal data stored on computers, nor on data breaches, but on the value that can be attached to private data.

As soon as people consent to the use of their data for marketing purposes, than the value of the data can be associated to the gain that the user may acquire in terms of discounts or other privileges in their purchasing activities. The value of the data is quite different if measured at the subject's premises (small value), and at the marketing company's premises (high value).

Then, in the case of cybercrime, which value is to be associated with stolen/misused data? In the absence of crime this is made all the more difficult to compute.

This study clearly points out the three factors affecting the value of private data stored and shared over the Internet: individual responsibility, market competition, and government regulation. Individual responsibility requires awareness of the benefits and risks that sharing data brings in itself. Market competition exists to the extent to which to a value can be attached to this data. Finally, governments can regulate this market as it happens in other sectors.

At present, this topic is addressed in different ways in the EU and the US. While EU is steering towards government regulation on the management of private data, the US is drawing a framework that would allow different sectors to self-regulate this market. While estimates of the value of data breaches are available, e.g., the reports produced by the Ponemon Institute (Ponemon Institute, 2014), Verizon (Verizon, 2015), it is worth pointing out that the values tend to be in a quite wide range in the absence of market regulation rules.

The problems associated with computing appropriate values in costing data breaches is highlighted in a recent online article, 'The hotly disputed black magic of data breach cost estimates' (Hackett, 2015). Verizon's newly published report '2015 DBIR' (Data Breach Investigation Report) (Verizon, 2015) concludes with vastly different costing sums compared to Ponemon's reports. According to the article the cost-per-records unit number for Ponemone is 'roughly \$200' while for Verizon it is \$0.58 .The explanation for such a variation is attributed to the different data collection and computation methodologies used for each report. The authors of the Verizon report conclude that neither model is faultless.

4.1.2 STATISTICS AND METRICS

Statistics or metrics is a vitally important domain in the study of cybercrime. Assurance in the quality and origin of the data reinforces dissemination. A reliable source is a fundamental of trusted metrics. However, in an industry where few standards exist knowing what constitutes reliable information can be problematic. Measurement is key to seeking out solutions as the extent of the problem requires accurate assessment. No reliable method of costing cybercrime exists but basic statistics what can be measured with some certainty lays a foundation for further progress.

To give an overview of the current security landscape a select sample of available metrics are represented here. Costing cybercrime has no standard model but it is possible to outline cybercrime activity through a number of indicators. For example;

- There were over 1 million+ measurable cyber-attacks counted in October 2014 (Akamai, 2014)



- 7% of all URLs malicious (Barracuda , 2015)
- There is over 350 million+ in total identifiable malware (AV-TEST, 2015)
- 85% of processed emails are spam (Barracuda, 2015)

The above metrics give a snapshot indication of the levels of cybercriminal activities at any one time. Cybercriminal activity is variable and the same results may not be achievable on any given day. When applying metrics to cybercrime this variability in activity requires consideration.

Reliable and quantifiable data is a cornerstone for measurement and a topic requiring further research. The problem in achieving an agreed base unit cost per cybercrime is highlighted in [Section 4.1.1](#) above. The methodologies employed in achieving costing for insurance purposes or those for measuring the extent of a problem are most likely to be different with variables on either side. Questions that remain to be solved include, what is trusted data, and what data is pertinent?

4.2 POLAND – A MICRO PERSPECTIVE

There are few technical or academic articles that deal with the subject of cybercrime in Poland. 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, however, they do not provide any context or analysis of actual cases that have been handled and bottlenecks they experienced (an example list can be found in (Cybercrime Research Centre, n.d.). Non-security vendor driven research on the other hand tends to focus on compliance with EU regulation, usually in the broader cybersecurity context (a list of such research is presented below).

Foreign, often vendor driven, research on the other hand tends to focus on technical observations (for example, malware infection levels in the Microsoft Security Intelligence Report (Microsoft Corp, 2014)) or makes assumptions on the level of cybercrime losses (i.e. cost of cybercrime) in the country as a whole (Norton, 2012). Especially in the latter case it is very unclear how accurate this is (which is not just an issue that applies only to Poland) (Greenberg, 2012).

4.2.1 CERT STATISTICS

CERT Polska, operating as 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 (CERT Polska, 2014). For instance, it estimates that on an average day in 2014, there were 280 000 computers that had some form of malicious bot. Over 50 000 of these were infected with a type of banking Trojan - crimeware specifically written to facilitate financial fraud.

As part of its mission, CERT Polska regularly publishes information on specific mechanics of cybercrime, including a lot of statistics regarding malware on Polish networks, malicious URLs, phishing, spam, DDoS and Command & Control elements etc. A full list of publications is available (CERT Polska, n.d.).

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 (CERT.gov.pl, n.d.). Other Polish entities exist that publish cybercrime related statistics but from an Internet safety aspect (such as child safety online, child pornography and hate material); the saferinternet.pl programme (Polish Safer Internet Centre, n.d.), dyzurnet.pl (Dyzurnet, n.d.) and Fundacja Dzieci Niczyje (Fundacja Dzieci Niczyje, n.d.), are good examples.



4.2.2 POLICE & GOVERNMENT STATISTICS

The Polish Police does not provide detailed statistics relating to cybercrime in their public reports (Polish Police, n.d.). More information can be gleaned from the MSW (Ministry of the Interior) reports (Polish Ministry of the Interior, n.d.) that include general statistics in terms of the amount of cases and (selected) laws applied. 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 - it 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. Pedophilia 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 in artifacts coming from crime and illegal trade of goods of national heritage
9. Extortion or threats by organized crime
10. Hacking, sniffing, breaking into systems and malware
11. Illegal gambling online

The MSW report also summarizes 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 mostly either single to triple digit at most, it is not always clear if they concern cybercrime, as in the statistical system used by the Police in 2013 it is not obligatory to clearly state if a crime was committed on a computer network or the Internet.

For those that can be attributed to cybercrime, as understood by the MSW report, the only large number of offenses were "computer fraud" (26 945 cases) and "pedophilia and child pornography" (1648 cases). In terms of cybercrime cases that actually ended up in court, the numbers are just in the single or double digits. The top 2 categories: 57 persons tried (47 sentenced) concerned "computer fraud", and 33 persons tried (18 sentenced) concerned destruction or damage of computer data. 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 9 (5) and 6 (4) respectively.

As part of the CyberROAD we have submitted two requests for public information. One request was sent to the Polish Police (through Press Office of The Police Headquarters), and another one to the Ministry of Justice. The Police were asked about 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 show that an overwhelming majority of investigations are discontinued due to the inability to establish the perpetrator. Most crimes against information security are related to unauthorized access to information (Art. 267 of Polish 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,



which we queried for numbers of trials and average sentences. Sadly, only one in about fifty crimes identified by the police result in a final conviction, with an average sentence of less than 9 months (using the same Art. 267 as an example).

4.2.3 NATIONAL CYBERSECURITY STRATEGY WITH REGARDS TO CYBERCRIME (POLAND)

Two major documents exist in regards to Poland's approach to cybersecurity. The first document is the "Cybersecurity Doctrine of the Republic of Poland 2015" (currently only available in Polish as "Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015") (BBN (Biuro Bezpieczeństwa Narodowego - National Security Bureau), 2015). While the document is broad in terms of discussing different cybersecurity issues, it essentially glosses over the topic of cybercrime, referencing it only twice and mentioning that it should be addressed, failing to mention the role of the Police in doing so.

The second document (which has an English version) is called the "Cyberspace Protection Policy of the Republic of Poland" (Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej) published by MAIC in June 2013 (Ministry of Administration and Digitisation, Polish Internal Security Agency, 2013). While the document introduces the concept of cybercrime, even providing a definition "*an offence committed in cyberspace*" it also fails to elaborate on the topic.

It should be noted that none of these documents are acts of law and legally binding. It is expected that official legal acts in this area will be implemented once the EU NIS directive is established.

Nevertheless, it can be said that Poland currently lacks a comprehensive programme in combating cybercrime.

4.2.4 A COMPARISON OF STATISTICS

Reports in the statistics published by different parties signal a big disparity between the number of observed security (including cybercrime) incidents by CERT Polska and Government statics regarding cybercrime cases. Based on the surveys carried out in the CyberROAD project, it would appear that most cases are simply not reported to the Police. Subsequent Police investigations into cases appear to be not very effective, with few ending up in court. The situation can be summarized with a quotation from Jerzy Kosinski "Cybercrime in Poland 2011-2012 (Kosinski, 2012)":

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

This may be because the affected companies are determined to fight with this problem, and have the resources to hire law firms and push legal cases.

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."

The Eurobarometer survey 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” (Eurobarometer TNS Opinion & Social, 2014)

Further evidence to support the view that most cases of cybercrime are not reported to the police is found in The United Nations on Drugs and Crime (UNODC) report (UNODC, 2013), Annex 2 entitled, ‘Measuring Cybercrime’ (pgs 259 – 266):

“...police-recorded crime statistics capture only those events that come to the attention of the police.... For cybercrime events, the difference between victimization and police-recorded crime can be many orders of magnitude.”

This report continues by using data from the Norton Cybercrime Report 2011 (Symantec, 2011):

“According to one population based survey of almost 20,000 individual internet users in 24 countries, only 21 per cent of respondents who said that they had been a victim of any cybercrime act indicated that they had reported the act to the police.”

Survey results on this topic will be subject to further analysis and possible escalation to D5.6.

4.3 TECHNOLOGICAL LANDSCAPE

This aspect is covered in detail in **D4.1 “Technology Landscape Report”**. For D5.1 this topic will be explored more fully through survey questions to obtain a viewpoint from a stakeholders’ perspective..

4.4 SOCIAL, ECONOMIC, POLITICAL, & LEGAL LANDSCAPES

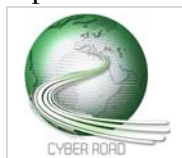
As a subject this area is covered in detail in **WP3 (D3.1 Social, Economic, Political & Legal Landscapes)**. For D5.1 these topics are explored mainly through this deliverable’s surveys. Survey #1 consists of a broad question base which Surveys #2 and #3 explore in more detail. It was considered if, for the second round of questions, there would be added value in designing a survey for each separate topic but in not wanting to make the surveys too laborious it was decided not to pursue that approach. Instead, for the second round there would be one technology-based survey and one survey that covered the other aspects – social, economic, political and legal.

In terms of the stakeholders, the ‘EBP Triad’ (see [Section 2.1](#)) is part of the analysis to determine in which category the sources from the stakeholder belong. This is to give an insight into the demographics of the participants in relation to the category of the stakeholder as a source (Aristolean, Galilean, Phenomolist) and to recognise the levels of representation across the social, economic, political and legal scale. This aspect will be escalated further for action in **D5.6**.

4.5 THE THREAT LANDSCAPE

Threats, what they are and what are the solutions, forms a major body of work within D5.4 Preliminary Cyber Security Solutions taxonomy for completion within D5.5 Cyber Security Solutions taxonomy. In D5.4 the importance of ‘Threat Modelling’ is outlined where the problem of technology designed without security as a priority is discussed. These issues have provided major impacts in the past and present a contributory reason for the vulnerabilities and weaknesses that cybercriminals have been able to exploit. If such issues are not addressed, similar problems will continue into the future.

ENISA provides a yearly overview of current and emerging cyber-threats in the showcase series of reports ‘ENISA Threat Landscape’ (ENISA, 2014). The 2014 report uses over 400 sources to display in



detail the emerging trends and top cyber threats. Changes in the threat landscape over the previous year, shown in graphic form, provide easy-to-understand formats of the most relevant movements in this domain. Following these movements over time may provide evidences towards accurate predictions of what is to come and what may be considered as a lesser threat. Such evidences are valuable for decision makers, security experts and interested individuals as an aid in future planning.

The information provided by ENISA in these reports provided guidance on threats that was useful in designing relevant questions for the CyberROAD cybercrime surveys. According to ENISA the top 10 threats in the emerging landscape are:

1. Malicious code: Worms/Trojans
2. Web-based attacks
3. Web application attacks /Injection attacks
4. Botnets
5. Denial of service
6. Spam
7. Phishing
8. Exploit kits
9. Data breaches
10. Physical damage/theft /loss

The ENISA report provided a useful model to form survey questions related to the likelihood of occurrence and risk. In Section 6 of Survey #2 ‘Threats’ (See Annex B) respondents were asked to rate the likelihood of occurrence of each of the ENISA top 10 emerging threats. This will provide interesting comparable data for further research and possible inclusion in D5.6.

4.6 A QUESTION OF TRUST

The notion of Trust is central in the security domain, as all the relationships among people, associations, companies, etc. are based on trust and reinforced by legal entities. Moreover, when decisions are to be taken on the policies needed to prevent security incidents, reliable information is needed on the probability of the events, on the data that can be targeted by attacks, and on the value of data loss and recovery. Consequently, sound metrics on the number of cybercrime events, their effects, and the damage that actually was caused from incidents is necessary for defence and recovery actions.

4.6.1 WHAT IS “TRUSTED” DATA?

Trusted data needs an agreed upon protocol for its acquisition, the measurements to be performed on the data, and the ways to securely store the data to prevent data pollution. Data in the cyber age, however, is a multi-faceted entity with few established guidelines, or classifications, for these processes. Data storage on the scale required today and into the future presents new challenges.

This chain can be enforced by clear national and supra national regulations that must require a uniform way for assessing the value of the assets in terms of data of companies, and the requirement to communicate any incident that has incurred, as well as a method for measuring the reach of the incident.



Incidents must be collected by a central point that ensures the correct processing of all data. This process in the EU is currently carried out by ENISA in an effort to provide for such trusted data. Metrics and protocols of communications still needs to be tailored in order to provide for data that should be not only be complete, but also reliable.

4.6.2 WHO CAN BE “TRUSTED” WITH DATA?

The adherence to standardized metrics and protocols allows trusting the party that provides such data. In other words, the protocols for gathering, processing and sending data to the central authority should provide in itself a means to assess the trust in those data.

4.6.3 THE ROLE OF PUBLIC SECTOR / PRIVATE SECTOR /GOVERNMENT/ GOVERNANCE, IN INFORMATION SHARING

The experience in UK (Cyber Essentials (UK Govt, 2015)) and in the USA (NIST CyberSecurity Framework (NIST, 2013)) provide examples of how metrics and procedures can be found by a joint effort of the private sector and the government. While the government acts as the central point for standardization of metrics and procedures that allows the production of official statistics, private companies must help in devising the set of mechanisms that can be actually implemented and represent the optimal trade-off between the cost of the solution and the data needed for the final assessment.

4.6.4 TRUST – SUMMARY OF THE ISSUES

There is no shortage of materials available that disseminate information and data. The question that arises is what is the value of these? The lack of quantifiable metrics, standards and practices makes this an unknown expanse. Reviews of small representative examples of a genre reveal a number of research gaps in this area.

A review of a small sample of the many studies available reveals a number of key areas where more research would be beneficial. Despite the lack of a common methodology where a like-for-like comparison becomes problematic, it is possible to thematically group the exposed research gaps. These form into five key areas:

- a) Definitions/Taxonomy
- b) Metrics
- c) Trusted Data
- d) Standards/Benchmarks
- e) Threats/cybercrime

At the centre and common to all groups is the issue of “trust”. This develops as a major theme that inter-links the individual parts. Diagrammatically, “trust” is a central supporting pivot.



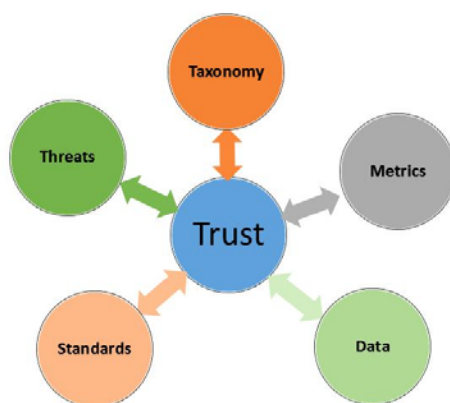


Figure 3: The Pivot of Trust

The groups surrounding the “Pivot of Trust” provide a structured foundation for the study of the research gaps in relation to current scenarios. Each group could be considered as a worthy standalone subject in its own right. Groups may overlap to a larger or lesser degree and may be disproportionate in terms of the subject range and extent but, in terms of importance to Trust, each has equal value.

The above scenarios will be recommended for further research in D5.6.

4.6.5 A SEARCHABLE DATABASE OR KNOWLEDGE BASE

Section 4 has provided an overview of a number of perspectives that form the state-of-the-art. Although it’s not possible to review every report and research paper in this assessment, a different approach was begun that could provide a lasting legacy beyond the end of the project.

In bringing together the evidence-based practices of ‘The Triad’ a searchable database was compiled to act as an aid for relevant references that have either been used in the project or have relevance to the state-of-the-art. The database contains references categorised according to the 3 groups and embodies the aims of D5.1 in using innovative practices to further the purposes of research.

The database will continue to be populated and developed as the project progresses (See Annex F).

It is anticipated that under or over representation of topics or areas of study will be revealed over time as more records are added. Work on this will continue beyond D5.1 and may contribute towards a full review of the current state of the art which is a research topic in its own right. This could serve as a useful central repository for references for other EU projects and save precious research time at the start of projects.



Continuing with the theme of a macro to micro analysis and to provide an early snapshot appraisal of the surveys it was decided that a specific country, Poland, should be used to compare with other regions. Poland was selected as it is one of the larger EU countries and is also represented by a national CERT team (CERT Polska) in the CyberROAD consortium. A Polish translation of both rounds of the Delphi-type questionnaire were prepared and made available through network connections, colleagues, CyberROAD.eu website and social media outlets.

Results from the Polish survey were compared against two other recent and well respected surveys: a) The Eurobarometer survey (conducted Oct 2014) on Cyber Security for the European Commission (Eurobarometer TNS Opinion & Social, 2014) and b) "EU Cybersecurity Dashboard" study by the BSA released in March 2015 (BSA, 2015).

5.1 SURVEY OVERVIEW – MACRO PERSPECTIVE

In following the Delphi survey approach **Survey #1 Cybercrime** was designed to include a wide range of topics within the scope of cybercrime. A few points of interest are:

- Overall participation was good with over 600 respondents completing the whole English version (as at 11th May 2015).
- Some questions had considerably more respondents (up to 850) than others.
- More than 200 respondents volunteered a contact email address for further participation in Surveys 2 & 3.
- For the Polish version over 350 participants completed Survey #1 (as at 11th May 2015).
- Respondents came from 42 countries around the world although the largest groups were from Switzerland, Italy, Portugal, United States, UK, Greece and Austria.

Survey #2 (Technology & Organisation) and **Survey #3 (Economic, Political & Social Issues)** were prepared using early results from Survey #1. The process involved is depicted in **Annex D**. All 3 surveys are ongoing in order to gain as much input as possible. A final cut-off date has yet to be decided and all end results will be escalated to D5.6 for further analysis.

In the following sections an early sample analysis for each topic type is represented. This serves to illustrate themes suitable for escalation to D5.6. Survey questions are available in Annexes A-C.

Note: All data is from responses available as at 11th May 2015.



5.1.1 ORGANISATIONAL – MACRO VIEW

The definition of cybercrime is a key topic for this deliverable and is a recommended theme for further research. Answers from the question “For me, cybercrime is ...) in Survey #1 (Figure 4) indicate that definitions of cybercrime vary greatly. Results from organisational based questions will contribute towards **D5.6 Cybercrime research topics**

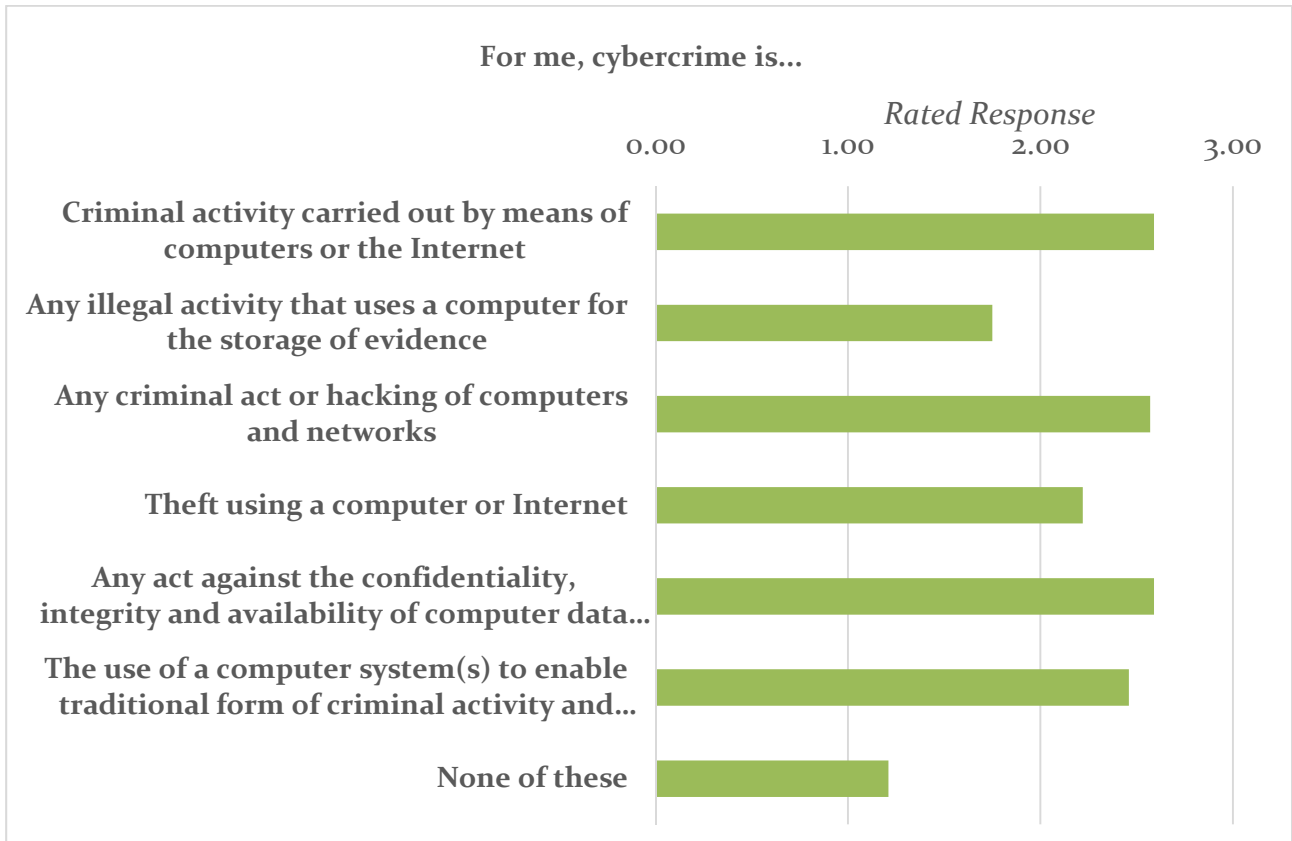


Figure 4: Cybercrime definition



5.1.2 TECHNOLOGY – MACRO VIEW

Enquiry into Technological themes is of major interest with questions covering a wide range of aspects. The sample in Figure 5 shows the most widely adopted security applications used by individuals. Figure 6 shows those used by organisations. Results from technology based questions will contribute to **D5.6 Cybercrime research** topics. The variation between the results is of note. Refer to surveys in **Annexes A-C**.

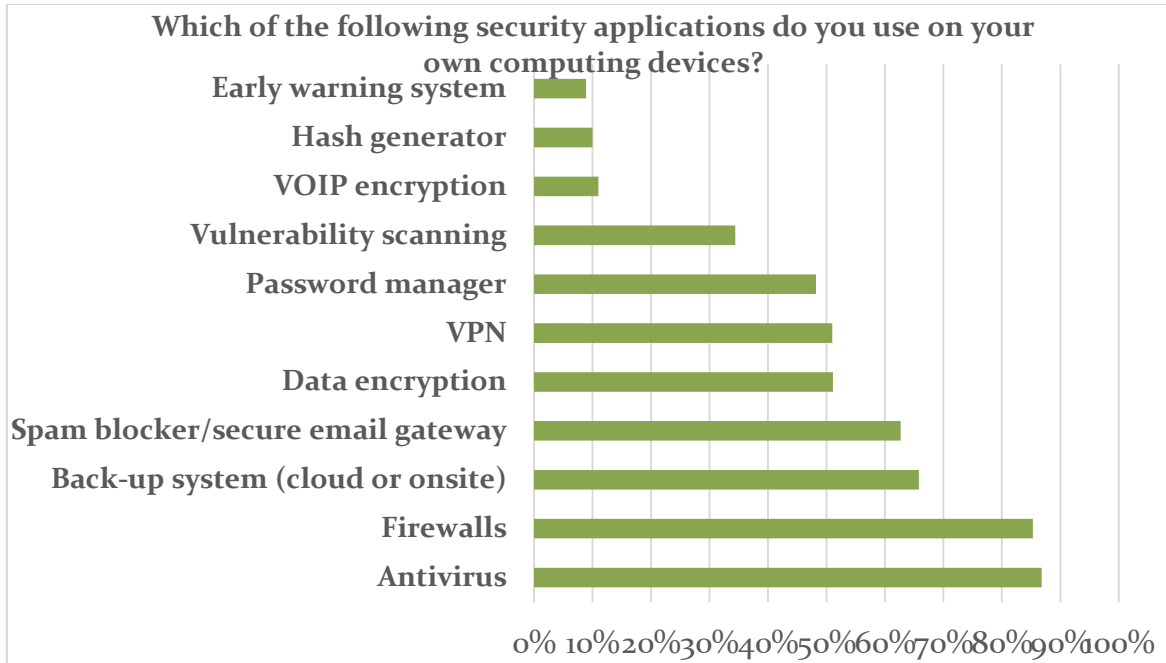


Figure 5: Security applications used by individuals

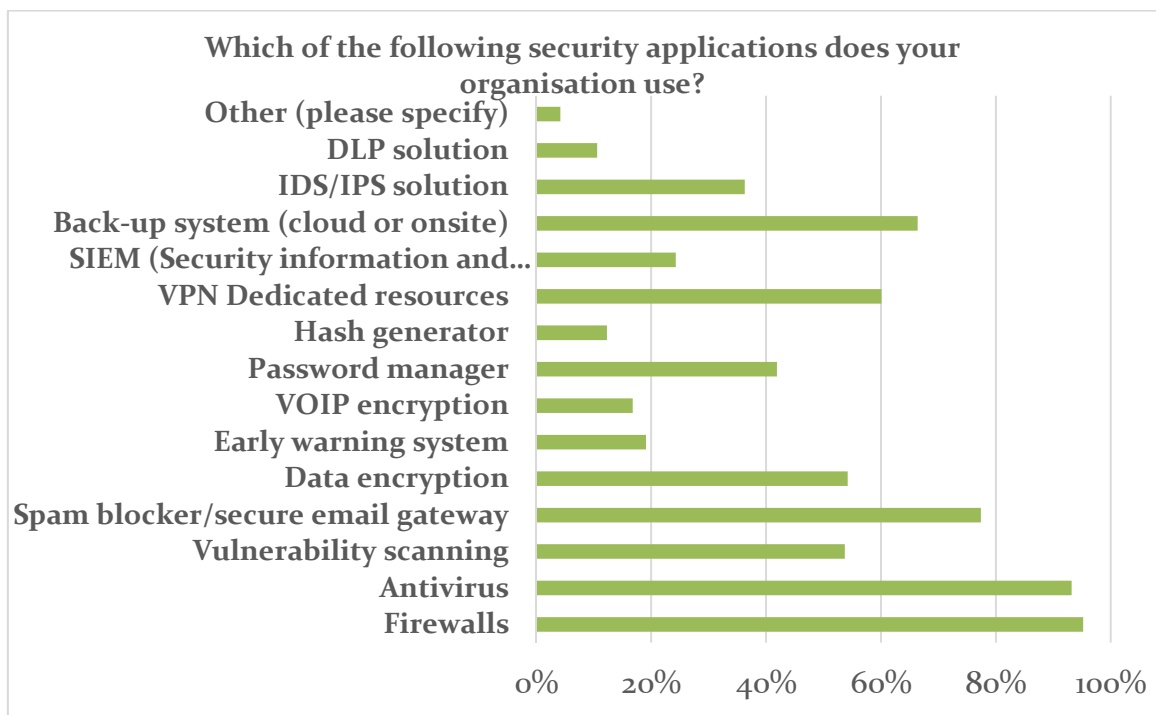


Figure 6: Security applications used by organisations

5.1.3 SOCIAL – MACRO VIEW

Social aspects of cybercrime is explored in detail in **D3.1, Social, Economic, Political and Legal Landscape**. It would be virtually impossible to conduct a survey without some form of social enquiry and results from D5.1 will contribute towards **D3.3 Social, Economic, Political, and Legal research topics** and **D5.6 Cybercrime research topics**. The sample result show in Figure 7 indicates high levels of concern about cybercrime. Refer to surveys in **Annexes A-C**.

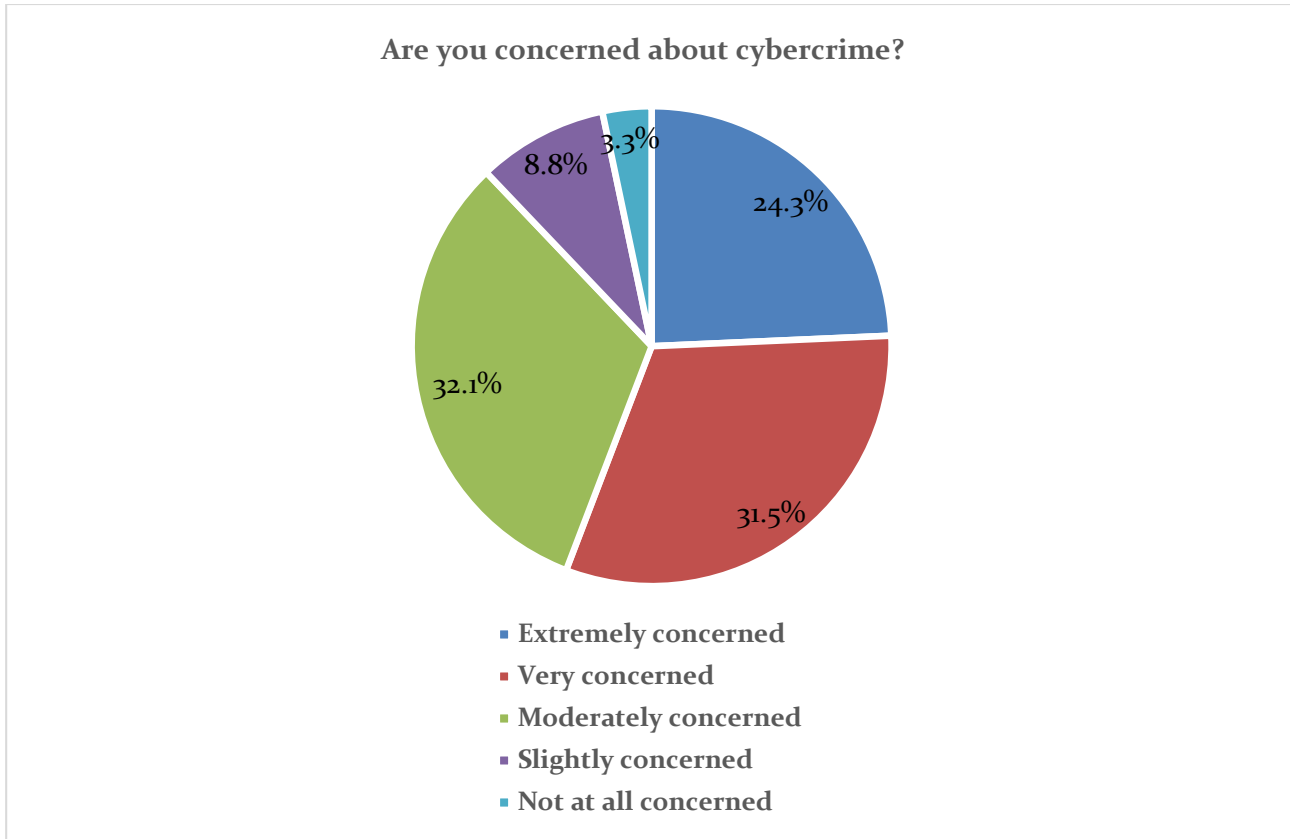


Figure 7: Concerns about cybercrime



5.1.4 LEGAL – MACRO VIEW

Legal aspects of cybercrime is explored in detail in **D3.1, Social, Economic, Political and Legal Landscape**. Results from questions related to legal aspects of cybercrime from D5.1 will contribute towards **D3.3 Social, Economic, Political, and Legal research topics** and **D5.6 Cybercrime research topics**. The sample depicted in Figure 8 indicates low levels of reporting to police. Refer to surveys in **Annexes A-C**.

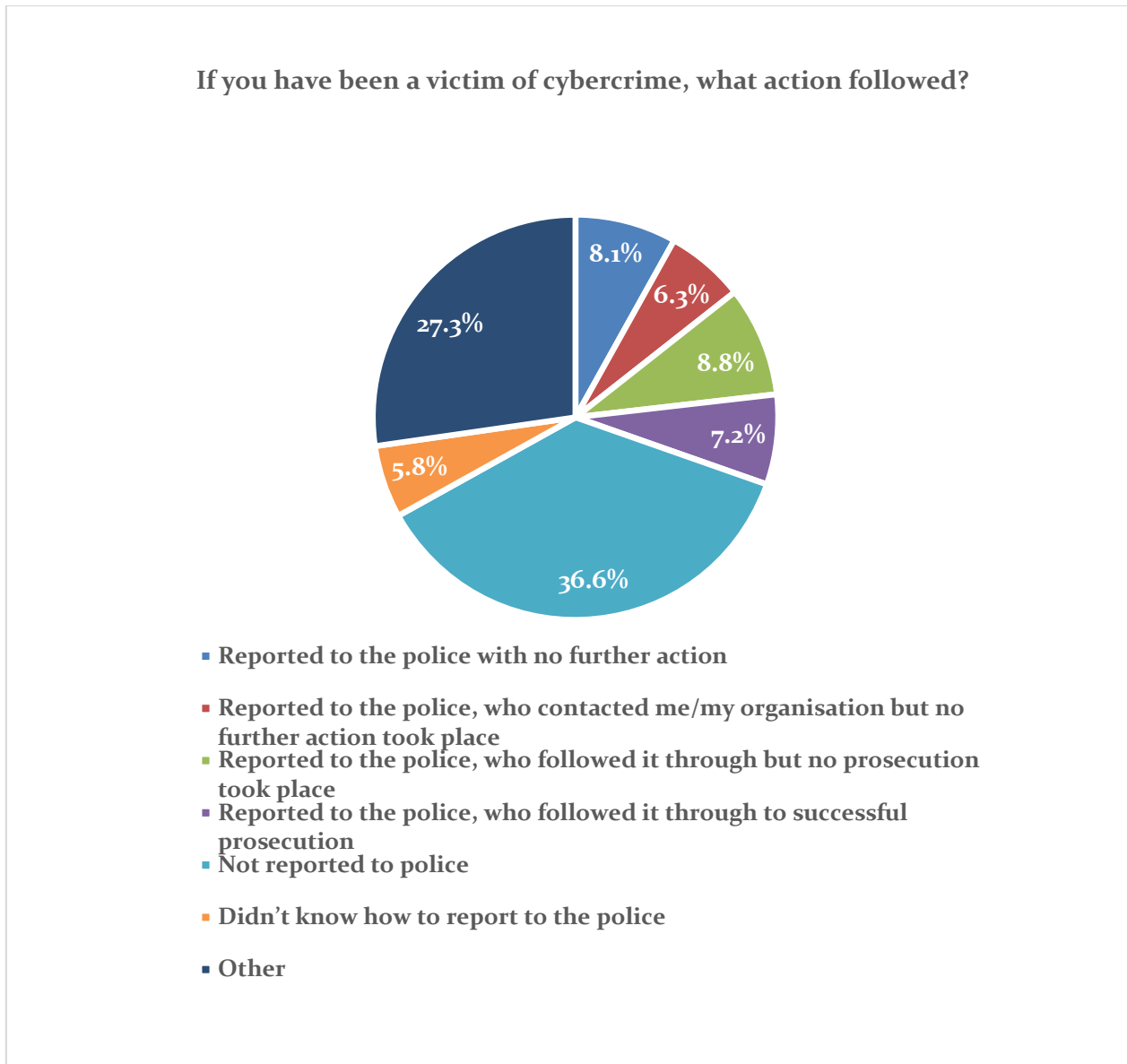


Figure 8: Levels of reporting cybercrime to police

5.1.5 ETHICAL – MACRO VIEW

Ethics in relation to cybercrime can be sometimes be a contentious issue and based on subjective analysis. The sample of the type of question asked on this topic (Figure 9) reveals that better education for users and improved technologies are the preferred options for more research. Results from Ethical questions will contribute towards **D5.6 Cybercrime research topics**. Refer to surveys in **Annexes A-C**.

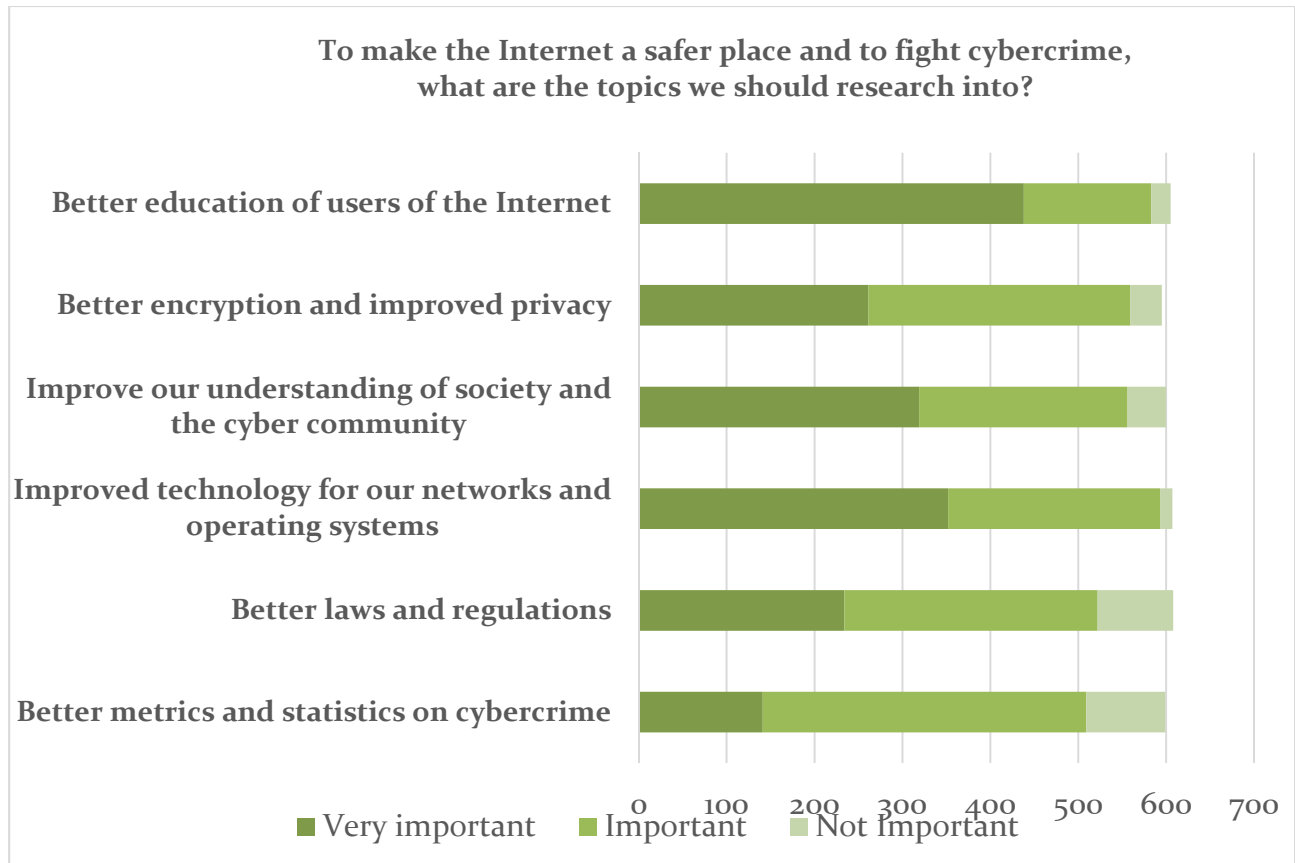


Figure 9: What should be topics for research? (Respondent count 609)



5.1.6 POLITICAL – MACRO VIEW

Political aspects of cybercrime is explored in detail in **D3.1, Social, Economic, Political and Legal Landscape**. Results from questions in Surveys #1, #2 and #3 that relate to legal aspects of cybercrime from D5.1 will contribute towards **D3.3** and **D5.6 Cybercrime research topics**. Refer to surveys in **Annexes A-C**. Figure 10 shows that most respondents see cybercrime as being rooted in economic interests.

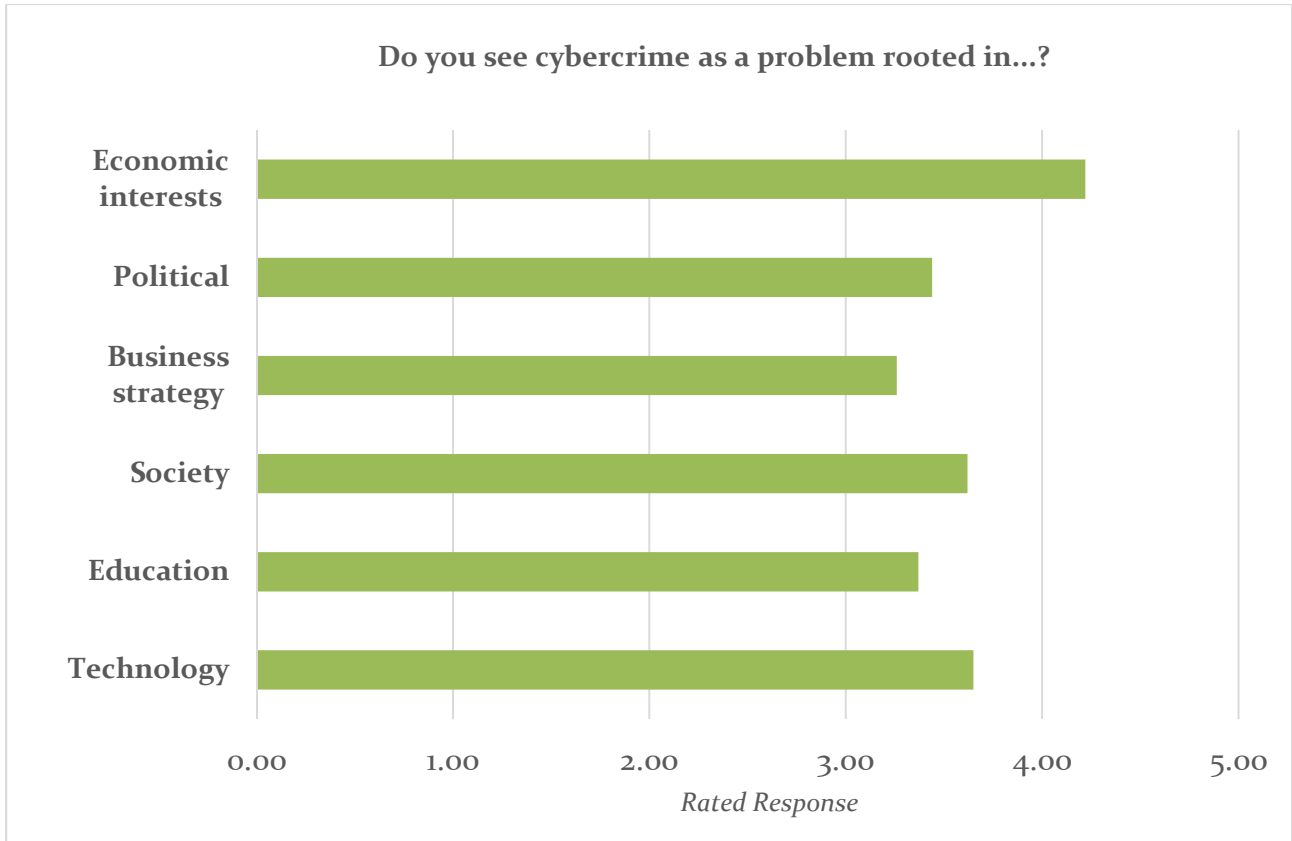
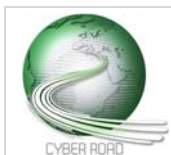


Figure 10: Respondent choices on the root causes of cybercrime



5.1.7 ECONOMIC – MACRO VIEW

Some economic aspects of cybercrime is explored in **D3.1, Social, Economic, Political and Legal Landscape**. Results from questions related to legal aspects of cybercrime from D5.1 will contribute towards **D3.3** and **D5.6 Cybercrime research topics**. Figure 11 shows the amount spent by individuals on preventing cybercrime. Refer to surveys in **Annexes A-C**.

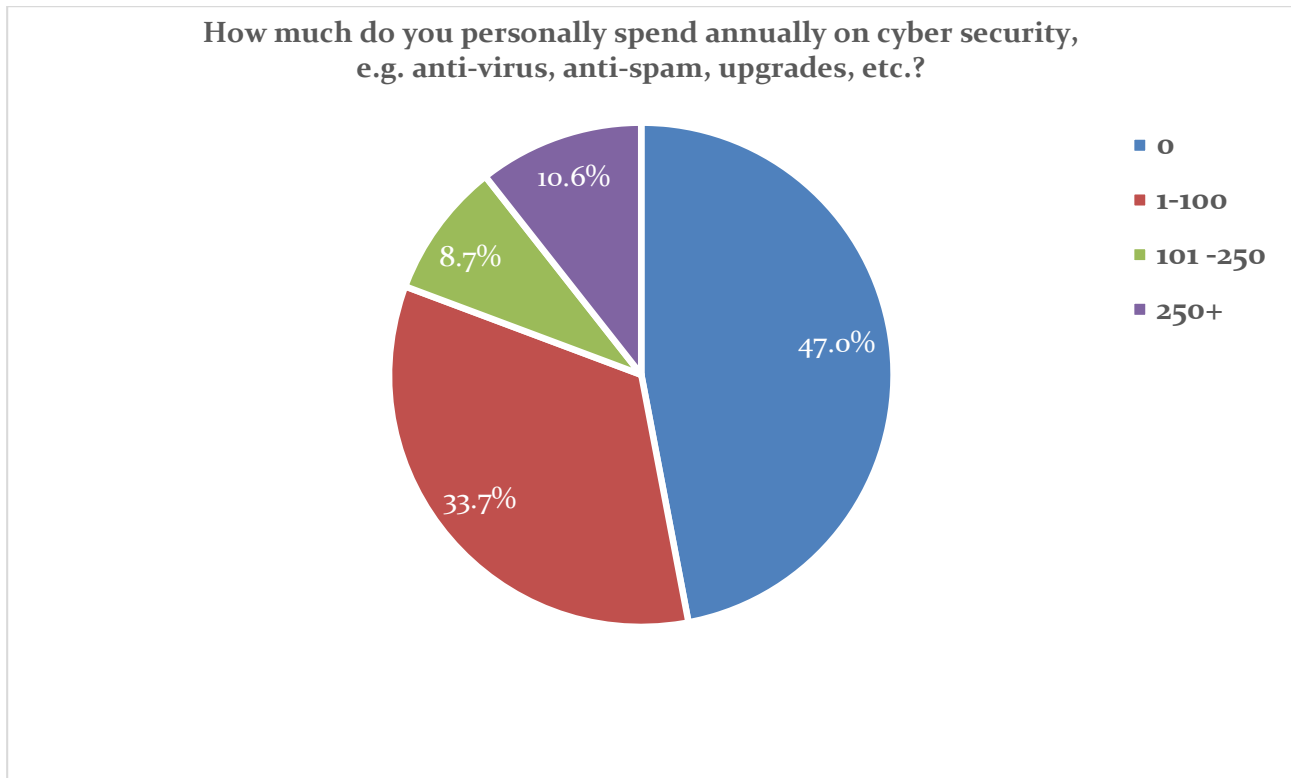


Figure 11: Individual spend on cybercrime prevention (USD)

5.2 AN EARLY ANALYSIS FROM A MICRO PERSPECTIVE (POLAND)

The initial results of the first survey are summarized below with an attempt to highlight the main differences between Polish and English speaking respondents:

- There is still a lot of confusion regarding definitions of cybercrime: most respondents understand cybercrime as being "Criminal activity carried out by means of computers or the Internet" or "Any act against the confidentiality, integrity and availability of computer data and systems".
- Polish respondents stated that cybercrime was a lesser concern for their organization compared to the English language respondents (39.2% of the respondents said that cybercrime was only a slight concern or none at all vs 16% of the English survey). This is despite the 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 vs 63.2% for the English survey. (Note: We included 'Don't know' as a de facto no training answer here as well).



- A higher percentage of Polish respondents had experienced cybercrime action in the last 5 years in a personal capacity (43% vs 26.7% English language survey respondents).
- A low impact of cybercrime for Polish respondents as victims: “inconvenience” or “no effect” gathered 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%).
- 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 vs 80.3% English survey responses).
- A low tendency to share information on attacks with other organizations - lower than that of respondents of the English language survey. (21.1% vs 35.4%).
- Education was pointed out as the main area for improvement (74.6% of English survey respondents - 72.3% stated it was a "very important" element to improve)

5.2.1 THE EUROBAROMETER SURVEY ON CYBER SECURITY

The Eurobarometer survey (conducted Oct 2014) on Cyber Security for the European Commission (Eurobarometer TNS Opinion & Social, 2014) gives insights into perceptions and experiences of EU citizen with cybercrime. It is also 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 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:

- Poles declared one of the highest concerns of online fraud (defined as “goods purchased were not delivered, counterfeit or not as advertised”).
- 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.



- Online banking fraud, was slightly less personally experienced by Polish respondents compared to the EU average, as well as slightly less an area of concern Cyberextortion (through ransomware) was deemed as slightly more concerning for Polish respondents than the EU average, but their experience with this form of cybercrime was equal to the EU average.
- Malicious software was deemed as slightly more concerning for Polish respondents but less experienced in practice than the EU average.

The authors of the survey make 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."* 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 (PwC, 2014) noted a drop in cybercrime as a problem for survey respondents -> 24% (2011) to 19% (2014). This is below worldwide average (24%), and also contrary to CERT Polska reports and statistics.

5.2.2 BSA REPORT ON LEGISLATION

A recent "EU Cybersecurity Dashboard" (BSA, 2015) study by the BSA released in March 2015 provides an overview of the cybersecurity landscape in Europe from the legislation and policy perspective, in particular covering aspects such as: "legal foundations for cybersecurity", "operational capabilities", "public-partner partnerships", "sector-specific cybersecurity plans" and "education". Poland was found to have a "comprehensive cybersecurity strategy with clear goals" but many were viewed as not yet implemented, and the legal cybersecurity framework not fully developed (in the opinion of the creators of the study).

Missing elements, according to the BSA, included:

- 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 cybersecurity audit.
- There is no legislation or policy in place in Poland that requires an annual cybersecurity 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 cybersecurity 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

5.2.3 OVERVIEW FROM A MICRO PERSPECTIVE - POLAND

In terms of the initial conclusions regarding cybercrime in Poland, the following has been observed as part of this study:

- There are sufficient cybercrime penal laws in place, but there appears to be a lack of adequate enforcement. Even if cases are reported, most end up discontinued.



- Reporting rate of cybercrime incidents to authorities appears 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 cybersecurity policies at the national level do not devote sufficient attention to the problem or recognize 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. We have to move beyond just technical observations of the tools used (like malware or malicious pages) and associated measurements and more into cybercrime itself.
- There is no established link between cases reported to the Police, successful prosecution in court and technical measurements/statistics from CERT reports.
- Awareness of cybercrime issues among the general public in Poland appears to be lower than in most other EU countries. Education should thus be viewed as a key component of a future national plan to tackle cybercrime.
- There appears to be a need for more active promotion of CERTs in Poland, in order to increase the rate of reporting of incidents.
- (From section 4 as in the statistical system used by the Police in 2013 it is not obligatory to clearly state if a crime was committed on a computer network or the Internet.)

5.3 *EARLY SURVEY ANALYSIS CONCLUSIONS*

The conclusions from these topics will form the basis for possible research topics for the roadmap gap analysis in D5.6. Of interest is the variation, or similarity, in results when comparing the macro view (world) with the micro view (Poland). Further analysis here is required as is a view from a purely EU perspective.

Some of the topics covered are expected to provide new information in areas that are not frequently covered in surveys. One example is the question concerning levels of training within organization. Another area of interest is the amount of best practices in operation within organisations.

On completion of the analysis an assessment of possible research areas for escalation to D5.6 will be considered. An overview of the recommendations gathered from both the early survey analysis and other body of work within this deliverable is in Section 7: Conclusions and Recommendations.



6.1 CURRENT SCENARIO

At present, the vast majority of governments address cyber security more within the framework of national defense rather than from the point of view of the protection of individual, social, and economic assets. One of the main reasons lies in the lack of clear figures on the real impact of computer incidents that prevents understanding:

- The extension of the threat (i.e., number of computers, individual, enterprises, etc. that have been victims of attacks)
- The total loss that was caused by attacks, both in terms of tangible and intangible assets

In such a scenario, it is quite difficult if not impossible, to take decisions on:

- The policies to set up in terms of education, training, awareness, as well as in terms of software and system verification and certification
- The money to spend to implement the above policies, are today quite limited as the real impact in terms of saving is not well defined.

In fact, laws and regulations need to be grounded on reliable data, that clearly shows how the money spent in prevention and monitoring actually decrease the likelihood of more serious consequences.

It turns out that the current scenario poses a serious threat as the lack of coordinated and focused actions from the legislative and government bodies paves the way for various forms of criminal activities that, if not properly tracked and recorded, does not provide evidence of the existence of a real threat.

6.2 FUTURE SCENARIO

An example of a desirable future scenario is one in which governments can rely on solid methodologies to collect reliable figures about the real impact of cybercrime on companies, individuals and the public sector in order to take decisions, and allocate budget that is proportionate to the real threat.

In this scenario:

- Individuals, companies and the like have a high level of awareness on the possible uses of their data by public and private bodies, thus assigning a value to their data
- The market is mature enough so that a value can be assigned to each piece of information
- It is mandatory to disclose cyber-attacks and data breaches to a central authority, associating the costs incurred in terms of lost assets, lost business, repair/refactoring of software, and of business procedures.
- The above obligation implies that novel techniques are in place that allow assessing the influence of the attack and data breach

On the basis of past data, and of the actual market values, cost estimates are possible. Consequently, it is possible to devise policies that are cost-effective in containing the vulnerability of software and systems, handling security incidents, and preventing their rapid diffusion.



As a scientific discipline, cybercrime is still in its infancy. Value can, therefore, be gained from the evolutionary experiences of other sciences. For example, research without some form of taxonomy would be chaotic in any area.

Accuracy of data is fundamental to other scientific research areas and is dependent upon tried and tested metrics for measurement. In some disciplines unreliable or untrustworthy data could be life threatening. With the advent of the Internet of Things, this could become a critical issue. Measurement is an essential, too, of risk assessment.

The issue of trusted data is emerging as an important topic as a result of this analysis. What trust is and how to quantify this is an element that has significant impact at ground-level involving perceptions as well as real events.

Trust and metrics are interwoven with the field of standards and benchmarks. Standards in industry are a cornerstone to improved safety, reliability and trust. Currently, this is not the case in the cybersecurity industry.

Initially, it would seem that the most importance place for more research would be in additional study of threats but it has emerged that this is only one of several key elements. Study of threats is essential but it is important to know if the money is being spent on the right type of investigation. To know this with any certainty there has to be a greater understanding of the metrics and measurement of all disciplines.

6.3 *STAKEHOLDER CONCERNS*

Survey analysis continues for escalation in D6.4 where potential research gaps will be investigated at a deeper level. An initial and brief evaluation suggests that, overall, stakeholders' needs are not currently being met.

When asked, 'Are you concerned about cybercrime', **88 percent of respondents answered that they were 'Moderately' to 'Extremely' concerned, 9 percent were 'Slightly' concerned while only 3 percent were, 'Not at all concerned'** (no. of respondents 728). An **overwhelming majority (91.5%) were pessimistic** in believing that cybercrime will increase over the next 5 years.

Survey 2 'Technology & Organisation' and Survey 3 'Social, Economic and Political' will explore this topic more fully but, in line with other surveys such as the Eurobarometer (Eurobarometer TNS Opinion & Social, 2014), it is clear that stakeholders' fears, either real or perceived, are on the increase.

As analysis of the surveys will unfold a clearer picture of what are the major concerns of stakeholders. This will provide valuable supporting data for the generation of potential research gap scenarios.



Reliable data is a fundamental on which revenues and budgets rely from the top at government level down to board level and individual stakeholders. To understand a problem, to know what is and how to tackle it, is a task that presents greater challenges when the size and extent of that problem remains very much shrouded in mystery. This body of work is a contribution towards finding the research gaps in the cybercrime domain by observations from the stakeholders' perspective and analysis of the current landscape.

Cybercrime as a subject of study is still in its infancy and much can be learned from the evolutionary development of other recently established sciences. To begin, a clear taxonomy is an essential element from which a framework for further study can be developed. Investigation of current and future scenarios via focused surveys and comparison of measurement related cybercrime reports reveals a number of potential research gaps that will require attention if solutions are to be achieved by 2020. Fundamental to the issue is the ability to quantify what we have and where we want to go. Currently, this study reveals a mis-match between the experiences of stakeholders and the information to hand which can be improved with quantification of the issues and trusted metrics for costing, risk assessments, etc. Central to this information is the issue of trust, as without it there will be no confidence in the way forward with more time and money being spent in the wrong places. Indeed, it is not an exaggeration to say that without quantification and measurement there will be no solution to the problem of cybercrime by 2020 or beyond.

7.1 WHERE ARE THE GAPS – CONCLUSIONS & RECOMMENDATIONS

In **Section 4.6 A Question of Trust**, a number of key areas for further research were identified in relation to the issue of trust. These topics also provide a concise summary of the problem areas as identified throughout this body of work. Some of the problem areas are not unique to a single topic which is representative of the need for cross-over and collaboration between different areas of study. Analysis of the surveys contains and final results will be used for the purposes of D5.6 but from this study the topics for further research are:

- i) Definitions/Taxonomy
- ii) Metrics
- iii) Trusted Data
- iv) Standards/Benchmarks
- v) Threats/cybercrime

Each area is detailed further in the following subsections.

7.1.1 DEFINITIONS & TAXONOMY

i) Definitions of cybercrime vary greatly and there is still a lot of confusion in this area. The question also arises: is having one concise definition relevant?

ii) Without taxonomy/classification science would be chaotic: cybercrime (and the study of) is lacking clearer classification arrangements, naming, describing, groups, etc, for identification and other purposes.



7.1.2 METRICS

- i) There is a mis-match between recorded cybercrime and victimisation. This is true for all crime statistics but evidences suggest that for cybercrime events the gap is greater. How can reporting rates be improved and the profile of CERTS, etc be raised?
- ii) There is a general lack of clear figures on the real impact of computer incidents. This is evidenced in the Polish Police system in 2013 where it was not obligatory to clearly state if a crime was committed on a computer network or the Internet. Is this a localised issue or a global one?
- iii) No measurement, no solution. What is a 'good' way of measuring quantitatively & qualitatively? This is important for; budgets, governments, research, risk assessment, insurance, finance, defence, cyber security industry, and all stakeholders.
- iv) Can established models in other disciplines be used to improve measurement? Can innovative models aid in the balanced gathering of sources of evidence, e.g. evidence-based practices 'the EBP Triad' for quantitative and qualitative assessment?
- v) There is confusion in current costing models over inclusion of intangible entities. A clear classification is lacking.

7.1.3 TRUSTED DATA

- i) A reliable source is a fundamental of trusted metrics. What is a trusted/reliable source?
- ii) There is a mis-match between the value of data from corporate and individual perspectives. Data shared with marketing companies is valued higher than private data not shared; this accounts for a wide range in value, so which should be used, when and where? Should there be government-led regulation or left to the free market? Which valuation is to be trusted?
- iii) Sharing information on cyber attacks with appropriate entities records low levels of practice. What is an appropriate entity and how can this situation be improved? Is this tendency country specific?

7.1.4 STANDARDS AND BENCHMARKS

- i) There is a low rate of best practice policies for BYOD (Bring Your Own Devices) in general (28.3% for English, 34.5% for Polish respondents) whereas the majority of employees are allowed to use their own devices in the workplace (65.6% English, 34.5% Polish). This is a clear mis-match and a potential source for vulnerabilities in the workplace. There are clear differences in workplace practices between English and Polish respondents. There are several themes here for further research.
- ii) There are low levels of relevant certification within the workplace (21.4% English, 22.1% Polish respondents). While there was a high percentage of 'Don't know' answers, definite 'No' answers were also relatively high (33.2% English, 43.1% Polish respondents). More research is needed here, for example, how relevant are current certifications?

7.1.5 THREATS AND CYBERCRIME

- i) An overwhelming majority of investigations into cybercrime are discontinued, many due to the inability to establish the perpetrator. The message is clear; the odds are clearly in favour of the cybercriminal. There are a variety of contributing factors and efforts to find solutions are needed.



ii) Governments tend to address cyber security and acts of cybercrime within the framework of national defence which excludes the context of the protection of the individual, social, and economic assets. The question arises: should these be treated as separate issues?

iii) Security training levels of respondents to Survey #1 are low with most only receiving training if there has already been a problem or once a year (48.3% English, 43.6% Polish). More research on this topic is required.

iv) Education was pointed out as the main area for improvement by survey respondents (74.6% of English, 72.3% of Polish respondents stated it was a "very important" element to improve).

v) A higher percentage of Polish respondents had experienced cybercrime 43% vs 26.7% English language survey respondents. The English results are slightly higher than some other survey results. Further research in this area is required.

vi) Analysis of the Polish macro view found that Poland lacks a comprehensive programme in combating cybercrime. Is this a feature that is unique to Poland?

vii) The evolutionary process of cybercrime indicates that security was not a priority. Without a change towards security-by-design cybercrime will continue and possibly increase. Effective responses for the future (Internet of Things, The Third Platform Innovation Stage (IDC, 2014), etc) are needed to bring about greater integration of critical services.

vii) Policies that are cost-effective in containing the vulnerability of software and systems, handling security incidents, and preventing their rapid diffusion are needed for the future.

7.1.6 MISCELLANEOUS

i) An overview of the current landscape or state-of-the-art is an essential element in all research projects. For a study on cybercrime there are thousands of available papers, articles, books, periodicals, etc. A standard bibliography or central repository for these sources is a useful tool. It is especially useful if the sources are categorized according to the evidence origin. For CyberROAD, a means of categorising the source of evidences (the EBP Triad) was applied to a bibliography and made available to the whole project. The usefulness of this resource will be further explored in D5.6.

ii) Analysis from all survey results is ongoing with a cut-off date still to be determined.





CyberROAD
Development of the Cybercrime and Cyberterrorism research roadmap
Research project funded by the European Commission under the Seventh Framework Programme
Grant agreement n°: **607642** - <http://www.cyberroad-project.eu>

Prof. Fabio ROLI
CyberROAD Project Coordinator
Department of Electrical and Electronics Eng.
University of Cagliari
P.zza D'Armi
09123 Cagliari, Italy

Subject: CyberROAD Deliverable “D5.1 – Stakeholder needs and threats evaluation” Data Sensitivity Report

Dear Prof. Roli,

following the examination of Deliverable “D5.1 – Stakeholder needs and threats evaluation”, in my role of member of the CyberROAD Data Sensitive Committee, I would hereby confirm that no sensitive data or information is contained into the examined deliverable.

Sincerely,
Capt. Antonio Romano

May 27, 2015





CyberROAD
Development of the Cybercrime and Cyberterrorism research roadmap
Research project funded by the European Commission under the Seventh Framework Programme
Grant agreement n°: 607642 - <http://www.cyberroad-project.eu>

Prof. Fabio ROLI
CyberROAD Project Coordinator
Department of Electrical and Electronics Eng.
University of Cagliari
P.zza D'Armi
09123 Cagliari, Italy

Subject: CyberROAD Deliverable “D5.1 – Stakeholder needs and threats evaluation” Data Sensitivity Report

Dear Prof. Roli,

following the examination of Deliverable “D5.1 – Stakeholder needs and threats evaluation”, in my role of member of the CyberROAD Data Sensitive Committee, I would hereby confirm that no sensitive data or information is contained into the examined deliverable.

Sincerely,
David Vara Cuesta

May 27th, 2015



SURVEY #1



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

CyberROAD: Cybercrime - Survey #1

Welcome to the CyberROAD Survey on Cybercrime

Thank you for participating in our survey.

CyberROAD is a research project funded by the European Commission. The project's aim is to identify current and future issues in the fight against cybercrime and cyberterrorism in order to develop a definitive research roadmap.

Cybercrime potentially affects all of us as technology penetrates ever deeper into our everyday lives. Appropriately, we should each be able to contribute to the development of a set of guidelines where the aim is to pinpoint areas of research that may currently be neglected or overlooked. The CyberROAD team would very much like your help in this matter in order that we may gather as much information, on a variety of subjects, as is possible.

We shall be providing an in-depth analysis of all the technological, social, legal, ethical, political, and economic aspects on which cybercrime and cyber-terrorism are rooted. You can contribute to this work through a series of 3 surveys. The initial survey targets basic aspects of your relationship with cybercrime, either personally or through your work.

We hope you will enjoy participating in our project and we look forward to your responses. Please note the survey is anonymous and providing contact data is entirely optional

Data Protection

The CyberROAD project is committed to the protection of personal data. CyberROAD adheres to **Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000** on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data. Further information is available here:

http://europa.eu/legislation_summaries/information_society/data_protection/l24222_en.htm

CyberROAD also adheres to the **Code of Standards and Ethics for Market, Opinion, and Social Research (CASRO)**. Further information is available here: <http://www.casro.org/?page=TheCASROCode2014>

Survey Contact - jart.armin@cyberroad.eu

1. About You & Your Work

i. In which country do you currently reside?

ii. What is your age?

- 18 to 24 35 to 54 65 +
 25 to 34 55 to 64

iii. Where is the main business of your company located

iv. How many employees work for your company?

- 1-5 21-100 501-1000
 6-20 101-500 1000+

v. Which category most closely fits your organisation type?

- Scholarly research Internet service provider or operator
 Policy making, Govt, legal or law enforcement Consumer group or end-user
 Cyber security practitioner, cyber security expert (any field) Commercial business
 Other (please specify)

2. The definition of cybercrime

i. Which of these definitions do you think best matches your view on cybercrime? (Note that individual countries set their own laws on crime and illegal activities in relation to computer offences.)

For me cybercrime is.....

	Less relevant	Average	Most relevant
Criminal activity carried out by means of computers or the Internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any illegal activity that uses a computer for the storage of evidence	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any criminal act or hacking of computers and networks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Theft using a computer or Internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any act against the confidentiality, integrity and availability of computer data and systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The use of a computer system(s) to enable traditional form of criminal activity and the use of a computer system(s) to launch a cyber attack	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None of these	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Cybercrime concerns

i. Are you concerned about cybercrime?

- Extremely concerned Moderately concerned Not at all concerned
- Very concerned Slightly concerned

ii. Is cybercrime a concern for your organisation?

- Extremely concerned Moderately concerned Not at all concerned
- Very concerned Slightly concerned

iii. Over the next 5 years do you think cybercrime will...?

- Increase Decrease Stay at the same level

4. What does cybercrime mean to you?

i. Do you think cybercrime is...?

- Here to stay
- Solvable
- Containable
- Not much of an issue

ii. Do you see cybercrime as a problem rooted in...?

	Not much	Lesser	Average	Higher	Top cause
Technology	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Education	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Society	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Business strategy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Political	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Economic interests	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. The targets of cybercrime

i. In your organisation, which do you think is most likely to be the target for cybercriminals?

- | | |
|--|---|
| <input type="checkbox"/> Critical infrastructures | <input type="checkbox"/> Logistics & supply chain |
| <input type="checkbox"/> Intellectual Property Rights | <input type="checkbox"/> Mobile devices (tablets, smartphones) |
| <input type="checkbox"/> Personal data | <input type="checkbox"/> Critical information |
| <input type="checkbox"/> Cloud infrastructures | <input type="checkbox"/> People (citizens) |
| <input type="checkbox"/> Unmanned systems | <input type="checkbox"/> People (employees) |
| <input type="checkbox"/> On-Line services/Web applications | <input type="checkbox"/> Workstations (Users' equipment) |
| <input type="checkbox"/> Embedded systems | <input type="checkbox"/> Communications with satellites, weather stations, etc. |
| <input type="checkbox"/> Payment systems | <input type="checkbox"/> Transport assets (airplanes, railways, ferries) |
| <input type="checkbox"/> Banking & financial service | <input type="checkbox"/> Business or personal reputations |

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

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

- Weekly Yearly Only if there is a problem
 Monthly Never 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 Not reported to police
 Reported to the police, who contacted me/my organisation but no further action took place Didn't know how to report to the police
 Reported to the police, who followed it through but no prosecution took place Other
 Reported to the police, who followed it through to successful prosecution

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?

- | | | |
|--|---|---|
| <input type="checkbox"/> Firewalls | <input type="checkbox"/> Data encryption | <input type="checkbox"/> Hash generator |
| <input type="checkbox"/> Antivirus | <input type="checkbox"/> Early warning system | <input type="checkbox"/> Back-up system (cloud or onsite) |
| <input type="checkbox"/> Vulnerability scanning | <input type="checkbox"/> VOIP encryption | |
| <input type="checkbox"/> Spam blocker/secure email gateway | <input type="checkbox"/> Password manager | |

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

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

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

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

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

- | | | |
|---------------------------|--------------------------|----------------------------------|
| <input type="radio"/> Yes | <input type="radio"/> No | <input type="radio"/> Don't know |
|---------------------------|--------------------------|----------------------------------|

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

- | | | |
|---------------------------|--------------------------|----------------------------------|
| <input type="radio"/> Yes | <input type="radio"/> No | <input type="radio"/> Don't know |
|---------------------------|--------------------------|----------------------------------|

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

- | | | |
|---|------------------------------|----------------------------------|
| <input type="radio"/> Penetration testing | <input type="radio"/> Audits | <input type="radio"/> Don't know |
| <input type="radio"/> Vulnerability testing | <input type="radio"/> Other | |

9. Economic impact

Pick a major currency for these economic questions

i. How much do you personally spend annually on cyber security, e.g. anti-virus, anti-spam, upgrades, etc.?

- 0 101 -250
 1-100 250+

ii. How much does your organisation spend annually on cyber security products?

- 0 101 -500 1,000 - 10,000
 1-100 501 - 1,000 10,000+

iii. What do you think is the cost of cybercrime to the economy of your country of residence per annum?

- Up to 25 million 100 million+
 26m - 100m No idea

iv. What do you think is the cost of cybercrime to the world economy?

- Less than 1billion 11bn - 25bn Over 100 billion
 1bn - 10bn 26bn - 100bn No idea

10. Research into cybercrime

To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?

	Not Important	Important	Very important
Better metrics and statistics on cybercrime	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Better laws and regulations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Improved technology for our networks and operating systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Improve our understanding of society and the cyber community	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Better encryption and improved privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Better education of users of the Internet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Other (please specify)

11. Next steps

Are you willing to participate in another and more advanced survey, to help develop the definitive research roadmap on cybercrime?

Yes

No

The following information is optional. If you're happy to give us your contact information we will inform you of the overall survey results, and when Questionnaire 2 (out of 3) is ready for your input. Your personal details will not be used for any other purpose. Thank you for participating.

Name

Company

Email Address

Dziękujemy za udział w naszej ankiecie

CyberROAD jest projektem badawczym finansowanym przez Komisję Europejską, którego celem jest określenie obecnych i przyszłych problemów w walce z cyberprzestępczością i cyberterroryzmem oraz wypracowanie planu badań nad tymi zagadnieniami.

Cyberprzestępczość potencjalnie będzie wpływać na nas wszystkich wraz z postępującym przenikaniem nowych technologii w każdy aspekt naszego życia codziennego. Właściwie każdy z nas powinien móc przyczynić się do opracowania szeregu wytycznych, których celem byłoby wskazania obszarów badań nad tym zagadnieniem, które obecnie mogą być zaniedbywane lub wręcz pomijane. Zespół CyberROAD byłby bardzo wdzięczny za Waszą pomoc w tej kwestii, tak abyśmy mogli zebrać jak najwięcej informacji z uwzględnieniem wielu punktów widzenia.

Naszym celem jest przeprowadzenie szczegółowej analizy wszystkich aspektów technologicznych, społecznych, prawnych, etycznych, politycznych i ekonomicznych, które wpływają na rozwój cyberprzestępczości i cyberterroryzmu. Możesz przyczynić się do tej pracy poprzez uczestnictwo w serii trzech badań. To pierwsze, wstępne, badanie dotyczy podstawowych doświadczeń ankietowych z cyberprzestępczością, czy to w życiu prywatnym czy też zawodowym.

Mamy nadzieję, że będziecie zadowoleni z uczestnictwa w naszym projekcie - czekamy na Wasze odpowiedzi!

Uwaga: udział w ankiecie jest anonimowy, a podanie danych kontaktowych opcjonalne.

Ochrona danych osobowych

Projekt CyberROAD zobowiązuje się do ochrony danych osobowych. CyberROAD stosuje się do rozporządzenia (WE) nr **45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000** w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i ciała Wspólnoty, oraz swobodnego przepływu tych danych. Więcej informacji dostępnych jest

tutaj: http://europa.eu/legislation_summaries/information_society/data_protection/l24222_en.htm

CyberROAD stosuje się również do Kodeksu Etyki i Standardów Rynku, Opinii i Badań Społecznych **Code of Standards and Ethics for Market, Opinion, and Social Research (CASRO)**. Further information is available here: <http://www.casro.org/?page=TheCASROCode2014>

- Poprzez przekazanie CyberRoad swoich danych osobowych Użytkownik wyraża zgodę na przetwarzanie przez CyberROAD danych osobowych Użytkownika w związku z jego udziałem w ankiecie.
- Administratorem danych osobowych jest CyberDefcon Ltd, The Old Casino, 28 Fourth Avenue, Hove, E Sussex, BN3 2PJ, UK
- Podanie przez Użytkownika danych osobowych jest dobrowolne.
- Po zakończeniu ankiety CyberRoad nie będzie uprawniony do przetwarzania danych osobowych Użytkownika.
- Zgoda na przetwarzanie danych osobowych może być w każdym czasie przez Użytkownika odwołana.
- Użytkownik ma w każdym czasie prawo wglądu w swoje dane osobowe przekazane CyberRoad, poprawiania ich i żądania ich usunięcia poprzez wysłanie oświadczenia drogą elektroniczną do admin@cyberdefcon.com

Więcej informacji lub pytania: info@cert.pl

1. O Tobie i Twojej pracy

i. W jakim kraju obecnie mieszkasz?

ii. Ile masz lat?

- od 18 do 24 od 35 do 54 od 65 +
- od 25 do 34 od 55 do 64

iii. Gdzie mieści się główna siedziba Twojej firmy?

iv. Ile osób pracuje w Twojej firmie?

- 1-5 21-100 501-1000
- 6-20 101-500 1000+

v. Która kategoria najlepiej opisuje Twoją organizację?

- uczelnia, instytut badawczy grupa konsumencka, użytkownik końcowy, osoba prywatna
- administracja rządowa, organy legislacyjne, prawnicze instytucja komercyjna
- praktyk lub ekspert bezpieczeństwa komputerowego inne (proszę uszczegółwić)
- dostawca Internetu, operator sieci

2. Definicja cyberprzestępczości

i. Która z poniższych definicji najlepiej pasuje do Twojego rozumienia cyberprzestępczości? (Uwaga: poszczególne Państwa mogą inaczej ustanawiać prawo w zakresie przestępczości i nielegalnych działań związanych z użyciem komputera lub sieci)

Dla mnie cyberprzestępczość to

	Mniej istotne	Średnie	Najbardziej istotne
Działalność przestępczą wykonywaną za pośrednictwem komputera/Internetu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Każda nielegalna działalność której ślady mogą pozostać na komputerze	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Każda działalność przestępcza związany z włamywaniem się do komputera i sieci	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kradzież z użyciem komputera/Internetu	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Każda działalność przeciwko poufności, integralności, dostępności danych komputerowych i systemów/sieci	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Użycie komputera/systemów komputerowych do tradycyjnych form przestępczości i użycie komputerów do przeprowadz	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Żadne z powyższych	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Zagadnienia związane z cyberprzestępczością

i. Jak bardzo przejmujesz się cyberprzestępczością?

- Bardzo mocno Średnio W ogóle się nie przejmuję
- Mocno Tylko trochę

ii. Czy cyberprzestępczość jest problemem dla Twojej organizacji?

- Bardzo dużym problemem Średnim problemem W ogóle nie jest problemem
- Dużym problemem Niewielkim problemem

iii. Czy uważasz, że przez najbliższe 5 lat cyberprzestępczość ...

- Zwiększy się Zmniejszy się Pozostanie na tym samym poziomie

4. Czym dla Ciebie jest cyberprzestępczość?

i. Czy uważasz, że cyberprzestępczość ...?

- jest zjawiskiem, które zawsze będzie obecne
- jest problemem, który można ograniczyć
- jest problemem, który zostanie rozwiązany
- nie jest żadnym problemem

ii. Czy uważasz, że cyberprzestępczość to problem, którego źródła/przyczyna tkwią w ...?

	Nie bardzo	W mniejszym stopniu	W średnim stopniu	W większym stopniu	Wiodąca przyczyna
technologii	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
edukacji	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
społeczeństwie	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
strategii biznesowej	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
polityce	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
interesach ekonomicznych	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. Cele cyberprzestępczości

i. Które elementy w Twojej organizacji uważasz za najbardziej prawdopodobny cel dla cyberprzestępców?

- | | |
|--|---|
| <input type="checkbox"/> krytyczna infrastruktura | <input type="checkbox"/> logistyka i łańcuch dostaw |
| <input type="checkbox"/> prawa własności intelektualnej | <input type="checkbox"/> urządzenia mobilne (tablety, smartfony) |
| <input type="checkbox"/> dane osobowe | <input type="checkbox"/> krytyczne informacje |
| <input type="checkbox"/> infrastrukturę w chmurze | <input type="checkbox"/> ludzie (obywatele) |
| <input type="checkbox"/> systemy bezzałogowe | <input type="checkbox"/> ludzie (pracownicy) |
| <input type="checkbox"/> usługi on-line/aplikacje webowe | <input type="checkbox"/> stacje robocze (sprzęt pracowników) |
| <input type="checkbox"/> systemy osadzone | <input type="checkbox"/> komunikacja z satelitami, stacjami pogodowymi itp. |
| <input type="checkbox"/> systemy płatności | <input type="checkbox"/> zasoby transportowe (samoloty, koleje, promy) |
| <input type="checkbox"/> systemy bankowe i finansowe | <input type="checkbox"/> reputacja biznesu lub poszczególnych osób |

6. Na jakie ryzyka jesteś narażony?

i. Czy Twoja organizacja (lub Ty sam) stosuje zarządzanie ryzykiem jako część strategii cyberbezpieczeństwa?

- tak nie nie wiem

ii. Czy ktoś w Twojej organizacji (lub Ty sam) formalnie i regularnie zapoznaje się z wiadomościami o cyberbezpieczeństwie za pośrednictwem...?

- ogólnotematycznych gazet i serwisów informacyjnych firm konsultingowych sieci społecznościowych
 specjalistycznych źródeł wiadomości czynności prowadzonych przez zewnętrzne firmy w ramach outsourcingu nie alokuję na to czasu

iii. Jak często personel jest szkolony w zakresie ryzyk związanych z cyberbezpieczeństwem?

- co tydzień co rok tylko wtedy, gdy wystąpi problem
 co miesiąc nigdy nie wiem

iv. Czy w Twojej organizacji pozwala się na korzystanie z własnych urządzeń (BYOD)?

- tak nie

v. Czy w Twojej organizacji opublikowano dobre praktyki w zakresie stosowania własnych urządzeń?

- tak nie nie wiem

7. Skutki cyberprzestępczości

i. Czy doświadczyłeś/doświadczyłaś działań cyberprzestępczych w ciągu ostatnich 5 lat...?

- w życiu osobistym w pracy nigdy

ii. Jeśli byłeś/byłaś ofiarą cyberprzestępczości w ciągu ostatnich 5 lat, jaki był skutek tych zdarzeń?

- strata pieniędzy niedogodność utrata dobrego imienia
 wstrzymanie pracy obciążenie psychiczne zaden

iii. Czy w wyniku ataku lub zagrożenia cybernetycznego wprowadzono w Twojej firmie zmiany do strategii cyberbezpieczeństwa?

- tak nie wiem
 nie nie dotyczy

iv. Jeśli doświadczyłeś/doświadczyłaś cyberataku, czy uważasz, że stanowił on ryzyko systemowe dla Twojej organizacji?

- tak nie nie wiem

v. Jeżeli byłeś/byłaś ofiarą cyberprzestępstwa, co zrobiono w tej sprawie?

- zgłoszono sprawę na policję, ale nic się później nie wydarzyło nie zgłoszono sprawy na policję
 zgłoszono sprawę na policję, która skontaktowała się z moją organizacją, ale nic się później nie wydarzyło nie wiedziałem/wiedziałam jak zgłosić sprawę na policję
 zgłoszono sprawę na policję, która poprowadziła ją, ale nie doprowadzono do ukarania sprawców inne
 zgłoszono sprawę na policję, która poprowadziła ją aż do ukarania sprawców

vi. Jeżeli byłeś/byłaś ofiarą cyberbezpieczeństwa, czy skontaktowałeś/skontaktowałaś się z narodowym lub rządowym zespołem CERT?

- zgłoszono sprawę do rządowego lub narodowego zespołu CERT, ale nic się później nie wydarzyło
 zgłoszono sprawę do rządowego lub narodowego zespołu CERT, który podjął działania
 nie zgłoszono sprawy do CERT, ale wiem, że policja kontaktowała się z takim zespołem
 Dnie zgłoszono sprawy do CERT ponieważ uznano to za nieodpowiednie miejsce
 nie wiedziałem/wiedziałam że mogę zgłosić sprawę do CERT
 nie wiem, czym jest CERT i jak się z nim skontaktować

8. Zarządzanie bezpieczeństwem

i. Których z poniższych rozwiązań używasz na swoich urządzeniach?

- | | | |
|---|--|---|
| <input type="checkbox"/> firewalle | <input type="checkbox"/> szyfrowanie danych | <input type="checkbox"/> generator hashy |
| <input type="checkbox"/> antywirusy | <input type="checkbox"/> systemy wczesnego ostrzegania | <input type="checkbox"/> system kopi zapasowej (w chmurze lub lokalnie) |
| <input type="checkbox"/> skanery podatności | <input type="checkbox"/> szyfrowanie VOIP | |
| <input type="checkbox"/> blokady i filtry spamu | <input type="checkbox"/> menadżer haseł | |

ii. Które z poniższych rozwiązań używa Twoja organizacja na swoich urządzeniach?

- | | | |
|---|--|---|
| <input type="checkbox"/> firewalle | <input type="checkbox"/> systemy wczesnego ostrzegania | <input type="checkbox"/> SIEM (Security information and event management) |
| <input type="checkbox"/> antywirusy | <input type="checkbox"/> szyfrowanie VOIP | <input type="checkbox"/> system kopi zapasowej (w chmurze lub lokalnie) |
| <input type="checkbox"/> skanery podatności | <input type="checkbox"/> menadżer haseł | <input type="checkbox"/> systemy IDS/IPS (wykrywanie intruzów) |
| <input type="checkbox"/> blokady i filtry spamu | <input type="checkbox"/> generator hashy | <input type="checkbox"/> systemy DLP (ochrona przed wyciekami danych) |
| <input type="checkbox"/> szyfrowanie danych | <input type="checkbox"/> dedykowane zasoby VPN | |
| <input type="checkbox"/> inne – jakie? | | |

iii. Jak zarządza się cyberbezpieczeństwem w Twojej organizacji?

- | | |
|--|---|
| <input type="radio"/> wewnątrz, przez osoby odpowiedzialne za polityki (bezpieczeństwa), na przykład administratora systemów | <input type="radio"/> przez outsourcing do niezależnego specjalisty lub firmy |
| <input type="radio"/> własny CERT | <input type="radio"/> przez dostawcę Internetu (ISP) |
| <input type="radio"/> sam/sama zarządzam cyberbezpieczeństwem | <input type="radio"/> nie wiem |

iv. Czy Ty, lub ktoś inny w firmie, dzieli się informacjami o zdarzeniach i cyberatakach z organizacją zewnętrzną?

- | | | |
|---------------------------|---------------------------|--------------------------------|
| <input type="radio"/> tak | <input type="radio"/> nie | <input type="radio"/> nie wiem |
|---------------------------|---------------------------|--------------------------------|

v. Czy Ty lub Twoja organizacja posiada certyfikaty z zarządzania bezpieczeństwem informacji, np. ISO 27001?

- | | | |
|---------------------------|---------------------------|--------------------------------|
| <input type="radio"/> tak | <input type="radio"/> nie | <input type="radio"/> nie wiem |
|---------------------------|---------------------------|--------------------------------|

vi. Czy Ty lub Twoja organizacja korzysta z następujących metod testów?

- | | | |
|--|------------------------------|--------------------------------|
| <input type="radio"/> testy penetracyjne | <input type="radio"/> audyty | <input type="radio"/> nie wiem |
| <input type="radio"/> testy podatności | <input type="radio"/> inne | |

9. Wpływ ekonomiczny

Wybierz walutę, w której wyrażone będą kwoty w poniższych pytaniach

i. Ile osobiście wydajesz na rozwiązania z zakresu cyberbezpieczeństwa (np. antywirus, antyspam, aktualizacje) w skali roku?

- 0 1-100 101 -250 250+

ii. Ile Twoja organizacja na rozwiązania z zakresu cyberbezpieczeństwa w skali roku?

- 0 1-100 101 -500 501 - 1,000 1,000 - 10,000 10,000+

iii. Jak oceniasz koszt cyberprzestępczości dla ekonomii Twojego kraju w skali roku?

- do 25 milionów 26 mln – 100 mln ponad 100 mln nie mam pojęcia

iv. Jak oceniasz koszt cyberprzestępczości dla światowej ekonomii?

- poniżej 1 miliarda 1 mld – 10 mld 11 mld – 25 mld 26 mld – 100 mld ponad 100 mld nie mam pojęcia

10. Badania nad cyberprzestępczością

Które tematy powinny być rozwijane badawczo aby Internet stał się bezpieczniejszym miejscem?

	Nieważne	Ważne	Bardzo ważne
lepsze metryki i statystyki dotyczące cyberprzestępczości	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lepsze regulacje i przepisy prawa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lepsze technologie w sieciach i systemach operacyjnych	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
poprawa naszego rozumienia społeczeństwa i cyberspoleczności	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lepsze mechanizmy szyfrowania i poprawa prywatności	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lepsza edukacja użytkowników Internetu	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

inne – jakie?

11. Kolejne kroki

Czy chciałbyś/chciałabyś wziąć udział w kolejnej, bardziej zaawansowanej ankiecie, aby pomóc w stworzeniu mapy drogowej badań nad cyberprzestępczością?

tak

nie

Poniższe informacje są opcjonalne. Jeśli zechcesz przekazać nam swoje dane kontaktowe, prześlemy Ci wyniki zbiorcze tego badania ankietowego oraz poinformujemy gdy Kwestionariusz 2 (z 3) będzie gotowy do wypełnienia przez Ciebie. Twoje dane osobowe nie będą wykorzystywane w żadnym innym celu. Bardzo dziękujemy za udział w badaniu.

Imię

Nazwisko

Adres email

SURVEY #2



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme



CyberROAD: Cybercrime - Survey #2 - Technology & Organisation

Welcome to the CyberROAD Survey on Cybercrime

Thank you for participating in the CyberROAD Cybercrime Survey #2.

This questionnaire is a follow-on from Survey #1 where participants provided responses to questions exploring an individual's relationship to aspects of cybercrime. Survey #2 probes further into two specific areas: technology and organisations.

Additionally, a third questionnaire, Survey #3, concentrates on social, economic and political issues.

Each survey in this round is independent of the others so you may choose to complete Survey #2 only, or Survey #3 only, but please try to find the time to make your contribution to our project even more valuable by completing both. Survey #2 should take about 10-15 minutes to complete.

We hope you will enjoy participating in our project and we look forward to your responses. Please note the survey is anonymous and providing personal data is entirely optional.

CyberROAD is a research project funded by the European Commission. The project's aim is to identify current and future issues in the fight against cybercrime and cyberterrorism in order to develop a definitive research roadmap.

Data Protection

The CyberROAD project is committed to the protection of personal data. CyberROAD adheres to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data. Further information is available here: http://europa.eu/legislation_summaries/information_society/data_protection/l24222_en.htm

CyberROAD also adheres to the Code of Standards and Ethics for Market, Opinion, and Social Research (CASRO). Further information is available here: <http://www.casro.org/?page=TheCASROCode2014>

Survey Contact - jart.armin@cyberroad.eu



CyberROAD: Cybercrime - Survey #2 - Technology & Organisation

1. About You & Your Work

i. In which country do you currently reside?

ii. Which category most closely fits your organization type?

- | | |
|--|---|
| <input type="radio"/> Scholarly research | <input type="radio"/> Internet service provider or operator |
| <input type="radio"/> Policy making, Govt, legal or law enforcement | <input type="radio"/> Consumer group or end-user |
| <input type="radio"/> Cyber security practitioner, cyber security expert (any field) | <input type="radio"/> Commercial business |



CyberROAD: Cybercrime - Survey #2 - Technology & Organisation

2. Cybercrime definitions and classifications

i. Which of these definitions do you think best matches your view on cybercrime?

Survey 1 respondents were asked, "For me cybercrime is...?". The 3 most popular answers are below. Please indicate your choice of definition.

	Less relevant	Average	Most relevant
Criminal activity carried out by means of computers or the Internet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any criminal act or hacking of computers and networks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Any act against the confidentiality, integrity and availability of computer data and systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify)

ii. Which of these do you think of as cyber criminal actions?

	Cybercrime	Maybe cybercrime	Not cybercrime	Not sure
Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Copyright infringement (e.g. movies, music...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DoS (denial of service) - critical safety operations (transport, utilities, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DoS (denial of service) - non-critical operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interception of private communications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit goods online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online fake pharmacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online Child Sexual Abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Black hat SEO	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hacking into servers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cybersex	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cybersquatting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Website defacement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber bullying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bullet proof hosting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tracking of web activity without permission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Writing malware or exploits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using malware or exploits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Distributing malware or exploits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Serving as a moneymule	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify)



3. The targets of cybercrime

i. Most respondents indicated "personal data" as the most likely target for cybercriminals in their organisation. Is personal data managed in your organization in any of the following ways?

- All devices (desktop and portables) are company property and IT has access to everything, even personal data
- Secure workspace technology (IT has control over secure areas but no access to personal data)
- Content management via app distribution and inventory on all devices (company and BYO)
- Personal data is not restricted on either company devices or BYOD
- Using company devices for personal data and content is not permitted
- Other (please specify)

ii. Are you satisfied with the current privacy policies on controlling the use of the personal data on most websites and social networks?

- Yes
- No
- Further comments



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 knowledge to prepare the documents
 Insufficient resources 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 Lack of knowledge in the subject
 Only specific staff i.e., those in a technical environment, need regular training Lack of time/human resources
 Perceived low effectiveness of training Cost too high
 Lack of awareness in executive management



5. Cyber Security Management

i. Do you feel you share responsibility for cyber security of your company or organisation?

- Yes, I feel I share responsibility I feel I only share a small responsibility No, it is not my responsibility

ii. Who in your opinion should take responsibility for cyber security on the Internet (pick 3)

- | | |
|--|---|
| <input type="checkbox"/> Internet service and content providers (ISPs & hosts) | <input type="checkbox"/> The end user |
| <input type="checkbox"/> Law enforcement | <input type="checkbox"/> Your government |
| <input type="checkbox"/> IT and security departments in companies | <input type="checkbox"/> Search engine operators (Google, MSN, Yahoo... etc.) |
| <input type="checkbox"/> CERTs | <input type="checkbox"/> Intergovernmental and international organisations (UN, ICANN, ITU... etc.) |
| <input type="checkbox"/> Other (please specify) | |

iii. There are many forms of cyber security training and certifications available. Pick the 3 you would choose as most important.

- | | |
|---|--|
| <input type="checkbox"/> Information Security (general) | <input type="checkbox"/> Cyber Threat intelligence |
| <input type="checkbox"/> Cyber security for IT Administrators | <input type="checkbox"/> CISSP (Certified Information Systems Security Professional) |
| <input type="checkbox"/> Mitigation Strategies | <input type="checkbox"/> Cyber security audits |
| <input type="checkbox"/> Incident prevention | <input type="checkbox"/> Data security law |
| <input type="checkbox"/> Secure coding | <input type="checkbox"/> Industrial control incident response |
| <input type="checkbox"/> Defending web applications | <input type="checkbox"/> Compliance |
| <input type="checkbox"/> Digital forensics | <input type="checkbox"/> Hosting - Securing Information Systems |

iv. Survey 1 indicates that security for the majority relies heavily on firewalls and antivirus while proactive tools (eg. EWS, VoIP encryption, DLP) have low rates of adoption. Why do you think this is?

- | | |
|---|--|
| <input type="radio"/> Cost of such tools is too high | <input type="radio"/> Difficulty in choosing the right tools |
| <input type="radio"/> Lack of knowledge of such tools | <input type="radio"/> Mindsets need to change about proactive security |

v. Identity theft accounted for more than half the total of all breach incidents in 2014 (Gemalto Breach-Level-Index-Annual-Report-2014). How is the flow of data managed in your organisation?

- | | |
|---|--|
| <input type="checkbox"/> I'm not aware that the data flow is managed | <input type="checkbox"/> Sensitive data is encrypted for internal movement |
| <input type="checkbox"/> Data is limited (contained) to certain places | <input type="checkbox"/> Sensitive data is encrypted for external movement |
| <input type="checkbox"/> The number of people with access to data is controlled | <input type="checkbox"/> Encryption keys are securely stored |
| <input type="checkbox"/> Users are authenticated | |

vi. Does your organisation have an escalation route where staff can report anything that seems suspicious?

- | | |
|---|---|
| <input type="radio"/> We have a proper action plan with designated people | <input type="radio"/> I trust that nothing suspicious can get through to me |
| <input type="radio"/> I am not actively encouraged to refer anything suspicious | <input type="radio"/> Don't know - I'm not aware of one |

vii. Respondents confirmed a low level of Information Security Management certificates in the work-place, e.g. ISO 27001. Do such certificates provide real benefits for the company?

- | | |
|--|---|
| <input type="radio"/> Yes, because they fulfil tender requirements | <input type="radio"/> No, because they require too many resources |
| <input type="radio"/> Yes, because they help increase security | <input type="radio"/> No, they provide no benefits, just additional bureaucracy |
| <input type="radio"/> Yes, because they are required by auditors | <input type="radio"/> No, I don't see how they are relevant to my line of work |
| <input type="radio"/> No, because they are too costly | <input type="radio"/> What is ISO 27001? |

viii. Most compromises are detected by an external entity. Do you think that this is because...?

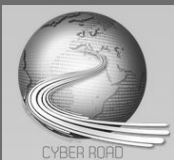
- | | |
|--|---|
| <input type="radio"/> The majority of compromises are from insiders | <input type="radio"/> Inability to detect network intrusion |
| <input type="radio"/> Most organizations do not have the internal resources for compromise detection | <input type="radio"/> Lack of awareness of data compromises |
| <input type="radio"/> Many organizations are not able to detect exfiltration of data | |

ix. Do you think there is too much pressure to prematurely roll out IT / web applications and projects, despite security concerns?

- | | |
|---------------------------|--------------------------|
| <input type="radio"/> Yes | <input type="radio"/> No |
|---------------------------|--------------------------|

x. If yes, what is the reason behind the pressure?

- | | |
|---|--|
| <input type="radio"/> Commercial | <input type="radio"/> Lack of security testing within the product or application plan |
| <input type="radio"/> Cost | <input type="radio"/> Lack of standards or certification of IT applications and projects |
| <input type="radio"/> Poor project planning | |



6. Threats

i. Social engineering is the most common form of attack on personal data, mainly via phishing and spear phishing. How highly do you rate your ability to thwart an attempt at phishing?

- | | |
|---|---|
| <input type="radio"/> Very high - I don't think I would get caught out | <input type="radio"/> I don't know what phishing is |
| <input type="radio"/> High - I'm confident I would catch most phishing attempts | <input type="radio"/> I don't know what spear phishing is |
| <input type="radio"/> Moderate - I'm aware of what it is but I can't be sure I would spot it every time | <input type="radio"/> I think everyone will fall for phishing, if it is well prepared for a specific person |
| <input type="radio"/> Not at all sure | |

ii. Using the likelihood scale provided what, according to your own experience, is the likelihood of the listed cyber threats occurring?

Scale of Likelihood		Likelihood of occurrence
Highly probable/Likely	10	1 per day - Very likely target
Medium/Possible	5	1 per week - Possible target
Low/Remote	2	1 per month - Remote target
Negligible/Unlikely	1	Unexpected - Unlikely target

Cyber threats (based on ENISA's Top Emerging Threats):

	Highly probable (10)	Medium/possible (5)	Low/remote (2)	Negligible/unlikely (1)
Malicious code: Worms/Trojans	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web-based attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web application / Injection attacks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Botnet activity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Denial of service (DoS, DDoS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exploit kits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data breaches	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Physical damage/theft/loss	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Insider threat	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information leakage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Identity theft/fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber espionage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ransomware/Rogueware/Scareware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber terrorism	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify)

iii. What would be the consequences of a cyber attack on the following top targets from Survey #1

Level		Consequence on assets
High/Severe	10	Irreparable harm to the company (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury
Medium/Major	5	Significant harm (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low/Moderate	2	Moderate harm (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.
Minor	1	Very unlikely to cause any harm to the company or caused injuries

Use the Consequence Scale to rate an asset at risk.

	Consequence Scale
Personal data	<input type="text"/>
Critical information	<input type="text"/>
Intellectual Property Rights	<input type="text"/>
On-Line services/Web applications	<input type="text"/>
Critical infrastructures	<input type="text"/>
Workstations (Users' equipment)	<input type="text"/>
People (employees)	<input type="text"/>
Banking & financial service	<input type="text"/>
Payment systems	<input type="text"/>
Mobile devices (tablets, smartphones)	<input type="text"/>

iv. Please quantify the importance of the following risks for your organisation.

	Very important	Medium importance	Not important
Direct financial losses & damage (money stolen from accounts, regulatory fees, loss of clients, business, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Indirect financial losses (loss of reputation, brand, trust, missed business opportunities, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health & safety	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Environmental	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

v. Please quantify the importance of threat analysis to your place of work.

- Highest importance
- Important but other areas receive more attention
- Not very high
- Low



7. Trust

i. What sources of cybercrime data do you trust most?

	No trust at all	Reasonable level of trust	High level of trust
Security news articles	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber security bloggers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Government advisories	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Academic papers / conference proceedings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blacklists / block lists	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media e.g via Twitter, Facebook, google+, & similar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Your own discoveries e.g. log files, infections, & incidents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-virus vendors	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cert vulnerability & threat advisories	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber security associations e.g Owasp, APWG, Maawg, & similar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Other (please specify)



CyberROAD: Cybercrime - Survey #2 - Technology & Organisation

8. Next steps

The following information is optional. If you're happy to give us your contact information we will inform you of the overall survey results. Your personal details will not be used for any other purpose. Thank you for participating.

Name

Company

Email Address

SURVEY #3



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme



CyberROAD: Cybercrime - Survey #3 - Social, Economic and Political issues.

Welcome to the CyberROAD Survey on Cybercrime

Thank you for participating in the CyberROAD Cybercrime Survey #3.

This questionnaire is a follow-on from Survey #1 where participants provided responses to questions exploring an individual's relationship to aspects of cybercrime. Survey #3 probes further into three specific areas: social, economic and political issues.

A second questionnaire in this round, Survey #2, concentrates on technology and organisations.

Each survey is independent of the others so you may choose to complete Survey #2 only, or Survey #3 only, but please try to find the time to make your contribution to our project even more valuable by completing both. Survey #3 should take around 15 - 20 minutes to complete.

We hope you will enjoy participating in our project and we look forward to your responses. Please note the survey is anonymous and providing personal data is entirely optional.

CyberROAD is a research project funded by the European Commission. The project's aim is to identify current and future issues in the fight against cybercrime and cyberterrorism in order to develop a definitive research roadmap.

Data Protection

The CyberROAD project is committed to the protection of personal data. CyberROAD adheres to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community, institutions and bodies and on the free movement of such data. Further information is available here: http://europa.eu/legislation_summaries/information_society/data_protection/l24222_en.htm

CyberROAD also adheres to the Code of Standards and Ethics for Market, Opinion, and Social Research (CASRO). Further information is available here: <http://www.casro.org/?page=TheCASROCode2014>

Survey Contact - jart.armin@cyberroad.eu

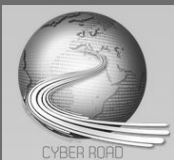


1. About You & Your Work

i. In which country do you currently reside?

ii. Which category most closely fits your organization type?

- Scholarly research
- Policy making, Govt, legal or law enforcement
- Cyber security practitioner, cyber security expert (any field)
- Other (please specify)
- Internet service provider or operator
- Consumer group or end-user
- Commercial business



2. Cybercrime definitions and classifications

i. The development of a taxonomy (classification into named categories based on shared characteristics) is an essential infrastructure in scientific research and other fields of study. Taxonomies help to: identify and enumerate, improve communications, publicise results, metrics and ranking for funding, etc. How important is the building of a recognised taxonomy to the study of cybercrime?

- Extremely Not very important
 Important but not essential Not at all important

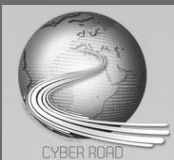
ii. Survey 1 respondents had no clear preference towards any one definition of cybercrime. How important do you think it is to achieve an internationally recognised definition?

- Extremely Not very important
 Important Not at all important

iii. What would be your definition?

iv. Established cybercriminal *modus operandi* are influencing the landscape of serious and organised crime, according to a recent report from Europol. Do you think that cybercrime is now a bigger risk than 'conventional' crime?

- Yes
 No
 It's becoming increasingly difficult to separate cybercrime and conventional crime



3. Cybercrime concerns

i. How real a problem do you think cyber espionage is?

- A matter of national security
 Political propaganda
 Exaggerated
 Legitimate form of intelligence gathering

ii. Do you believe any of the following actions are socially acceptable?

	Yes	No	Undecided
Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Copyright infringement (e.g. movies, music...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DoS (denial of service) - critical safety operations (transport, utilities, etc)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DoS (denial of service) - non-critical operations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interception of private communications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit goods online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online fake pharmacy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online Child Sexual Abuse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Black hat SEO	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hacking into servers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cybersex	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cybersquatting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Website defacement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber bullying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bullet proof hosting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tracking of web activity without permission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



4. Education in cybercrime

i. Survey 1 respondents see cybercrime as a problem rooted mainly in economic interests. Do you believe that cybercrime is mainly driven by an opportunity for easy money?

Yes

No

Please give a reason for your answer

ii. Do you think it is possible to fully determine the root causes of cybercrime ?

Yes

No

Please give a reason for your answer

iii. Respondents indicate a low level of training on cybersecurity within the workplace. Who should be responsible for the cost of training?

Governments

Schools/colleges by adding to the syllabus

Work organizations

Yourself

iv. Should organisations require members of staff to hold a current license or qualification in use of the Internet and cybercrime prevention?

Yes

No



5. The targets of cybercrime

i. Why do you think most respondents to Survey 1 only receive cybersecurity training after a problem and not on a regular basis?

- 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

ii. Give an example of the cybercriminal activity you personally encountered either at home or at work.

- Phishing
- Spam
- Rogueware/Ransomware/Scareware
- Data Breaches (Compromising Confidential Information)
- Information leakage
- Targeted Attack
- Botnet
- Malware
- Drive-by exploit from an infected website
- Code injection
- Exploit Kit
- DNS manipulation
- Not sure what the cause was

iii. **For previous victims of cybercrime only.** Survey 1 participants describe the two greatest effects of cybercrime as: "down time" & "inconvenience". How much time would you estimate you lost when you became a victim of cybercrime?

- < 4 hours
- 5 - 8 hours
- 9 - 24 hours
- 25 hours +
- 60 hours +

iv. Do you believe that expected penalties for cybercrime are:

- Too low
- Adequate
- Too high
- Not sure what the penalties are



6. What risks are you exposed to?

i. Have we lost control of our personal data online?

Yes

No

It's not important if control is lost

It's time to take control back

ii. Do you think about your security when you surf/use the Internet?

Yes, I think about it all the time

Yes, primarily when someone expects some
action/reaction from me

I think about it from time to time

No, I do not think about it at all



7. The effects of cybercrime

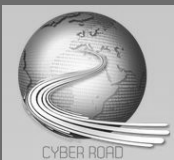
i. Should consumer rights organizations in any country or region (e.g., the European BEUC, Bureau Européen des Unions de Consommateurs, or National Data Protection Authorities DPA's, similar to the Federal Trade Commission, FTC in the USA), be given enhanced powers to sanction heavier legal & financial penalties, when poor security measures result in data breaches or cybercriminal events?

Yes No

Other (please specify)

ii. What sources of cybercrime information do you trust most?

- | | |
|--|---|
| <input type="radio"/> National news services | <input type="radio"/> Anti-virus / commercial vendors |
| <input type="radio"/> International news sources | <input type="radio"/> Social media e.g via Twitter, Facebook, google+.... |
| <input type="radio"/> Government information sources | <input type="radio"/> Academic papers / conference proceedings |
| <input type="radio"/> CERT vulnerability & threat advisories | <input type="radio"/> Web articles and blogs |
| <input type="radio"/> Other (please specify) | |



8. Cyber Security Management

i. Do you feel responsible for your own security on the Internet?

- Yes, it is entirely my responsibility
 No, it is of little concern
 Yes, I feel very responsible
 No, I do not feel responsible at all
 Yes, I feel partly responsible

ii. Who in your opinion is, or should be, responsible for security on the Internet? More than 1 choice can be selected.

- Internet service and content providers (ISPs ... Mobile Operators..)
 Police
 Government agencies
 IT and security departments in companies
 International Internet organizations; e.g. ICANN
 CERTs
 Search Engine or web browser providers; e.g. Google, Yahoo, Microsoft
 End users
 System providers; e.g. Microsoft, Apple
 Other (please specify)

iii. To improve cyber security ROI (Return On Investment) where should money be spent in the future?

	Top ROI	2nd	3rd	4th	5th	Bottom ROI
Cybercrime definitions and classifications	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Education in cybercrime prevention	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Risks & effects of cybercrime	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyber security management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Economic impact of cybercrime	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Laws and policies on cybercrime	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

iv. Sharing of information of cybercrime events within an organization with outside entities is not common practice according to Survey 1 respondents. Do you think information sharing is...?

- A waste of time
- Unnecessary
- Useful to others but I don't trust another entity with the information
- Useful to others but I don't know who to share this with
- Useful to others but it is too time consuming/complicated
- Potentially damaging for me/my organization to report this information

v. Would you share information about cybercrime events/attack with any of the following?

- Internet service and content providers
- Government
- Police
- IT and security departments in companies
- CERTs
- Independent groups
- Please expand your answer if needed
- Private specialists - large company
- Private specialists - small company
- Not for profits
- End users
- No one - this information doesn't need to be shared

vi. Do you think that free software covers all your security needs, the needs of your organisation, or would you spend more on your online security, if finance were not an issue?

- Yes I would spend more if I could
- No I do not need to spend more
- Free open source software fulfils my personal security needs
- Free open source software fulfils my organisation's needs
- Free open source software does not fulfil my personal security needs
- Free open source software does not fulfil my organisation's needs

vii. Do you think money is currently being invested into the right technologies to fight cybercrime?

- Yes
- No

Please expand on your answer here if needed



9. Economic impact of cybercrime

i. What do you think the estimated spend (in US Dollars) will be on information security worldwide in 2015?

- | | |
|---------------------------------------|--|
| <input type="radio"/> 20 - 35 billion | <input type="radio"/> 80 - 95 billion |
| <input type="radio"/> 35 - 50 billion | <input type="radio"/> 95 - 110 billion |
| <input type="radio"/> 50 - 65 billion | <input type="radio"/> 110+ billion |
| <input type="radio"/> 65 - 80 billion | |

ii. Half of respondents had 'no idea' what the cost of cybercrime is to either the economy of their country or the world. Is this because...?

- | | |
|--|---|
| <input type="radio"/> It is not important to know how much it costs the economy | <input type="radio"/> It is too large a scale to comprehend |
| <input type="radio"/> I am only interested in how cybercrime affects me personally | <input type="radio"/> The cost of cybercrime is too complex to measure accurately |
| <input type="radio"/> I don't believe the figures in the news | |

iii. Respondents view education of end-users as very important. Who should be responsible for their education?

- | | |
|--|---|
| <input type="radio"/> Individual end-users | <input type="radio"/> Service providers |
| <input type="radio"/> Government | <input type="radio"/> System providers |
| <input type="radio"/> CERTS | <input type="radio"/> Schools/colleges |
| <input type="radio"/> Other (please specify) | |



10. Research into cybercrime

i. There are opposing views on encryption, which do you think is most valid?

(1) One of the major methods for fighting cybercrime & improved privacy is better encryption of data and communications.

(2) "Encrypted communications are becoming perhaps the biggest problem for the police and the security service authorities in dealing with the threats from terrorism" & "Concerned at moves by companies such as Apple to allow customers to encrypt data on their smartphones." - (Europol's chief, and other governmental agencies)

- (a) better and more encryption of data and communications
- (b) less encryption of data and communications
- (c) a balance is appropriate, for some level of encryption, but provide police and security service authorities the ability to de-encrypt any data or communications
- (d) Not sure

ii. If you selected (b), (c) or (d) for question 10. ii., which of the following do you think is acceptable?

- Only my national police or security service authority can intercept and / or decrypt my online data or communications when dealing with threats from terrorism
- Any police or security service authority internationally can intercept and / or decrypt my online data or communications when dealing with threats from terrorism
- Interception or decryption of my personal online data or communications, can only be carried out by police or security service authority in response to a court order or warrant.
- There should be no interception or decryption of my or others' personal online data or communications



11. Next steps

The following information is optional. If you're happy to give us your contact information we will inform you of the overall survey results. Your personal details will not be used for any other purpose. Thank you for participating.

Name

Company

Email Address

THE DELPHI PROCESS IN PRACTICE



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

Questions	Survey 1	Survey 1 - English	Survey # 2	Rank	Survey # 2	Rank	Survey #3	Survey #3	Survey #3	Rank														
			Technical	1 to 5	Organizational	1 to 5	Social	Economic	Political	1 to 5														
1	In which country do you currently reside? Repeat	respondents from 42 countries (890)	In which country are you based?	5	In which country are you based?	5	In which country are you based?	In which country are you based?	In which country are you based?	5														
2	What is your age?	<table border="1"> <tr><td>18 to 24</td><td>4.6%</td></tr> <tr><td>25 to 34</td><td>31.0%</td></tr> <tr><td>35 to 54</td><td>53.5%</td></tr> <tr><td>55 to 64</td><td>9.0%</td></tr> <tr><td>65 +</td><td>1.9%</td></tr> </table>	18 to 24	4.6%	25 to 34	31.0%	35 to 54	53.5%	55 to 64	9.0%	65 +	1.9%												
18 to 24	4.6%																							
25 to 34	31.0%																							
35 to 54	53.5%																							
55 to 64	9.0%																							
65 +	1.9%																							
3	Where is the main business of your company located	respondents from 42 countries																						
4	How many employees work for your company?	<table border="1"> <tr><td>1-5</td><td>11.1%</td></tr> <tr><td>6-20</td><td>9.3%</td></tr> <tr><td>21-100</td><td>16.4%</td></tr> <tr><td>101-500</td><td>21.0%</td></tr> <tr><td>501-1000</td><td>11.8%</td></tr> <tr><td>1000+</td><td>30.4%</td></tr> </table>	1-5	11.1%	6-20	9.3%	21-100	16.4%	101-500	21.0%	501-1000	11.8%	1000+	30.4%										
1-5	11.1%																							
6-20	9.3%																							
21-100	16.4%																							
101-500	21.0%																							
501-1000	11.8%																							
1000+	30.4%																							
5	Which category most closely fits your organisation type? Repeat	<table border="1"> <tr><td>Scholarly research</td><td>32.3%</td></tr> <tr><td>Policy making, Govt, legal or law enforcement</td><td>10.1%</td></tr> <tr><td>Cyber security practitioner, cyber security expert (any Internet service provider or operator</td><td>14.7%</td></tr> <tr><td>Consumer group or end-user</td><td>6.0%</td></tr> <tr><td>Commercial business</td><td>1.8%</td></tr> <tr><td>Other (please specify)</td><td>14.5%</td></tr> <tr><td></td><td>20.7%</td></tr> </table>	Scholarly research	32.3%	Policy making, Govt, legal or law enforcement	10.1%	Cyber security practitioner, cyber security expert (any Internet service provider or operator	14.7%	Consumer group or end-user	6.0%	Commercial business	1.8%	Other (please specify)	14.5%		20.7%	Which organizational category most closely fits you? <Triad>	5	Which organizational category most closely fits you? <Triad>	5	Which organizational category most closely fits you? <Triad>	Which organizational category most closely fits you? <Triad>	Which organizational category most closely fits you? <Triad>	5
Scholarly research	32.3%																							
Policy making, Govt, legal or law enforcement	10.1%																							
Cyber security practitioner, cyber security expert (any Internet service provider or operator	14.7%																							
Consumer group or end-user	6.0%																							
Commercial business	1.8%																							
Other (please specify)	14.5%																							
	20.7%																							
Definition of cybercrime																								
6	For me cybercrime is.....	<p>For me cybercrime is.....</p>	<p>Top 3 from survey # 1 = pick best one:</p> <ul style="list-style-type: none"> -Criminal activity carried out by means of computers or the Internet - Any criminal act or hacking of computers and networks - Any act against the confidentiality, integrity and availability of computer data and systems 	5	<p><graded response></p> <ul style="list-style-type: none"> * spam * phishing * spear phishing * copyright infringement (e.g. Megaupload) * DDos * Interception of private communications * counterfeit goods online * online fake pharmacy * child pornography * Blackhat SEO * hacking into server or data operations * cybersex * data breach * cybersquatting * hacking websites for defacement * cyber bullying * Bullet proof hosting <use comment box> Others? 	5	<p>Survey 1 respondents had no clear preference towards any one definition of cybercrime. How important do you think it is to achieve an internationally recognised definition?</p> <ul style="list-style-type: none"> * Extremely * Important but not essential * Not very important * Not at all important <p>* <comment box maximum 140 characters> what would be your definition?</p>	<p><graded response></p> <ul style="list-style-type: none"> * spam * phishing * spear phishing * copyright infringement (e.g. Megaupload) * DDos * Interception of private communications * counterfeit goods online * online fake pharmacy * child pornography * Blackhat SEO * hacking into server or data operations * cybersex * data breach * cybersquatting * hacking websites for defacement * cyber bullying * Bullet proof hosting <use comment box> Others? 	5															
	Taxonomy						<p>The development of a taxonomy (define...) is an essential infrastructure to scientific research and other fields of study, helping with communications, publishing of results, metrics, ranking for funding, etc. How important is the building of a recognised taxonomy to the study of cybercrime?</p> <ul style="list-style-type: none"> * Extremely * Important but not essential * Not very important * Not at all important 			4														
Cybercrime concerns																								
7	Are you concerned about cybercrime?	<table border="1"> <tr><td>Extremely concerned</td><td>24.3%</td></tr> <tr><td>Very concerned</td><td>31.5%</td></tr> <tr><td>Moderately concerned</td><td>32.1%</td></tr> <tr><td>Slightly concerned</td><td>8.8%</td></tr> <tr><td>Not at all concerned</td><td>3.3%</td></tr> </table>	Extremely concerned	24.3%	Very concerned	31.5%	Moderately concerned	32.1%	Slightly concerned	8.8%	Not at all concerned	3.3%					Do you believe any form of cybercrime is socially acceptable? Yes/No - If yes what ?		Do you believe cyber espionage is a real problem? 1= a matter of national security - 2= exaggerated 3= political propaganda, 4= legitimate form of intelligence gathering	3				
Extremely concerned	24.3%																							
Very concerned	31.5%																							
Moderately concerned	32.1%																							
Slightly concerned	8.8%																							
Not at all concerned	3.3%																							
8	Is cybercrime a concern for your organisation?	<table border="1"> <tr><td>Extremely concerned</td><td>22.3%</td></tr> <tr><td>Very concerned</td><td>27.9%</td></tr> <tr><td>Moderately concerned</td><td>33.8%</td></tr> <tr><td>Slightly concerned</td><td>12.8%</td></tr> <tr><td>Not at all concerned</td><td>3.2%</td></tr> </table>	Extremely concerned	22.3%	Very concerned	27.9%	Moderately concerned	33.8%	Slightly concerned	12.8%	Not at all concerned	3.2%					<p>Established cybercriminal <i>modus operandi</i> are influencing the landscape of serious and organised crime, according to a recent report from Europol. Do you think that cybercrime is now a bigger risk than 'conventional' crime?</p> <ul style="list-style-type: none"> * Yes * No * It's becoming increasingly difficult to separate cybercrime and conventional crime 	<p>What do you think the estimated spend (in US Dollars) will be on information security in 2015?</p> <p>20 - 35 billion 35 - 50 billion 50 - 65 billion 65 - 80 billion 80 - 95 billion 95 - 110 billion 110+ billion</p>		3				
Extremely concerned	22.3%																							
Very concerned	27.9%																							
Moderately concerned	33.8%																							
Slightly concerned	12.8%																							
Not at all concerned	3.2%																							
9	Over the next 5 years do you think cybercrime will...?	<table border="1"> <tr><td>Increase</td><td>91.5%</td></tr> <tr><td>Decrease</td><td>1.8%</td></tr> <tr><td>Stay at the same level</td><td>6.7%</td></tr> </table>	Increase	91.5%	Decrease	1.8%	Stay at the same level	6.7%																
Increase	91.5%																							
Decrease	1.8%																							
Stay at the same level	6.7%																							

What does cybercrime mean to you																				
10	Do you think cybercrime is...?	<table border="1"> <tr> <td>Here to stay</td> <td>57.5%</td> </tr> <tr> <td>Solvable</td> <td>3.8%</td> </tr> <tr> <td>Containing</td> <td>37.7%</td> </tr> <tr> <td>Not much of an issue</td> <td>1.0%</td> </tr> </table>	Here to stay	57.5%	Solvable	3.8%	Containing	37.7%	Not much of an issue	1.0%										
Here to stay	57.5%																			
Solvable	3.8%																			
Containing	37.7%																			
Not much of an issue	1.0%																			
11	Do you see cybercrime as a problem rooted in...?	<p>4. Do you see cybercrime as a problem rooted in...?</p>				<p><research gap?> Is it possible to determine the root causes of cybercrime ?</p> <p>Do you believe that cybercrime is mainly driven by an opportunity for easy money?</p>	<p>Who in your opinion is responsible for security on the Internet (pick 3)</p> <ul style="list-style-type: none"> • Internet service and content providers • the Police (and government in general) • IT and security departments in companies • CERTs • the end user • others 	5												
Targets of cybercrime																				
12	In your organisation, which do you think is most likely to be the target for cybercriminals?	<p>1. In your organisation, which do you think is most likely to be the target for cybercriminals?</p>	<p>Most respondents indicated "personal data" as the most likely target for cybercriminals in their organization. Should personal data be separated from the workplace?</p>			<p>Have we lost control of our personal data online?</p> <ul style="list-style-type: none"> • Yes • No • It's time to take control back • It's not important if control is lost 														
What risks are you exposed to																				
13	Does your organisation (or do you) apply risk management as part of a cyber security strategy?	<table border="1"> <tr> <td>Yes</td> <td>54.0%</td> </tr> <tr> <td>No</td> <td>20.7%</td> </tr> <tr> <td>Don't know</td> <td>25.3%</td> </tr> </table>	Yes	54.0%	No	20.7%	Don't know	25.3%												
Yes	54.0%																			
No	20.7%																			
Don't know	25.3%																			
14	Does someone in the company (or do you) formally and regularly keep up-to-date with cybercrime related news via...?	<table border="1"> <tr> <td>Generic newspapers and news broadcaster</td> <td>17.2%</td> </tr> <tr> <td>Specialized news sources</td> <td>46.1%</td> </tr> <tr> <td>Consulting companies</td> <td>5.2%</td> </tr> <tr> <td>Activities outsourced to external company/ies</td> <td>5.6%</td> </tr> <tr> <td>Social network contacts</td> <td>7.9%</td> </tr> <tr> <td>No time allocated to do this</td> <td>18.0%</td> </tr> </table>	Generic newspapers and news broadcaster	17.2%	Specialized news sources	46.1%	Consulting companies	5.2%	Activities outsourced to external company/ies	5.6%	Social network contacts	7.9%	No time allocated to do this	18.0%		<p>Do you feel you share responsibility for the IT security of your company?</p> <ul style="list-style-type: none"> • Yes, I think about it all the time • Yes, primarily when someone expects some action/reaction from me • I think about it from time to time • No, I do not think about it at all • I only share a small responsibility • No, I do not share responsibility 				
Generic newspapers and news broadcaster	17.2%																			
Specialized news sources	46.1%																			
Consulting companies	5.2%																			
Activities outsourced to external company/ies	5.6%																			
Social network contacts	7.9%																			
No time allocated to do this	18.0%																			
15	How often are staff given training about cyber security risks?	<table border="1"> <tr> <td>Weekly</td> <td>5.6%</td> </tr> <tr> <td>Monthly</td> <td>8.5%</td> </tr> <tr> <td>Yearly</td> <td>22.7%</td> </tr> <tr> <td>Never</td> <td>16.5%</td> </tr> <tr> <td>Only if there is a problem</td> <td>25.6%</td> </tr> <tr> <td>Don't know</td> <td>21.1%</td> </tr> </table>	Weekly	5.6%	Monthly	8.5%	Yearly	22.7%	Never	16.5%	Only if there is a problem	25.6%	Don't know	21.1%	<p>Do you hold certificates in, or attended, technical security training in any of the following areas:</p> <ul style="list-style-type: none"> -Information Security (general) -Cyber security for IT Administrators -Mitigation Strategies -Advanced Security -Incident prevention -Secure coding -Defending web applications -Digital forensics -Incident forensics -Cyber Threat intelligence -CISSP (Certified Information Systems Security Professional) -Security audits -Data security law -Industrial control incident response -Compliance -Hosting - Securing Information Systems Other (Specify) 			<p>Respondents indicate a low level of training on cybersecurity within the workplace. Who should be responsible for the cost of training?</p> <ul style="list-style-type: none"> • Governments • Organization • school / collage add to syllabus 	<p>Should organizations require members of staff to hold a current license or qualification in use of the Internet & cybercrime preventions?</p>	
Weekly	5.6%																			
Monthly	8.5%																			
Yearly	22.7%																			
Never	16.5%																			
Only if there is a problem	25.6%																			
Don't know	21.1%																			
16	Does your organisation allow the use of Bring Your Own Devices (BYOD)?	<table border="1"> <tr> <td>Yes</td> <td>65.6%</td> </tr> <tr> <td>No</td> <td>34.4%</td> </tr> </table>	Yes	65.6%	No	34.4%	<p>Survey 1 indicates BYOD is now common within the workplace but rates of best practices/guidance on safe use are low. How highly do you rate this as a potential security risk?</p> <ul style="list-style-type: none"> • Very high • High • Medium • Low 													
Yes	65.6%																			
No	34.4%																			

17	Does your organisation have a best practices policy for BYOD?	<table border="1"> <tr> <td>Yes</td> <td>28.3%</td> </tr> <tr> <td>No</td> <td>41.6%</td> </tr> <tr> <td>Don't know</td> <td>30.2%</td> </tr> </table>	Yes	28.3%	No	41.6%	Don't know	30.2%	Do you think that there is a need for BYOD security policies to be introduced in every organisation?											
Yes	28.3%																			
No	41.6%																			
Don't know	30.2%																			
					<p>Many respondents indicated a general lack of formal policies on cybersecurity management in their place of work. Why do you think this is?</p> <ul style="list-style-type: none"> • Insufficient awareness within executive management • Insufficient resources to prepare the documents • Insufficient knowledge to prepare the documents • There is no need for such policies • Other (specify) 															
			<p>How effective do you think benchmarking and best practices could be in raising performance and developing trust?</p> <p>i) Extremely ii) Very iii) Slightly iv) Not at all Other (specify)</p>																	
			<p>For most respondents staff training in cybersecurity only takes place when there is a problem or, at best, once a year. Why do you think this is?</p> <ul style="list-style-type: none"> • 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 			<p>For most respondents staff training in cybersecurity only takes place when there is a problem or, at best, once a year. Why do you think this is?</p> <ul style="list-style-type: none"> • 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 														
The effects of cybercrime																				
18	Have you experienced a cybercriminal action in the last 5 years in a...?	<table border="1"> <caption>i. Have you experienced a cybercriminal action in the last 5 years in a...?</caption> <thead> <tr> <th>Category</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Personal capacity</td> <td>~25%</td> </tr> <tr> <td>Through work</td> <td>~42%</td> </tr> <tr> <td>Never</td> <td>~42%</td> </tr> </tbody> </table>	Category	Percentage	Personal capacity	~25%	Through work	~42%	Never	~42%				<p>Give an example of the cybercriminal activity you personally encountered in your company or in your private life.</p> <ul style="list-style-type: none"> • Phishing • Spam • Rogueware/Ransomware/Scareware • Data Breaches (Compromising Confidential Information) • Information leakage • Targeted Attack • Botnet • Worm/Trojan • Drive-by exploit • Code injection • Exploit Kit • DNS manipulation 						
Category	Percentage																			
Personal capacity	~25%																			
Through work	~42%																			
Never	~42%																			
19	If you have been a victim of cybercrime in the last 5 years, what was the effect of the action?	<table border="1"> <tr> <td>Loss of money</td> <td>14.1%</td> </tr> <tr> <td>Down time</td> <td>29.8%</td> </tr> <tr> <td>Inconvenience</td> <td>46.8%</td> </tr> <tr> <td>Psychologically harmful</td> <td>10.5%</td> </tr> <tr> <td>Loss of reputation</td> <td>10.5%</td> </tr> <tr> <td>No effect</td> <td>33.3%</td> </tr> </table>	Loss of money	14.1%	Down time	29.8%	Inconvenience	46.8%	Psychologically harmful	10.5%	Loss of reputation	10.5%	No effect	33.3%				<p>Victims of cybercrime describe the two largest effects were: "down time" & "inconvenience" - What would you estimate the time lost was:</p> <ul style="list-style-type: none"> < 4 hours 5 - 8 hours 9 - 24 hours 25 hours + 		
Loss of money	14.1%																			
Down time	29.8%																			
Inconvenience	46.8%																			
Psychologically harmful	10.5%																			
Loss of reputation	10.5%																			
No effect	33.3%																			
20	As a direct result of a cybercriminal attack or threat, did you/your work make any changes to the cyber security strategy?	<table border="1"> <tr> <td>Yes</td> <td>44.7%</td> </tr> <tr> <td>No</td> <td>12.4%</td> </tr> <tr> <td>Don't know</td> <td>15.7%</td> </tr> <tr> <td>N/A</td> <td>27.2%</td> </tr> </table>	Yes	44.7%	No	12.4%	Don't know	15.7%	N/A	27.2%										
Yes	44.7%																			
No	12.4%																			
Don't know	15.7%																			
N/A	27.2%																			
21	If you have experienced a cyber attack, do you think it posed a systemic risk to you or your organisation?	<table border="1"> <tr> <td>Yes</td> <td>41.0%</td> </tr> <tr> <td>No</td> <td>28.9%</td> </tr> <tr> <td>Don't know</td> <td>30.1%</td> </tr> </table>	Yes	41.0%	No	28.9%	Don't know	30.1%												
Yes	41.0%																			
No	28.9%																			
Don't know	30.1%																			

22	If you have been a victim of cybercrime, what action followed?	<table border="1"> <tr><td>Reported to the police with no further action</td><td>8.1%</td></tr> <tr><td>Reported to the police, who contacted me /my</td><td>6.3%</td></tr> <tr><td>Reported to the police, who followed it through but no</td><td>8.8%</td></tr> <tr><td>Reported to the police, who followed it through to</td><td>7.2%</td></tr> <tr><td>Not reported to police</td><td>36.6%</td></tr> <tr><td>Didn't know how to report to the police</td><td>5.8%</td></tr> <tr><td>Other</td><td>27.3%</td></tr> </table>	Reported to the police with no further action	8.1%	Reported to the police, who contacted me /my	6.3%	Reported to the police, who followed it through but no	8.8%	Reported to the police, who followed it through to	7.2%	Not reported to police	36.6%	Didn't know how to report to the police	5.8%	Other	27.3%			Survey 1 showed that most victims of cybercrime never reported their case to the Police. Why do you think that is?		Do you believe that realistically expected penalties for cybercrime are: <ul style="list-style-type: none"> • Too low • Adequate • Too high 																
Reported to the police with no further action	8.1%																																				
Reported to the police, who contacted me /my	6.3%																																				
Reported to the police, who followed it through but no	8.8%																																				
Reported to the police, who followed it through to	7.2%																																				
Not reported to police	36.6%																																				
Didn't know how to report to the police	5.8%																																				
Other	27.3%																																				
23	If you have been a victim of cybercrime, did you contact your national or government CERT for assistance?	<table border="1"> <tr><td>Reported to national or government CERT, with no</td><td>8.7%</td></tr> <tr><td>Reported to national or government CERT, with action</td><td>10.9%</td></tr> <tr><td>Did not contact CERT but I know the police did</td><td>6.2%</td></tr> <tr><td>Did not contact my national or government CERT</td><td>28.6%</td></tr> <tr><td>Did not know I could report to a CERT</td><td>16.9%</td></tr> <tr><td>Do not know what a CERT is or how to contact them</td><td>28.6%</td></tr> </table>	Reported to national or government CERT, with no	8.7%	Reported to national or government CERT, with action	10.9%	Did not contact CERT but I know the police did	6.2%	Did not contact my national or government CERT	28.6%	Did not know I could report to a CERT	16.9%	Do not know what a CERT is or how to contact them	28.6%			Survey 1 indicates awareness of CERTs (National Computer Emergency Response Team's) is very low. How can this be improved?																				
Reported to national or government CERT, with no	8.7%																																				
Reported to national or government CERT, with action	10.9%																																				
Did not contact CERT but I know the police did	6.2%																																				
Did not contact my national or government CERT	28.6%																																				
Did not know I could report to a CERT	16.9%																																				
Do not know what a CERT is or how to contact them	28.6%																																				
Security management																																					
24	Which of the following security applications do you use on your own computing devices?	<table border="1"> <tr><td>Firewalls</td><td>85.3%</td></tr> <tr><td>Antivirus</td><td>86.8%</td></tr> <tr><td>Vulnerability scanning</td><td>34.4%</td></tr> <tr><td>Spam blocker/secure email gateway</td><td>62.7%</td></tr> <tr><td>Data encryption</td><td>51.1%</td></tr> <tr><td>Early warning system</td><td>8.9%</td></tr> <tr><td>VOIP encryption</td><td>11.0%</td></tr> <tr><td>Password manager</td><td>48.2%</td></tr> <tr><td>VPN</td><td>51.0%</td></tr> <tr><td>Hash generator</td><td>10.0%</td></tr> <tr><td>Back-up system (cloud or onsite)</td><td>65.8%</td></tr> </table>	Firewalls	85.3%	Antivirus	86.8%	Vulnerability scanning	34.4%	Spam blocker/secure email gateway	62.7%	Data encryption	51.1%	Early warning system	8.9%	VOIP encryption	11.0%	Password manager	48.2%	VPN	51.0%	Hash generator	10.0%	Back-up system (cloud or onsite)	65.8%	Survey 1 indicates that the security strategy for the majority heavily relies on firewalls and antivirus while proactive tools (eg. EWS, VoIP encryption, DLP) have low rates of adoption. Why do you think this is? <ul style="list-style-type: none"> • Cost of such tools is too high • Lack of knowledge of such tools • Difficulty in choosing the right tools • Mindsets need to change about proactive security • Other (please specify) 			Do you feel responsible for your own security on the Internet? <ul style="list-style-type: none"> • Yes, it is entirely my responsibility • Yes, I feel very responsible • Yes, I feel partly responsible • No, it is of little concern • No, I do not feel responsible at all 	Who in your opinion is, or should be, responsible for security on the Internet <ul style="list-style-type: none"> • Internet service and content providers • Government • Police • IT and security departments in companies • CERTs • End users • Others (Specify) 								
Firewalls	85.3%																																				
Antivirus	86.8%																																				
Vulnerability scanning	34.4%																																				
Spam blocker/secure email gateway	62.7%																																				
Data encryption	51.1%																																				
Early warning system	8.9%																																				
VOIP encryption	11.0%																																				
Password manager	48.2%																																				
VPN	51.0%																																				
Hash generator	10.0%																																				
Back-up system (cloud or onsite)	65.8%																																				
25	Which of the following security applications does your organisation use?	<table border="1"> <tr><td>Firewalls</td><td>95.2%</td></tr> <tr><td>Antivirus</td><td>93.2%</td></tr> <tr><td>Vulnerability scanning</td><td>53.7%</td></tr> <tr><td>Spam blocker/secure email gateway</td><td>77.4%</td></tr> <tr><td>Data encryption</td><td>54.2%</td></tr> <tr><td>Early warning system</td><td>19.1%</td></tr> <tr><td>VOIP encryption</td><td>16.8%</td></tr> <tr><td>Password manager</td><td>41.9%</td></tr> <tr><td>Hash generator</td><td>12.3%</td></tr> <tr><td>VPN Dedicated resources</td><td>60.1%</td></tr> <tr><td>SIEM (Security information and event management)</td><td>24.3%</td></tr> <tr><td>Back-up system (cloud or onsite)</td><td>66.4%</td></tr> <tr><td>IDS/IPS solution</td><td>36.3%</td></tr> <tr><td>DLP solution</td><td>10.6%</td></tr> <tr><td>Other (please specify)</td><td>4.2%</td></tr> </table>	Firewalls	95.2%	Antivirus	93.2%	Vulnerability scanning	53.7%	Spam blocker/secure email gateway	77.4%	Data encryption	54.2%	Early warning system	19.1%	VOIP encryption	16.8%	Password manager	41.9%	Hash generator	12.3%	VPN Dedicated resources	60.1%	SIEM (Security information and event management)	24.3%	Back-up system (cloud or onsite)	66.4%	IDS/IPS solution	36.3%	DLP solution	10.6%	Other (please specify)	4.2%	Identity theft accounted for more than half the total of all attacks in 2014. Data needs to be secured both inside & outside the network. How is the flow of data managed in your organisation? <ul style="list-style-type: none"> • I'm not aware that the data flow is managed • Data is limited (contained) to certain places • The number of people with access to data is controlled • Users are authenticated • Sensitive data is encrypted for internal movement • Sensitive data is encrypted for external movement • Encryption keys are securely stored • Other 			What investment in security should be made to return the greatest improvements at the lowest possible cost?	
Firewalls	95.2%																																				
Antivirus	93.2%																																				
Vulnerability scanning	53.7%																																				
Spam blocker/secure email gateway	77.4%																																				
Data encryption	54.2%																																				
Early warning system	19.1%																																				
VOIP encryption	16.8%																																				
Password manager	41.9%																																				
Hash generator	12.3%																																				
VPN Dedicated resources	60.1%																																				
SIEM (Security information and event management)	24.3%																																				
Back-up system (cloud or onsite)	66.4%																																				
IDS/IPS solution	36.3%																																				
DLP solution	10.6%																																				
Other (please specify)	4.2%																																				
26	How is your own/your organisation's cyber security managed?	<table border="1"> <tr><td>In-house by someone who is in charge of (security)</td><td>50.8%</td></tr> <tr><td>In-house CERT</td><td>12.5%</td></tr> <tr><td>I manage my own cyber security</td><td>11.9%</td></tr> <tr><td>Outsourced to a independent specialist or</td><td>4.7%</td></tr> <tr><td>By the Internet Service Provider</td><td>1.9%</td></tr> <tr><td>Don't know</td><td>18.2%</td></tr> </table>	In-house by someone who is in charge of (security)	50.8%	In-house CERT	12.5%	I manage my own cyber security	11.9%	Outsourced to a independent specialist or	4.7%	By the Internet Service Provider	1.9%	Don't know	18.2%	Social engineering is the most common form of attack on personal data, mainly via phishing and spear phishing. How highly do you rate your ability to thwart an attempt at phishing? <ul style="list-style-type: none"> • Very high - I don't think I would get caught out • High - I'm confident I would catch most phishing attempts • Moderate - I'm aware of what it is but I can't be sure I would spot it every time • Not at all sure • I don't know what spear phishing is 																						
In-house by someone who is in charge of (security)	50.8%																																				
In-house CERT	12.5%																																				
I manage my own cyber security	11.9%																																				
Outsourced to a independent specialist or	4.7%																																				
By the Internet Service Provider	1.9%																																				
Don't know	18.2%																																				
27	Do you, or does someone else in your organisation, share information about cyber events/attacks with an outside organisation?	<table border="1"> <tr><td>Yes</td><td>35.4%</td></tr> <tr><td>No</td><td>24.8%</td></tr> <tr><td>Don't know</td><td>39.8%</td></tr> </table>	Yes	35.4%	No	24.8%	Don't know	39.8%	Does your organisation have an escalation route			Sharing of information with outside entities is not common practice. Do you think information sharing is...? <ul style="list-style-type: none"> • Unnecessary • A waste of time • Useful to others but I don't trust another entity with the information • Useful to others but I don't know who to share this with • Useful to others but it is too time consuming/complicated • Potentially damaging for me/my organization to report this information 	Would you share information about cyber events/attack with any of the following? <ul style="list-style-type: none"> • Internet service and content providers • Government • Police • IT and security departments in companies • CERTs • Independent groups • Private specialists - large company • Private specialists - small company • Not for profits • End users • No one - this information doesn't need to be shared • Others (Specify) 																								
Yes	35.4%																																				
No	24.8%																																				
Don't know	39.8%																																				

28	Do you/your organisation hold any Information Security Management certificates, e.g., ISO 27001?	<table border="1"> <tr> <td>Yes</td> <td>21.4%</td> </tr> <tr> <td>No</td> <td>33.2%</td> </tr> <tr> <td>Don't know</td> <td>45.4%</td> </tr> </table>	Yes	21.4%	No	33.2%	Don't know	45.4%	<p>Respondents confirmed a low level of Information Security Management certificates in the work-place, e.g. ISO 27001. Do such certificates provide real benefits for the company?</p> <ul style="list-style-type: none"> • Yes, because they fulfil tender requirements • Yes, because they help increase security, • Yes, because they are required by auditors • No, because they are too costly, • No, because they require too many resources, • No, they provide no benefits, just additional bureaucracy. • No, I don't see how they are relevant to my line of work • No, today's technology moves too quickly for such standards • Other (specify) 														
Yes	21.4%																						
No	33.2%																						
Don't know	45.4%																						
29	Do you/your organisation use the following security testing techniques?	<table border="1"> <tr> <td>Penetration testing</td> <td>16.1%</td> </tr> <tr> <td>Vulnerability testing</td> <td>11.8%</td> </tr> <tr> <td>Audits</td> <td>16.4%</td> </tr> <tr> <td>Other</td> <td>5.0%</td> </tr> <tr> <td>Don't know</td> <td>50.7%</td> </tr> </table>	Penetration testing	16.1%	Vulnerability testing	11.8%	Audits	16.4%	Other	5.0%	Don't know	50.7%	<p><Security by design question(s)> Do you think there is too much pressure to prematurely roll out IT applications and projects, despite security concerns. </n></p> <p>What pressure?</p> <ul style="list-style-type: none"> • Commercial • Cost • Poor project planning • Lack of security testing within the product or application plan • Lack of standards or certification of IT applications and projects 										
Penetration testing	16.1%																						
Vulnerability testing	11.8%																						
Audits	16.4%																						
Other	5.0%																						
Don't know	50.7%																						
			DNS & Open resolvers question / insecure / vulnerable cyber infrastructure.....																				
Economic impact																							
30	Currency	<table border="1"> <tr> <td>US\$</td> <td>12.7%</td> </tr> <tr> <td>EURO</td> <td>59.4%</td> </tr> <tr> <td>GBP</td> <td>3.0%</td> </tr> <tr> <td>CHF</td> <td>24.5%</td> </tr> <tr> <td>YEN</td> <td>0.2%</td> </tr> <tr> <td>CAS</td> <td>0.0%</td> </tr> <tr> <td>AUS</td> <td>0.2%</td> </tr> </table>	US\$	12.7%	EURO	59.4%	GBP	3.0%	CHF	24.5%	YEN	0.2%	CAS	0.0%	AUS	0.2%							
US\$	12.7%																						
EURO	59.4%																						
GBP	3.0%																						
CHF	24.5%																						
YEN	0.2%																						
CAS	0.0%																						
AUS	0.2%																						
31	How much do you personally spend annually on cyber security, e.g. anti-virus, anti-spam, upgrades, etc.?	<table border="1"> <tr> <td>0</td> <td>47.0%</td> </tr> <tr> <td>1-100</td> <td>33.7%</td> </tr> <tr> <td>101 -250</td> <td>8.7%</td> </tr> <tr> <td>250+</td> <td>10.6%</td> </tr> </table>	0	47.0%	1-100	33.7%	101 -250	8.7%	250+	10.6%	<p>Most compromises are detected by an external entity. Do you think that this is...?</p> <ul style="list-style-type: none"> • Acceptable • Not acceptable • Not acceptable but I don't know what can be done to change this • Not acceptable but it's not my problem • Not acceptable, I think this can be improved by ... (specify) 			<p>If finances were not an issue, would you spend more on your online security? Or do you think that free software covers all your security needs or the needs of your organisation?</p> <ul style="list-style-type: none"> • Yes I would spend more if I could • No I do not need to spend more • Free software fulfils my personal security needs • Free software fulfils my organisation's needs • Free software does not fulfil my personal security needs • Free software does not fulfil my organisation's needs 									
0	47.0%																						
1-100	33.7%																						
101 -250	8.7%																						
250+	10.6%																						
32	How much does your organisation spend annually on cyber security products?	<table border="1"> <tr> <td>0</td> <td>74%</td> </tr> <tr> <td>1-100</td> <td>6.8%</td> </tr> <tr> <td>101 -500</td> <td>9.2%</td> </tr> <tr> <td>501 - 1,000</td> <td>10.2%</td> </tr> <tr> <td>1,000 - 10,000</td> <td>26.2%</td> </tr> <tr> <td>10,000+</td> <td>40.2%</td> </tr> </table>	0	74%	1-100	6.8%	101 -500	9.2%	501 - 1,000	10.2%	1,000 - 10,000	26.2%	10,000+	40.2%					<p>Do you think money is currently being invested into the right technologies to fight cybercrime?</p> <ul style="list-style-type: none"> • Yes • No • The investment may be right but not enough of these technologies are being used 				
0	74%																						
1-100	6.8%																						
101 -500	9.2%																						
501 - 1,000	10.2%																						
1,000 - 10,000	26.2%																						
10,000+	40.2%																						

33	What do you think is the cost of cybercrime to the economy of your country of residence per annum?	<table border="1"> <tr> <td>Up to 25million</td> <td>60%</td> </tr> <tr> <td>26m - 100m</td> <td>14.9%</td> </tr> <tr> <td>100 million+</td> <td>23.6%</td> </tr> <tr> <td>No idea</td> <td>55.4%</td> </tr> </table>	Up to 25million	60%	26m - 100m	14.9%	100 million+	23.6%	No idea	55.4%				<p>Half of respondents had 'no idea' what the cost of cybercrime is to either the economy of their country or to the world. Is this because...?</p> <ul style="list-style-type: none"> • It is not important to know how much it costs the economy • I am only interested in how cybercrime affects me personally • I don't believe the figures in the news • It is too large a scale to comprehend • The cost of cybercrime is too complex to measure accurately 																						
Up to 25million	60%																																			
26m - 100m	14.9%																																			
100 million+	23.6%																																			
No idea	55.4%																																			
34	What do you think is the cost of cybercrime to the world economy?	<table border="1"> <tr> <td>Less than 1billion</td> <td>1.0%</td> </tr> <tr> <td>1bn - 10bn</td> <td>6.8%</td> </tr> <tr> <td>11bn - 25bn</td> <td>6.7%</td> </tr> <tr> <td>26bn - 100bn</td> <td>14.7%</td> </tr> <tr> <td>Over 100 billion</td> <td>15.7%</td> </tr> <tr> <td>No idea</td> <td>55.2%</td> </tr> </table>	Less than 1billion	1.0%	1bn - 10bn	6.8%	11bn - 25bn	6.7%	26bn - 100bn	14.7%	Over 100 billion	15.7%	No idea	55.2%																						
Less than 1billion	1.0%																																			
1bn - 10bn	6.8%																																			
11bn - 25bn	6.7%																																			
26bn - 100bn	14.7%																																			
Over 100 billion	15.7%																																			
No idea	55.2%																																			
Research																																				
35	To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?	<p>To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?</p> <table border="1"> <thead> <tr> <th>Topic</th> <th>Very important</th> <th>Important</th> <th>Not important</th> </tr> </thead> <tbody> <tr> <td>Better metrics and statistics on cybercrime</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> <tr> <td>Better laws and regulations</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> <tr> <td>Improved technology for reporting and responding</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> <tr> <td>Improvement of understanding of cyber community</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> <tr> <td>Better education and improved privacy</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> <tr> <td>Better software of users of the Internet</td> <td>~200</td> <td>~400</td> <td>~100</td> </tr> </tbody> </table>	Topic	Very important	Important	Not important	Better metrics and statistics on cybercrime	~200	~400	~100	Better laws and regulations	~200	~400	~100	Improved technology for reporting and responding	~200	~400	~100	Improvement of understanding of cyber community	~200	~400	~100	Better education and improved privacy	~200	~400	~100	Better software of users of the Internet	~200	~400	~100	What technical areas to improve? (... Multiple choice)				<p>Respondents view education of end-users as very important. Who should be responsible for their education?</p> <ul style="list-style-type: none"> • Individual end-users • Government • CERTS • Service providers • Schools/colleges • Other (specify) 	
Topic	Very important	Important	Not important																																	
Better metrics and statistics on cybercrime	~200	~400	~100																																	
Better laws and regulations	~200	~400	~100																																	
Improved technology for reporting and responding	~200	~400	~100																																	
Improvement of understanding of cyber community	~200	~400	~100																																	
Better education and improved privacy	~200	~400	~100																																	
Better software of users of the Internet	~200	~400	~100																																	
+	Threat analysis ... ref: ENISA & USCert	<table border="1"> <tr> <td>Yes</td> <td>50.3%</td> </tr> <tr> <td>No</td> <td>49.7%</td> </tr> </table>	Yes	50.3%	No	49.7%	Threat analysis ... ref: ENISA & USCert		<p>The EU has detailed 3 main objectives for the new framework on the protection of personal data: i) to meet the challenges of globalisation and new technologies, ii) to strengthen individual's rights, iii) to improve the clarity and coherence of the rules. What else should be in the new regulations:</p> <ol style="list-style-type: none"> National Data Protection Authorities (DPAs) given more power to impose substantial fines DPAs able to file class actions against violations of data protection DPAs able to regulate the collection and processing of personal data in advertising, market opinion, user profiles, data warehousing, etc Independent consumer rights groups other than DPAs e.g. industry groups, consumer protection agencies, etc., given powers to carry out the above actions Other (specify) 																											
Yes	50.3%																																			
No	49.7%																																			
+					<p>Can you foresee a future when cybercrime is managed via fully global collaborative actions?</p> <ul style="list-style-type: none"> • Yes, within 5 years • Yes, within 5 -10 years • Yes, within 10 – 20 years • Yes, in 20+ years • Never - why? Specify 		<p>Could consumer rights organizations be given enhanced powers such as the ability to sanction legal & financial penalties, due to poor security measures resulting in data breaches or cybercriminal events?</p> <ul style="list-style-type: none"> • No • May be effective but only in addition to technical solutions 																													

								<p>If a system of financial penalties were to be imposed due to poor security measures resulting in data breaches or cybercriminal events, what should the money collected be used for?</p> <p>i) To fund the activities of the DPA's or other independent bodies ii) The public purse iii) Compensation for victims iv) Other (specify)</p>	4
Trust		<p>What sources of cybercrime data do you trust most, please provide a 'trust factor' range 1-5 (1= low trust factor 5= highest):</p> <ul style="list-style-type: none"> - Security news articles - Cyber security bloggers - Government advisories - Academic papers / conference proceedings - Black / block lists - Social media e.g via Twitter, Facebook, google+.... - Your own discoveries e.g. log files, infections, & incidents - Anti-virus vendors - Cert vulnerability & threat advisories - Cyber security associations e.g Owasp, APWG, IMAag.... - Others (please state) 	5				<p>What sources of cybercrime information do (we) you trust most, please provide a 'trust factor' - range 1-5 (1= low trust factor 5= highest):</p> <ul style="list-style-type: none"> - National news services - International news sources - Government information sources - CERT vulnerability & threat advisories - Anti-virus / commercial vendors - Social media e.g via Twitter, Facebook, google+.... - Academic papers / conference proceedings - Web articles - Others (please state) 	5	

SURVEY #1 WHOLE TO POLAND COMPARISON



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

Survey 1		Survey 1 - English		Survey 1 - Polish																																	
#	Questions																																				
1	In which country do you currently reside?	respondents from 42 countries (890)		respondents 97% from Poland (359)																																	
2	What is your age?	18 to 24 25 to 34 35 to 54 55 to 64 65 +	4.6% 31.0% 53.5% 9.0% 1.9%	od 18 do 24 od 25 do 34 od 35 do 54 od 55 do 64 od 65 +	30.7% 42.3% 25.9% 0.9% 0.3%																																
3	Where is the main business of your company located	respondents from 42 countries		respondents 87.3% from Poland																																	
4	How many employees work for your company?	1-5 6-20 21-100 101-500 501-1000 1000+	11.1% 9.3% 16.4% 21.0% 11.8% 30.4%	1-5 6-20 21-100 101-500 501-1000 1000+	21.7% 7.2% 18.7% 16.6% 5.1% 30.7%																																
5	Which category most closely fits your organisation type?	Scholarly research Policy making, Govt, legal or law enforcement Cyber security practitioner, cyber security expert (any Internet service provider or operator Consumer group or end-user Commercial business Other (please specify)	32.3% 10.1% 14.7% 6.0% 1.8% 14.5% 20.7%	uczelnia, instytut badawczy administracja rządu, organy legislacyjne, praktyk lub ekspert bezpieczeństwa komputerowego dostawca Internetu, operator sieci grupa konsumencka, użytkownik końcowy, osoba instytucja komercyjna inne (proszę uszczegółowić)	10.8% 12.5% 8.1% 8.4% 12.8% 35.5% 11.9%																																
Definition of cybercrime																																					
6	For me cybercrime is.....	<p>For me cybercrime is.....</p> <table border="1"> <caption>Data for 'For me cybercrime is.....' chart</caption> <thead> <tr> <th>Category</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>None of these</td> <td>~1.2%</td> </tr> <tr> <td>The use of a computer system(s) to enable traditional form of criminal activity and the use...</td> <td>~2.5%</td> </tr> <tr> <td>Any act against the confidentiality, integrity and availability of computer data and systems</td> <td>~2.6%</td> </tr> <tr> <td>Theft using a computer or Internet</td> <td>~2.2%</td> </tr> <tr> <td>Any criminal act or hacking of computers and networks</td> <td>~2.5%</td> </tr> <tr> <td>Any illegal activity that uses a computer for the storage of evidence</td> <td>~1.8%</td> </tr> <tr> <td>Criminal activity carried out by means of computers or the Internet</td> <td>~2.5%</td> </tr> </tbody> </table>		Category	Percentage	None of these	~1.2%	The use of a computer system(s) to enable traditional form of criminal activity and the use...	~2.5%	Any act against the confidentiality, integrity and availability of computer data and systems	~2.6%	Theft using a computer or Internet	~2.2%	Any criminal act or hacking of computers and networks	~2.5%	Any illegal activity that uses a computer for the storage of evidence	~1.8%	Criminal activity carried out by means of computers or the Internet	~2.5%	<p>Dla mnie cyberprzestępczość to</p> <table border="1"> <caption>Data for 'Dla mnie cyberprzestępczość to' chart</caption> <thead> <tr> <th>Category</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Zadne z powyższych</td> <td>~1.2%</td> </tr> <tr> <td>Użycie komputera/systemów komputerowych do tradycyjnych form przestępczości i użycie...</td> <td>~2.5%</td> </tr> <tr> <td>Każda działalność przeciwko poufności, integralności, dostępności danych...</td> <td>~2.6%</td> </tr> <tr> <td>Kradzież z użyciem komputera/Internetu</td> <td>~2.2%</td> </tr> <tr> <td>Każda działalność przestępcza związana z włączyaniem się do komputera i sieci</td> <td>~2.5%</td> </tr> <tr> <td>Każda nielegalna działalność której ślady mogą pozostać na komputerze</td> <td>~1.8%</td> </tr> <tr> <td>Działalność przestępczą wykonywaną z a pośrednictwem komputera/Internetu</td> <td>~2.5%</td> </tr> </tbody> </table>		Category	Percentage	Zadne z powyższych	~1.2%	Użycie komputera/systemów komputerowych do tradycyjnych form przestępczości i użycie...	~2.5%	Każda działalność przeciwko poufności, integralności, dostępności danych...	~2.6%	Kradzież z użyciem komputera/Internetu	~2.2%	Każda działalność przestępcza związana z włączyaniem się do komputera i sieci	~2.5%	Każda nielegalna działalność której ślady mogą pozostać na komputerze	~1.8%	Działalność przestępczą wykonywaną z a pośrednictwem komputera/Internetu	~2.5%
Category	Percentage																																				
None of these	~1.2%																																				
The use of a computer system(s) to enable traditional form of criminal activity and the use...	~2.5%																																				
Any act against the confidentiality, integrity and availability of computer data and systems	~2.6%																																				
Theft using a computer or Internet	~2.2%																																				
Any criminal act or hacking of computers and networks	~2.5%																																				
Any illegal activity that uses a computer for the storage of evidence	~1.8%																																				
Criminal activity carried out by means of computers or the Internet	~2.5%																																				
Category	Percentage																																				
Zadne z powyższych	~1.2%																																				
Użycie komputera/systemów komputerowych do tradycyjnych form przestępczości i użycie...	~2.5%																																				
Każda działalność przeciwko poufności, integralności, dostępności danych...	~2.6%																																				
Kradzież z użyciem komputera/Internetu	~2.2%																																				
Każda działalność przestępcza związana z włączyaniem się do komputera i sieci	~2.5%																																				
Każda nielegalna działalność której ślady mogą pozostać na komputerze	~1.8%																																				
Działalność przestępczą wykonywaną z a pośrednictwem komputera/Internetu	~2.5%																																				
Cybercrime concerns																																					
7	Are you concerned about cybercrime?	Extremely concerned Very concerned Moderately concerned Slightly concerned Not at all concerned	24.3% 31.5% 32.1% 8.8% 3.3%	Bardzo mocno Mocno Średnio Tylko trochę W ogóle się nie przejmuję	26.4% 49.5% 17.3% 5.4% 1.4%																																
8	Is cybercrime a concern for your organisation?	Extremely concerned Very concerned Moderately concerned Slightly concerned Not at all concerned	22.3% 27.9% 33.8% 12.8% 3.2%	Bardzo dużym problemem Dużym problemem Średnim problemem Niewielkim problemem W ogóle nie jest problemem	10.5% 22.6% 27.1% 26.7% 13.2%																																

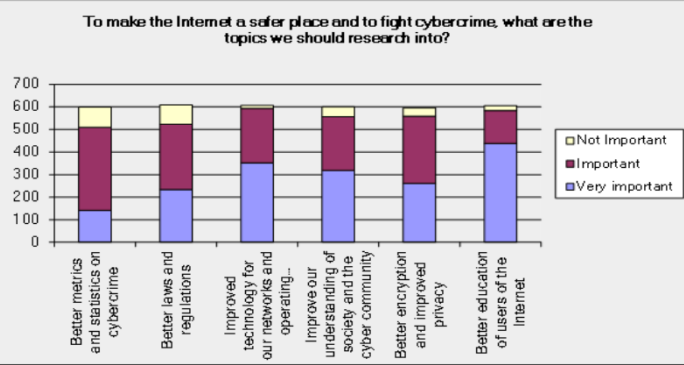
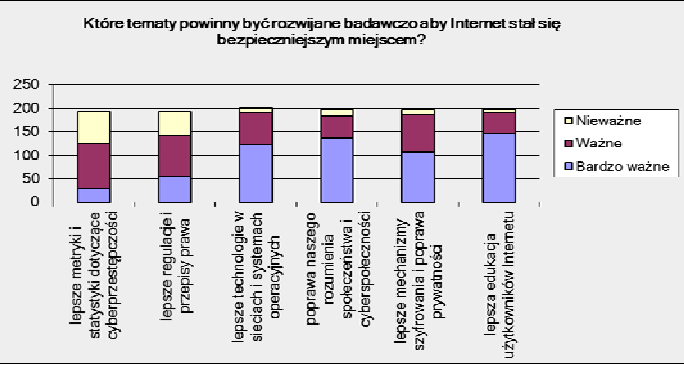
9	Over the next 5 years do you think cybercrime will...?	<table border="1"> <tr> <td>Increase</td> <td>91.5%</td> </tr> <tr> <td>Decrease</td> <td>1.8%</td> </tr> <tr> <td>Stay at the same level</td> <td>6.7%</td> </tr> </table>	Increase	91.5%	Decrease	1.8%	Stay at the same level	6.7%																																
Increase	91.5%																																							
Decrease	1.8%																																							
Stay at the same level	6.7%																																							
What does cybercrime mean to you																																								
10	Do you think cybercrime is...?	<table border="1"> <tr> <td>Here to stay</td> <td>57.5%</td> </tr> <tr> <td>Solvable</td> <td>3.8%</td> </tr> <tr> <td>Containable</td> <td>37.7%</td> </tr> <tr> <td>Not much of an issue</td> <td>1.0%</td> </tr> </table>	Here to stay	57.5%	Solvable	3.8%	Containable	37.7%	Not much of an issue	1.0%																														
Here to stay	57.5%																																							
Solvable	3.8%																																							
Containable	37.7%																																							
Not much of an issue	1.0%																																							
11	Do you see cybercrime as a problem rooted in...?	<p>ii. Do you see cybercrime as a problem rooted in...?</p> <table border="1"> <tr><th>Category</th><th>Value</th></tr> <tr><td>Economic interests</td><td>4.2</td></tr> <tr><td>Political</td><td>3.5</td></tr> <tr><td>Business strategy</td><td>3.3</td></tr> <tr><td>Society</td><td>3.6</td></tr> <tr><td>Education</td><td>3.4</td></tr> <tr><td>Technology</td><td>3.6</td></tr> </table>	Category	Value	Economic interests	4.2	Political	3.5	Business strategy	3.3	Society	3.6	Education	3.4	Technology	3.6																								
Category	Value																																							
Economic interests	4.2																																							
Political	3.5																																							
Business strategy	3.3																																							
Society	3.6																																							
Education	3.4																																							
Technology	3.6																																							
Targets of cybercrime																																								
12	In your organisation, which do you think is most likely to be the target for cybercriminals?	<p>i. In your organisation, which do you think is most likely to be the target for cybercriminals?</p> <table border="1"> <tr><th>Target</th><th>Percentage</th></tr> <tr><td>Critical infrastructures</td><td>40.0%</td></tr> <tr><td>Intellectual Property</td><td>45.0%</td></tr> <tr><td>Personal data</td><td>70.0%</td></tr> <tr><td>Cloud infrastructures</td><td>30.0%</td></tr> <tr><td>Unmanned systems</td><td>5.0%</td></tr> <tr><td>On-Line services/Web</td><td>45.0%</td></tr> <tr><td>Embedded systems</td><td>10.0%</td></tr> <tr><td>Payment systems</td><td>35.0%</td></tr> <tr><td>Banking & financial</td><td>35.0%</td></tr> <tr><td>Logistics & supply chain</td><td>5.0%</td></tr> <tr><td>Mobile devices</td><td>35.0%</td></tr> <tr><td>Critical information</td><td>50.0%</td></tr> <tr><td>People (citizens)</td><td>15.0%</td></tr> <tr><td>People (employees)</td><td>35.0%</td></tr> <tr><td>Workstations (Users)</td><td>40.0%</td></tr> <tr><td>Communications with</td><td>10.0%</td></tr> <tr><td>Transport assets</td><td>5.0%</td></tr> <tr><td>Business or personal</td><td>35.0%</td></tr> </table>	Target	Percentage	Critical infrastructures	40.0%	Intellectual Property	45.0%	Personal data	70.0%	Cloud infrastructures	30.0%	Unmanned systems	5.0%	On-Line services/Web	45.0%	Embedded systems	10.0%	Payment systems	35.0%	Banking & financial	35.0%	Logistics & supply chain	5.0%	Mobile devices	35.0%	Critical information	50.0%	People (citizens)	15.0%	People (employees)	35.0%	Workstations (Users)	40.0%	Communications with	10.0%	Transport assets	5.0%	Business or personal	35.0%
Target	Percentage																																							
Critical infrastructures	40.0%																																							
Intellectual Property	45.0%																																							
Personal data	70.0%																																							
Cloud infrastructures	30.0%																																							
Unmanned systems	5.0%																																							
On-Line services/Web	45.0%																																							
Embedded systems	10.0%																																							
Payment systems	35.0%																																							
Banking & financial	35.0%																																							
Logistics & supply chain	5.0%																																							
Mobile devices	35.0%																																							
Critical information	50.0%																																							
People (citizens)	15.0%																																							
People (employees)	35.0%																																							
Workstations (Users)	40.0%																																							
Communications with	10.0%																																							
Transport assets	5.0%																																							
Business or personal	35.0%																																							
What risks are you exposed to																																								
13	Does your organisation (or do you) apply risk management as part of a cyber security strategy?	<table border="1"> <tr> <td>Yes</td> <td>54.0%</td> </tr> <tr> <td>No</td> <td>20.7%</td> </tr> <tr> <td>Don't know</td> <td>25.3%</td> </tr> </table>	Yes	54.0%	No	20.7%	Don't know	25.3%																																
Yes	54.0%																																							
No	20.7%																																							
Don't know	25.3%																																							
14	Does someone in the company (or do you) formally and regularly keep up-to-date with cybercrime related news via...?	<table border="1"> <tr> <td>Generic newspapers and news broadcaster</td> <td>17.2%</td> </tr> <tr> <td>Specialized news sources</td> <td>46.1%</td> </tr> <tr> <td>Consulting companies</td> <td>5.2%</td> </tr> <tr> <td>Activities outsourced to external company/ies</td> <td>5.6%</td> </tr> <tr> <td>Social network contacts</td> <td>7.9%</td> </tr> <tr> <td>No time allocated to do this</td> <td>18.0%</td> </tr> </table>	Generic newspapers and news broadcaster	17.2%	Specialized news sources	46.1%	Consulting companies	5.2%	Activities outsourced to external company/ies	5.6%	Social network contacts	7.9%	No time allocated to do this	18.0%																										
Generic newspapers and news broadcaster	17.2%																																							
Specialized news sources	46.1%																																							
Consulting companies	5.2%																																							
Activities outsourced to external company/ies	5.6%																																							
Social network contacts	7.9%																																							
No time allocated to do this	18.0%																																							

Zwiększy się	95.6%																																						
Zmniejszy się	0.4%																																						
Pozostanie na tym samym poziomie	4.0%																																						
jest zjawiskiem, które zawsze będzie obecne 75.0%																																							
jest problemem, który zostanie rozwiązany 0.8%																																							
jest problemem, który można ograniczyć 24.2%																																							
nie jest żadnym problemem 0.0%																																							
ii. Czy uważasz, że cyberprzestępczość to problem, którego źródła/przyczyna tkwiąw ...?																																							
<table border="1"> <tr><th>Category</th><th>Value</th></tr> <tr><td>interesach ekonomicznych</td><td>4.0</td></tr> <tr><td>polityce</td><td>3.2</td></tr> <tr><td>strategii biznesowej</td><td>3.1</td></tr> <tr><td>społeczeństwie</td><td>3.6</td></tr> <tr><td>edukacji</td><td>3.4</td></tr> <tr><td>technologii</td><td>3.3</td></tr> </table>		Category	Value	interesach ekonomicznych	4.0	polityce	3.2	strategii biznesowej	3.1	społeczeństwie	3.6	edukacji	3.4	technologii	3.3																								
Category	Value																																						
interesach ekonomicznych	4.0																																						
polityce	3.2																																						
strategii biznesowej	3.1																																						
społeczeństwie	3.6																																						
edukacji	3.4																																						
technologii	3.3																																						
Targets of cybercrime																																							
i. Które elementy w Twojej organizacji uważasz za najbardziej prawdopodobny cel dla cyberprzestępców?																																							
<table border="1"> <tr><th>Element</th><th>Percentage</th></tr> <tr><td>krytyczna</td><td>45.0%</td></tr> <tr><td>prawa własności</td><td>30.0%</td></tr> <tr><td>dane osobowe</td><td>70.0%</td></tr> <tr><td>infrastruktura w</td><td>20.0%</td></tr> <tr><td>systemy</td><td>5.0%</td></tr> <tr><td>usługi on-</td><td>45.0%</td></tr> <tr><td>systemy osadzone</td><td>10.0%</td></tr> <tr><td>systemy płatności</td><td>35.0%</td></tr> <tr><td>systemy bankowe</td><td>35.0%</td></tr> <tr><td>logistyka i</td><td>10.0%</td></tr> <tr><td>zarządzania</td><td>35.0%</td></tr> <tr><td>krytyczne</td><td>55.0%</td></tr> <tr><td>ludzie (obywateli)</td><td>15.0%</td></tr> <tr><td>ludzie</td><td>35.0%</td></tr> <tr><td>stacje robocze</td><td>40.0%</td></tr> <tr><td>komunikacja z</td><td>10.0%</td></tr> <tr><td>zasoby</td><td>5.0%</td></tr> <tr><td>reputacja biznesu</td><td>35.0%</td></tr> </table>		Element	Percentage	krytyczna	45.0%	prawa własności	30.0%	dane osobowe	70.0%	infrastruktura w	20.0%	systemy	5.0%	usługi on-	45.0%	systemy osadzone	10.0%	systemy płatności	35.0%	systemy bankowe	35.0%	logistyka i	10.0%	zarządzania	35.0%	krytyczne	55.0%	ludzie (obywateli)	15.0%	ludzie	35.0%	stacje robocze	40.0%	komunikacja z	10.0%	zasoby	5.0%	reputacja biznesu	35.0%
Element	Percentage																																						
krytyczna	45.0%																																						
prawa własności	30.0%																																						
dane osobowe	70.0%																																						
infrastruktura w	20.0%																																						
systemy	5.0%																																						
usługi on-	45.0%																																						
systemy osadzone	10.0%																																						
systemy płatności	35.0%																																						
systemy bankowe	35.0%																																						
logistyka i	10.0%																																						
zarządzania	35.0%																																						
krytyczne	55.0%																																						
ludzie (obywateli)	15.0%																																						
ludzie	35.0%																																						
stacje robocze	40.0%																																						
komunikacja z	10.0%																																						
zasoby	5.0%																																						
reputacja biznesu	35.0%																																						
What risks are you exposed to																																							
<table border="1"> <tr> <td>tak</td> <td>52.9%</td> </tr> <tr> <td>nie</td> <td>25.0%</td> </tr> <tr> <td>nie wiem</td> <td>22.1%</td> </tr> </table>		tak	52.9%	nie	25.0%	nie wiem	22.1%																																
tak	52.9%																																						
nie	25.0%																																						
nie wiem	22.1%																																						
<table border="1"> <tr> <td>o ogólnoludzkich gazetach i serwisach informacyjnych</td> <td>20.1%</td> </tr> <tr> <td>specjalistycznych źródeł wiadomości</td> <td>61.9%</td> </tr> <tr> <td>firm konsultingowych</td> <td>1.3%</td> </tr> <tr> <td>czynności prowadzonych przez zewnętrzne firmy w sieci społecznościowych</td> <td>2.5%</td> </tr> <tr> <td>nie alokuje na to czasu</td> <td>7.1%</td> </tr> </table>		o ogólnoludzkich gazetach i serwisach informacyjnych	20.1%	specjalistycznych źródeł wiadomości	61.9%	firm konsultingowych	1.3%	czynności prowadzonych przez zewnętrzne firmy w sieci społecznościowych	2.5%	nie alokuje na to czasu	7.1%																												
o ogólnoludzkich gazetach i serwisach informacyjnych	20.1%																																						
specjalistycznych źródeł wiadomości	61.9%																																						
firm konsultingowych	1.3%																																						
czynności prowadzonych przez zewnętrzne firmy w sieci społecznościowych	2.5%																																						
nie alokuje na to czasu	7.1%																																						

15	How often are staff given training about cyber security risks?	Weekly 5.6% Monthly 8.5% Yearly 22.7% Never 16.5% Only if there is a problem 25.6% Don't know 21.1%	co tydzień 3.4% co miesiąc 3.4% co rok 20.1% nigdy 24.8% tylko wtedy, gdy wystąpi problem 23.5% nie wiem 24.8%																
16	Does your organisation allow the use of Bring Your Own Devices (BYOD)?	Yes 65.6% No 34.4%	tak 54.3% nie 45.7%																
17	Does your organisation have a best practices policy for BYOD?	Yes 28.3% No 41.6% Don't know 30.2%	tak 34.5% nie 51.1% nie wiem 14.5%																
The effects of cybercrime																			
18	Have you experienced a cybercriminal action in the last 5 years in a...?	<p>i. Have you experienced a cybercriminal action in the last 5 years in a...?</p> <table border="1"> <tr><th>Category</th><th>Percentage</th></tr> <tr><td>Personal capacity</td><td>27.0%</td></tr> <tr><td>Through work</td><td>43.0%</td></tr> <tr><td>Never</td><td>43.0%</td></tr> </table>	Category	Percentage	Personal capacity	27.0%	Through work	43.0%	Never	43.0%	<p>i. Czy doświadczyłeś/doświadczyłaś działań cyberprzestępczych w ciągu ostatnich 5 lat...?</p> <table border="1"> <tr><th>Category</th><th>Percentage</th></tr> <tr><td>w życiu osobistym</td><td>43.0%</td></tr> <tr><td>w pracy</td><td>48.0%</td></tr> <tr><td>nigdy</td><td>30.0%</td></tr> </table>	Category	Percentage	w życiu osobistym	43.0%	w pracy	48.0%	nigdy	30.0%
Category	Percentage																		
Personal capacity	27.0%																		
Through work	43.0%																		
Never	43.0%																		
Category	Percentage																		
w życiu osobistym	43.0%																		
w pracy	48.0%																		
nigdy	30.0%																		
19	If you have been a victim of cybercrime in the last 5 years, what was the effect of the action?	Loss of money 14.1% Down time 29.8% Inconvenience 46.8% Psychologically harmful 10.5% Loss of reputation 10.5% No effect 33.3%	strata pieniędzy 13.8% wstrzymanie pracy 20.5% niedogodność 41.0% obciążenie psychiczne 22.6% utrata dobrego imienia 10.8% zaden 42.6%																
20	As a direct result of a cybercriminal attack or threat, did you/your work make any changes to the cyber security strategy?	Yes 44.7% No 12.4% Don't know 15.7% N/A 27.2%	tak 34.7% nie 19.2% nie wiem 13.2% nie dotyczy 32.9%																
21	If you have experienced a cyber attack, do you think it posed a systemic risk to you or your organisation?	Yes 41.0% No 28.9% Don't know 30.1%	tak 53.3% nie 21.6% nie wiem 25.1%																

22	If you have been a victim of cybercrime, what action followed?	Reported to the police with no further action 8.1%	zgłoszono sprawę na policję, ale nic się później nie 8.2%
		Reported to the police, who contacted me /my 6.3%	zgłoszono sprawę na policję, która skontaktowała 3.5%
		Reported to the police, who followed it through but no 8.8%	zgłoszono sprawę na policję, która poprowadził a ją, 14.0%
		Reported to the police, who followed it through to 7.2%	zgłoszono sprawę na policję, która poprowadził a ją 5.3%
		Not reported to police 36.6%	nie zgłoszono sprawy na policję 35.1%
		Didn't know how to report to the police 5.8%	nie wiedział em/wiedział am jak zgłosić sprawę na 4.7%
		Other 27.3%	inne 29.2%
23	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 8.7%	zgłoszono sprawę do rządowego lub narodowego 7.7%
		Reported to national or government CERT, with action 10.9%	zgłoszono sprawę do rządowego lub narodowego 7.7%
		Did not contact CERT but I know the police did 6.2%	nie zgłoszono sprawy do CERT, ale wiem, że policja 3.2%
		Did not contact my national or government CERT 28.6%	nie zgłoszono sprawy do CERT ponieważ uznano to 30.3%
		Did not know I could report to a CERT 16.9%	nie wiedział em/wiedział am że mogę zgłosić sprawę 40.6%
		Do not know what a CERT is or how to contact them 28.6%	nie wiem, czym jest CERT i jak się z nim skontaktować 10.3%
Security management			
24	Which of the following security applications do you use on your own computing devices?	Firewalls 85.3%	fire walle 88.5%
		Antivirus 86.8%	antywirusy 90.0%
		Vulnerability scanning 34.4%	skanery podatności 29.7%
		Spam blocker/secure email gateway 62.7%	blokady i filtry spamu 67.5%
		Data encryption 51.1%	szyfrowanie danych 68.4%
		Early warning system 8.9%	systemy wczesnego ostrzegania 12.9%
		VOIP encryption 11.0%	VPN 54.1%
		Password manager 48.2%	szyfrowanie VOIP 7.7%
		VPN 51.0%	menadżer hasel 48.8%
		Hash generator 10.0%	generator hashy 20.6%
		Back-up system (cloud or onsite) 65.8%	system kopi zapasowej (w chmurze lub lokalnie) 64.1%
25	Which of the following security applications does your organisation use?	Firewalls 95.2%	fire walle 95.0%
		Antivirus 93.2%	antywirusy 93.0%
		Vulnerability scanning 53.7%	skanery podatności 42.2%
		Spam blocker/secure email gateway 77.4%	blokady i filtry spamu 69.3%
		Data encryption 54.2%	szyfrowanie danych 63.8%
		Early warning system 19.1%	systemy wczesnego ostrzegania 24.6%
		VOIP encryption 16.8%	szyfrowanie VOIP 15.6%
		Password manager 41.9%	menadżer hasel 30.2%
		Hash generator 12.3%	generator hashy 18.6%
		VPN Dedicated resources 60.1%	dedykowane zasoby VPN 55.8%
		SIEM (Security information and event management) 24.3%	SIEM (Security information and event management) 22.1%
		Back-up system (cloud or onsite) 66.4%	system kopi zapasowej (w chmurze lub lokalnie) 68.3%
		IDS/IPS solution 36.3%	systemy IDS/IPS (wykrywanie intruzów) 45.7%
		DLP solution 10.6%	systemy DLP (o chrona przed wyciekiem danych) 19.1%
		Other (please specify) 4.2%	inne -jakie? 4.5%
26	How is your own/your organisation's cyber security managed?	In-house by someone who is in charge of (security) 50.8%	wewnetrznie, przez osoby odpowiedzialne za polityki 55.6%
		In-house CERT 12.5%	własny CERT 10.2%
		I manage my own cyber security 11.9%	sam/sama zarządzam cyberbezpieczeństwem 16.1%
		Outsourced to a independent specialist or 4.7%	przez outsourcing do niezależnego specjalisty lub 2.0%
		By the Internet Service Provider 1.9%	przez dostawcę Internetu (ISP) 2.9%
		Don't know 18.2%	nie wiem 13.2%

27	Do you, or does someone else in your organisation, share information about cyber events/attacks with an outside organisation?	Yes No Don't know	35.4% 24.8% 39.8%	tak nie nie wiem	21.1% 45.6% 33.3%
28	Do you/your organisation hold any Information Security Management certificates, e.g., ISO 27001?	Yes No Don't know	21.4% 33.2% 45.4%	tak nie nie wiem	22.1% 43.1% 34.8%
29	Do you/your organisation use the following security testing techniques?	Penetration testing Vulnerability testing Audits Other Don't know	16.1% 11.8% 16.4% 5.0% 50.7%	testy penetracyjne testy podatności audyty inne nie wiem	21.7% 5.6% 26.8% 6.6% 39.4%
Economic impact					
30	Currency	US\$ EURO GBP CHF YEN CA\$ AU\$	12.7% 59.4% 3.0% 24.5% 0.2% 0.0% 0.2%	US\$ EURO GBP CHF YEN CA\$ AU\$	17.1% 81.8% 1.1% 0.0% 0.0% 0.0% 0.0%
31	How much do you personally spend annually on cyber security, e.g. anti-virus, anti-spam, upgrades, etc.?	0 1-100 101 -250 250+	47.0% 33.7% 8.7% 10.6%	0 1-100 101 -250 250+	52.3% 35.7% 9.0% 3.0%
32	How much does your organisation spend annually on cyber security products?	0 1-100 101 -500 501 - 1,000 1,000 - 10,000 10,000+	7.4% 6.8% 9.2% 10.2% 26.2% 40.2%	0 1-100 101 -500 501 - 1,000 1,000 - 10,000 10,000+	15.9% 8.5% 11.4% 9.1% 23.9% 31.3%
33	What do you think is the cost of cybercrime to the economy of your country of residence per annum?	Up to 25million 26m- 100m 100 million+ No idea	6.0% 14.9% 23.6% 55.4%	do 25 milionów 26 mln - 100 mln ponad 100 mln nie mam pojęcia	6.6% 18.3% 26.9% 48.2%

34	What do you think is the cost of cybercrime to the world economy?	<table border="1"> <tr> <td>Less than 1billion</td> <td>1.0%</td> </tr> <tr> <td>1bn - 10bn</td> <td>6.8%</td> </tr> <tr> <td>11bn - 25bn</td> <td>6.7%</td> </tr> <tr> <td>26bn - 100bn</td> <td>14.7%</td> </tr> <tr> <td>Over 100 billion</td> <td>15.7%</td> </tr> <tr> <td>No idea</td> <td>55.2%</td> </tr> </table>	Less than 1billion	1.0%	1bn - 10bn	6.8%	11bn - 25bn	6.7%	26bn - 100bn	14.7%	Over 100 billion	15.7%	No idea	55.2%	<table border="1"> <tr> <td>ponizej 1 miliarda</td> <td>1.0%</td> </tr> <tr> <td>1 mld - 10 mld</td> <td>3.5%</td> </tr> <tr> <td>11 mld - 25 mld</td> <td>7.0%</td> </tr> <tr> <td>26 mld - 100 mld</td> <td>11.1%</td> </tr> <tr> <td>ponad 100 mld</td> <td>26.6%</td> </tr> <tr> <td>nie mam pojęcia</td> <td>50.8%</td> </tr> </table>	ponizej 1 miliarda	1.0%	1 mld - 10 mld	3.5%	11 mld - 25 mld	7.0%	26 mld - 100 mld	11.1%	ponad 100 mld	26.6%	nie mam pojęcia	50.8%																																
Less than 1billion	1.0%																																																										
1bn - 10bn	6.8%																																																										
11bn - 25bn	6.7%																																																										
26bn - 100bn	14.7%																																																										
Over 100 billion	15.7%																																																										
No idea	55.2%																																																										
ponizej 1 miliarda	1.0%																																																										
1 mld - 10 mld	3.5%																																																										
11 mld - 25 mld	7.0%																																																										
26 mld - 100 mld	11.1%																																																										
ponad 100 mld	26.6%																																																										
nie mam pojęcia	50.8%																																																										
Research																																																											
35	To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?	<p style="text-align: center;">To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?</p>  <table border="1"> <caption>Approximate data for 'To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?' (Values in counts)</caption> <thead> <tr> <th>Topic</th> <th>Very important</th> <th>Important</th> <th>Not Important</th> </tr> </thead> <tbody> <tr> <td>Better metrics and statistics on cybercrime</td> <td>130</td> <td>370</td> <td>100</td> </tr> <tr> <td>Better laws and regulations</td> <td>230</td> <td>290</td> <td>100</td> </tr> <tr> <td>Improved technology for our networks and our operating...</td> <td>350</td> <td>230</td> <td>100</td> </tr> <tr> <td>Improve our understanding of society and the cyber community</td> <td>300</td> <td>270</td> <td>100</td> </tr> <tr> <td>Better encryption and improved privacy</td> <td>250</td> <td>320</td> <td>100</td> </tr> <tr> <td>Better education of users of the Internet</td> <td>420</td> <td>180</td> <td>100</td> </tr> </tbody> </table>	Topic	Very important	Important	Not Important	Better metrics and statistics on cybercrime	130	370	100	Better laws and regulations	230	290	100	Improved technology for our networks and our operating...	350	230	100	Improve our understanding of society and the cyber community	300	270	100	Better encryption and improved privacy	250	320	100	Better education of users of the Internet	420	180	100	<p style="text-align: center;">Które tematy powinny być rozwijane badawczo aby Internet stał się bezpieczniejszym miejscem?</p>  <table border="1"> <caption>Approximate data for 'Które tematy powinny być rozwijane badawczo aby Internet stał się bezpieczniejszym miejscem?' (Values in counts)</caption> <thead> <tr> <th>Topic</th> <th>Bardzo ważne</th> <th>Ważne</th> <th>Nieważne</th> </tr> </thead> <tbody> <tr> <td>lepsze metryki i statystyki dotyczące cyberprzestępczości</td> <td>30</td> <td>90</td> <td>100</td> </tr> <tr> <td>lepsze regulacje i przepisy prawa</td> <td>50</td> <td>100</td> <td>100</td> </tr> <tr> <td>lepsze technologie w sieciach i systemach operacyjnych</td> <td>120</td> <td>70</td> <td>100</td> </tr> <tr> <td>poprawa naszego rozumienia społeczeństwa i cyberbezpieczeństwa</td> <td>130</td> <td>60</td> <td>100</td> </tr> <tr> <td>lepsze mechanizmy szyfrowania i poprawa prywatności</td> <td>100</td> <td>90</td> <td>100</td> </tr> <tr> <td>lepsza edukacja użytkowników internetu</td> <td>140</td> <td>50</td> <td>100</td> </tr> </tbody> </table>	Topic	Bardzo ważne	Ważne	Nieważne	lepsze metryki i statystyki dotyczące cyberprzestępczości	30	90	100	lepsze regulacje i przepisy prawa	50	100	100	lepsze technologie w sieciach i systemach operacyjnych	120	70	100	poprawa naszego rozumienia społeczeństwa i cyberbezpieczeństwa	130	60	100	lepsze mechanizmy szyfrowania i poprawa prywatności	100	90	100	lepsza edukacja użytkowników internetu	140	50	100
Topic	Very important	Important	Not Important																																																								
Better metrics and statistics on cybercrime	130	370	100																																																								
Better laws and regulations	230	290	100																																																								
Improved technology for our networks and our operating...	350	230	100																																																								
Improve our understanding of society and the cyber community	300	270	100																																																								
Better encryption and improved privacy	250	320	100																																																								
Better education of users of the Internet	420	180	100																																																								
Topic	Bardzo ważne	Ważne	Nieważne																																																								
lepsze metryki i statystyki dotyczące cyberprzestępczości	30	90	100																																																								
lepsze regulacje i przepisy prawa	50	100	100																																																								
lepsze technologie w sieciach i systemach operacyjnych	120	70	100																																																								
poprawa naszego rozumienia społeczeństwa i cyberbezpieczeństwa	130	60	100																																																								
lepsze mechanizmy szyfrowania i poprawa prywatności	100	90	100																																																								
lepsza edukacja użytkowników internetu	140	50	100																																																								
36	Are you willing to participate in another and more advanced survey, to help develop the definitive research roadmap on cybercrime?	<table border="1"> <tr> <td>Yes</td> <td>50.3%</td> </tr> <tr> <td>No</td> <td>49.7%</td> </tr> </table>	Yes	50.3%	No	49.7%	<table border="1"> <tr> <td>tak</td> <td>53.5%</td> </tr> <tr> <td>nie</td> <td>46.5%</td> </tr> </table>	tak	53.5%	nie	46.5%																																																
Yes	50.3%																																																										
No	49.7%																																																										
tak	53.5%																																																										
nie	46.5%																																																										

SEARCHABLE DATABASE (KNOWLEDGE BASE)

<http://cyberroad.eu/bibliography/>

THE CURRENT LANDSCAPE



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

BIBLIOGRAPHY

Acquisti, A., Taylor, C. & Wagman, L., 2015. The Economics of Privacy. *Journal of Economic Literature*, Issue March 18.

Akamai Technologies, Inc, 2015. *Akamai PLXsert's Q4 2014 State of the Internet – Security Report Released*. [Online] Available at: <http://www.akamai.com/html/about/press/releases/2015/press-012915.html> [Accessed May 2015].

Akamai, 2014. *Real-time Web Monitor*. [Online] Available at: <http://www.akamai.com/html/technology/datavizi.html> [Accessed Oct 2014].

Anderson, R. et al., 2013. *Measuring the Cost of Cybercrime*, s.l.: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Armin, J. & Foti, P., 2015. *0-Day Vulnerabilities and Cybercrime Key Players, Markets and Technologies Paper*. s.l., Unpublished paper at: ARES First International Workshop on Future Scenarios for Cyber Crime and Cyber Terrorism.

AV-TEST, 2015. *Malware*. [Online] Available at: <http://www.av-test.org/en/statistics/malware/> [Accessed April 2015].

Barracuda , 2015. *Web Data*. [Online] Available at: <http://www.barracudacentral.org/data/web> [Accessed April 2015].

Barracuda, 2015. *Spam Data*. [Online] Available at: www.barracudacentral.org/data/spam [Accessed April 2015].

BBN (Biuro Bezpieczeństwa Narodowego - National Security Bureau), 2015. *Cyberspace Protection Policy of the Republic of Poland*, s.l.: National Security Bureau.

BSA, 2015. *EU Cybersecurity Maturity Dashboard 2015*. [Online] Available at: http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_poland.pdf [Accessed May 2015].

Burns, S. F., 2005. *Threat Modelling: A Process To Ensure Application Security*. [Online] Available at: <http://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646> [Accessed 18 May 2015].

CERT Polska, 2014. *Raport roczny 2014*. [Online] Available at: http://www.cert.pl/PDF/Raport_CP_2014.pdf [Accessed May 2015].

CERT Polska, n.d. *CERT Polska*. [Online] Available at: http://www.cert.pl/raporty/langswitch_lang/en [Accessed May 2015].

CERT.gov.pl, n.d. *cert.gov.pl - publications*. [Online] Available at: <http://www.cert.gov.pl/cer/publikacje> [Accessed May 2015].



Constantin, L., 2015. *PC World: Researchers show that IoT devices are not designed with security in mind*. [Online] Available at: <http://www.pcworld.com/article/2906952/researchers-show-that-iot-devices-are-not-designed-with-security-in-mind.html> [Accessed May 2015].

Council of Europe, n.d. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. [Online] Available at: <http://conventions.coe.int/Treaty/en/Summaries/Html/189.htm> [Accessed May 2015].

Cybercrime Research Centre, n.d. *Cybercrime Research Centre - Journals & Articles*. [Online] Available at: <http://www.cybercrime.umk.pl/publications,7,en.html> [Accessed <http://www.cybercrime.umk.pl/publications,7,en.html> May 2015].

CyberDefcon, 2015. *Intrusion Attempts vs Peak Attack Traffic - Logarithmic Scale*. s.l.:CyberDefcon.

CyberROAD.eu, 2015. *CERT.PL*. [Online] Available at: http://www.cert.pl/news/9671/langswitch_lang/en [Accessed May 2015].

Dyzurnet, n.d. *Dyzurnet.pl*. [Online] Available at: <http://www.dyzurnet.pl> [Accessed May 2015].

ENISA, 2014. *ENISA Threat Landscape 2014*. [Online] Available at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape#b_start=0 [Accessed May 2015].

Eurobarometer TNS Opinion & Social, 2014. *Eurobarometer Cyber Security Survey*. [Online] Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf [Accessed May 2015].

Freeman, R. E., 1984. *Strategic Management: A stakeholder approach*. Boston: Pitman.

Fundacja Dzieci Niczyje, n.d. *Fundacja Dzieci Niczyje homepage*. [Online] Available at: <http://fdn.pl> [Accessed May 2015].

Global Economic Symposium, 2015. *Solution for Cybercrime, Cybersecurity and the Future of the Internet*. [Online] Available at: http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/solutions/To_tackle_cybercrime_effectively_establish...[Accessed May 2015].

Greenberg, A., 2012. McAfee explains dubious math behind its unscientific 1 trillion data loss claim. *Forbes (online)*, Issue 8th Mar 2012.

Hackett, R., 2015. *Fortune.com (part of Time.com)*. [Online] Available at: <http://fortune.com/2015/04/24/data-breach-cost-estimate-dispute/> [Accessed May 2015].

Hall, A. & Chapman, R., 2002. Correctness by Construction: Developing a Commercial Secure System. *IEEE Software*, Volume 19, pp. 18-25.

Help Net Security, 2015. *Mobile App Developers Are Not Investing in Security*. [Online] [Accessed 18 May 2015].



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

Hsu, C.-C. & Sandford, B. A., 2007. The Delphi Technique: Making Sense Of Consensus. *Practical Assessment, Research & Evaluation*, Aug. Volume 12 (No 10).

IDC, 2014. *IDC Predicts the 3rd Platform Will Bring Innovation, Growth, and Disruption Across All Industries in 2015*. [Online] Available at: <http://www.idc.com/getdoc.jsp?containerId=prUS25285614> [Accessed May 2015].

Jeffray, C., 2014. *The Threat of Cyber-Crime to the UK (Briefing Paper)*, s.l.: s.n.

Kanama, D. M. M. G., 2013. *Development of Technology Foresight: Integration of Technology Roadmapping and the Delphi Method*. s.l.:s.n.

Kosinski, J., 2012. *Research Gate - Cybercrime in Poland 2011-12*. [Online] Available at: http://www.academia.edu/3878063/Cybercrime_in_Poland [Accessed May 2015].

Leblanc, D., 2007. 'DREADful' David LeBlanc's Web Log. [Online] Available at: http://blogs.msdn.com/b/david_leblanc/archive/2007/08/13/dreadful.aspx [Accessed 18 May 2015].

Leblanc, D. & Howard, M., 2002. *Writing Secure Code*. 2nd ed. s.l.:Irwin Professional.

Lee, H. W., 2014. *The Roles of Stakeholders in Cybersecurity*. [Online] Available at: http://www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/101 [Accessed May 2015].

Mateski, M. et al., 2012. *Cyber Threat Metrics (Sandia National Laboratories)*. [Online] Available at: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-065.pdf>

McGraw, G., Viega, J. & IBM, 2000. *Don't wait till a costly security breach*. [Online] Available at: <http://www.ibm.com/developerworks/security/library/s-assurance.html> [Accessed May 2015].

Microsoft Corp, 2014. *Microsoft Security Intelligence Report*, s.l.: s.n.

Ministry of Administration and Digitisation, Polish Internal Security Agency, 2013. *National Cyber Security Strategies in the World, ENISA*. [Online] Available at: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world> [Accessed May 2015].

Mobile Working Group, 2015. *Security Guidance for Early Adopters of the Internet of Things (IoT)*. CSA Cloud Security Alliance, ed, RSA Conference(https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf).

NIST, 2013. *Cybersecurity Framework*. [Online] Available at: <http://www.nist.gov/cyberframework/> [Accessed May 2015].

National Security Bureau, n.d. *Cybersecurity Doctrine of the Republic of Poland 2015*. [Online] Available at: <http://www.bbn.gov.pl/ftp/dok/01/DCB.pdf> [Accessed May 2015].

Norton, 2012. *Norton Cybercrime Report 2012*. [Online] Available at: <http://us.norton.com/cybercrimereport> [Accessed May 2015].



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme

Polish Ministry of the Interior, n.d. *Polish Ministry of the Interior reports on security in Poland*. [Online] Available at: <http://bip.msw.gov.pl/bip/raport-o-stanie-bezpie/18405.Raport-o-stanie-bezpieczenstwa.html> [Accessed May 2015].

Polish Police, n.d. *Polish Police public statistics*. [Online] Available at: <http://www.statystyka.policja.pl/> [Accessed May 2015].

Polish Safer Internet Centre, n.d. *Polish Safer Internet Centre homepage*. [Online] Available at: <http://www.saferinternet.pl> [Accessed May 2015].

Ponemon Institute for Accenture, 2009. *Beyond the Tipping Point*. [Online] Available at: <https://www.ponemon.org> [Accessed May 2015].

Ponemon Institute, 2014. *2014 Global Report on the Cost of Cyber Crime*. [Online] Available at: <http://www.ponemon.org/> [Accessed May 2015].

Ponemon Institute, 2015. [Online] Available at: <http://www.ponemon.org/>

PwC, 2014. *World Economic Crime Survey 2014 (Poland)*. [Online] Available at: http://www.pwc.pl/en/biuroprasowe/assets/pwc_poland_global_economic_crime_survey_2014_presentation.pdf [Accessed May 2015].

Sander, T. & Tschudin, C. F., 1998. Protecting Mobile Agents Against Malicious Hosts. *Lecture Notes in Computer Science*, p. 44–60.

Seiwald, C., 2014. *Winning Strategies: Software Development for the Internet of Things*. [Online] Available at: <http://insights.wired.com/profiles/blogs/winning-strategies-software-development-for-the-internet-of> [Accessed 18 May 2015].

Symantec, 2011. *Norton Cybercrime Report 2011*. s.l.:s.n.

SysSec, 2013. *The Red Book: A Roadmap for Systems Security Research*. D. B. Evangelos Markatos ed. s.l.:s.n.

TNS Opinion & Social (requested by EU Commission), 2015. *Eurobarometer Special Surveys*. [Online] Available at: http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#432 [Accessed May 2015].

UK Govt, 2015. *Cyber Essentials*. [Online] Available at: <https://www.cyberstreetwise.com/cyberessentials/> [Accessed May 2015].

UNODC, 2013. *UNODC Emerging Crimes - Cybercrime Study 2013*. [Online] Available at: <http://www.unodc.org/unodc/search.html?q=cybercrime> [Accessed May 2015].

Verizon, 2015. *2015 DBIR (Data Breach Investigation Report)*. [Online] Available at: <http://fortune.com/2015/04/24/data-breach-cost-estimate-dispute/> [Accessed May 2015].

Wurster, G., van Oorschot, P. C. & Somayaji, A., 2005. A Generic Attack on Checksumming-Based Software Tamper Resistance. *IEEE Symposium on Security and Privacy*.



D5.1 Stakeholder needs and threats evaluation

Funded by the European Commission under the Seventh Framework Programme