2016 - Cybercrime Surveys Report

Authors – Jart Armin & Bryn Thompson (CyberDefcon) & Piotr Kijewski (NASK)

Table of Contents

Acknowledgements

The authors would like to provide grateful thanks to all the many survey participants & respondents who gave up valuable time to complete the surveys, this report is primarily for you. To the European Commission Seventh Framework Programme, that made this possible. APWG, MAAWG, ENISA, and the wider cyber security community. LinkedIn, Survey Monkey, Google, & the CyberROAD team;

UNIVERSITÀ DEGLI STUDI DI CAGLIARI, TECHNISCHE UNIVERSITAET DARMSTADT, INDRA, POSTE ITALIANE, SECURITY MATTERS, VITROCISET, FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS, INOV, DEMOKRITOS, SBA, PROPRS, MINISTÉRIO DA JUSTIÇA (PORTUGAL), CEFRIEL, SUPSI, ROYAL HOLLOWAY, MINISTRY OF NATIONAL DEFENCE, GREECE, MELANI

1 Overview of the Cybercrime Surveys

1.1 Introduction

Partners from academia, industry, computer security, and legal enforcement agencies came together for the CyberROAD project (June 2014 – May 2016) with the aim of developing a cybercrime and cyber terrorism roadmap of the research areas vital to facing forthcoming threats in the lead up to 2020.

This report summarizes the findings from the CyberROAD cybercrime surveys circulated to interested stakeholders across target groups ranging from subject specialists in industry and academia, policy makers, law enforcement, hosting providers and knowledgeable IT users.

In total 2,200 English or Polish speaking stakeholders, in the EU and 20 other countries, responded to the wide-ranging, Delphi-based, survey questions.

The findings provide a snapshot of cybercrime-related, real-life experiences across a diverse landscape of technology-enabled scenarios. Areas of research, that are sometimes overlooked, are explored in this series of surveys through the actual experiences of the participants. These contributing evidences help to form the basis of academic papers and publications presented at the ARES Conference in 2015 '2020 Cybercrime Economic Costs: No Measure No Solution'[1] and a forthcoming Springer publication[2].

The surveys provide an insight into the impact of cybercrime on stakeholders, achieving a major goal of the project, and serve as a primary contributor to the concluding CyberROAD roadmap, i.e. what areas of technological and social research should the EU invest in.

1.2 Methodology

The surveys were designed using specialist online software based on the Delphi method where a series of surveys drawdown to explore previously answered questions at a deeper level. The initial survey was of a generic nature followed by two further surveys divided by the subject matter; Survey 2 – Technical and Organizational; Survey 3 – Social, Economic and Political.

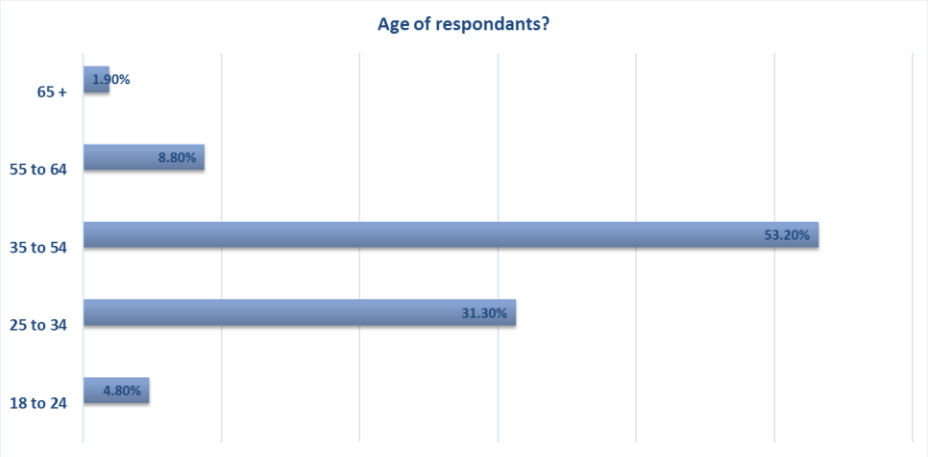
In order to capitalize upon the intended European standpoint of the surveys they were designed to allow for a comparative study between different regions from world to EU and to country specific (macro to micro). Two versions of the surveys were made available: one for English speakers worldwide and the other translated into Polish and aimed at Polish users. Poland was primarily selected as a statistical control group, as the Polish language is primarily spoken only within one country and therefore the results provide a crossmatch of one EU country versus multiple countries to establish any cultural bias or imbalance of survey questions from the results. As the results shown, all Polish results were within 5% of the English language survey results.

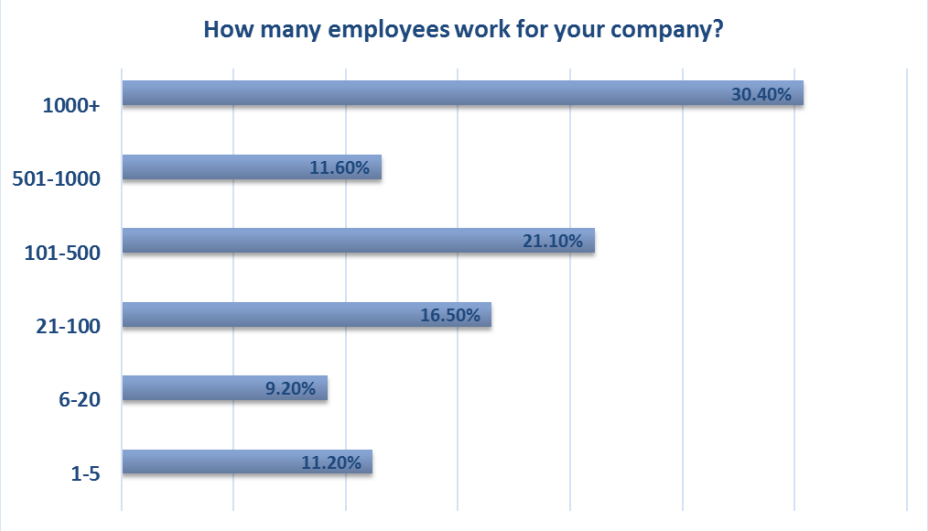
The surveys were distributed in a variety of formats: project website, a dedicated website, announcements via social media, and prompting by email to interested parties.

The breakdown of respondents can be shown as:

[1] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7299982
[2] http://www.springer.com/gb/


Which category most closely fits your organisation type?
Scholarly research
32.10%
Consumer group or end-user
22.30%
Cyber security practitioner
15.00%
Commercial business
14.50%
Policy making, Govt, legal or law enforcement
10.10%
Internet service provider or operator
6.00%

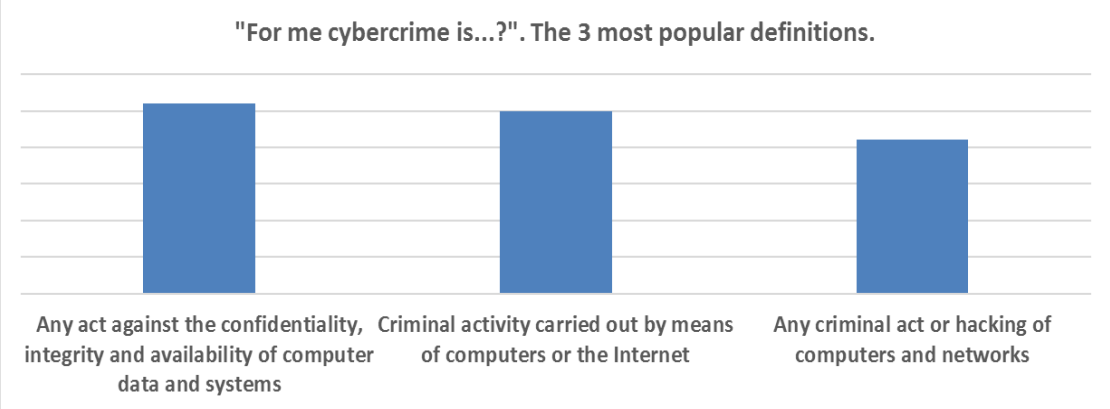

Age of respondants?
65 +
1.90%
55 to 64
8.80%
35 to 54
53.20%
25 to 34
31.30%
18 to 24
4.80%


How many employees work for your company?
1000+
30.40%
501-1000
11.60%
101-500
21.10%
21-100
16.50%
6-20
9.20%
1-5
11.20%

2 Results and Findings

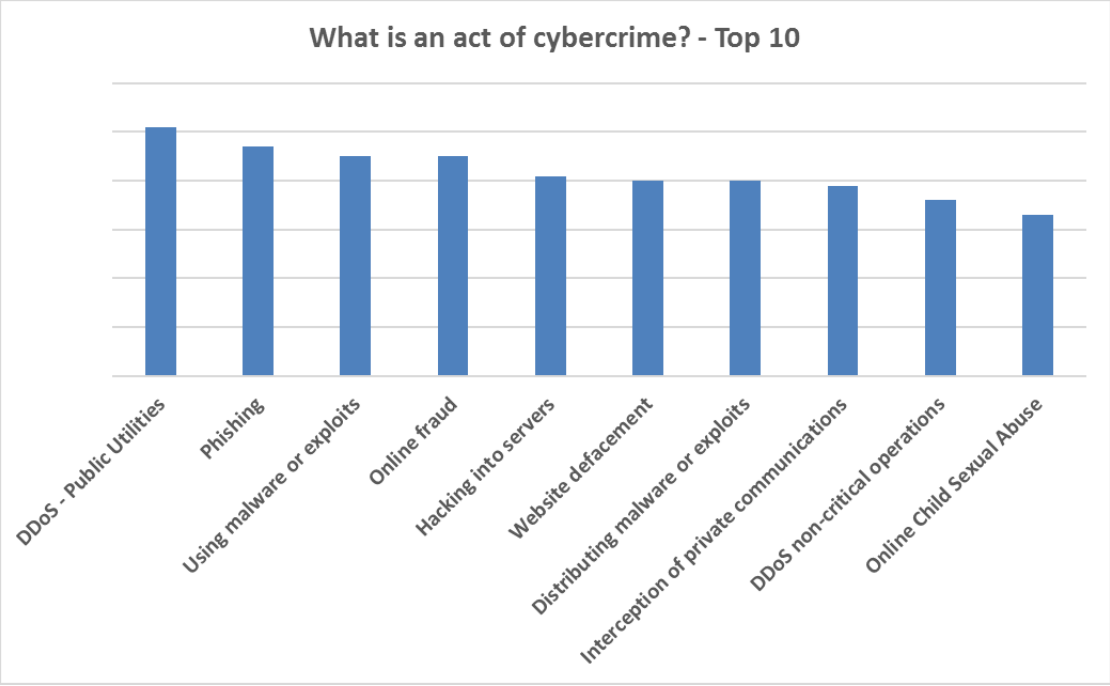
2.1 Definitions of cybercrime

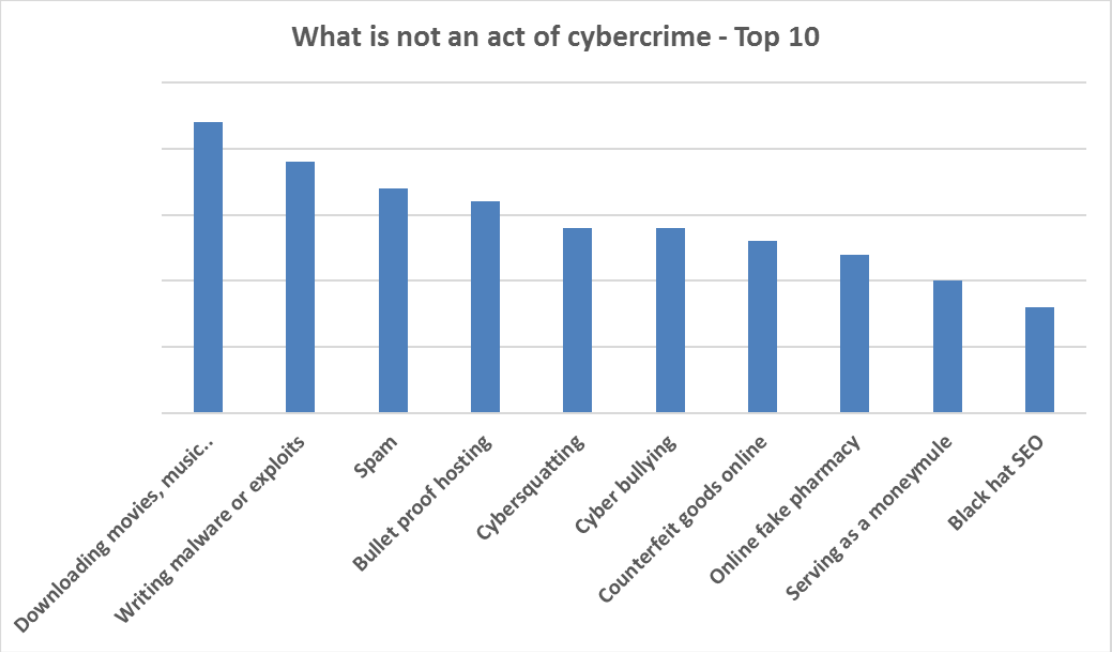
The definition of cybercrime was explored in the surveys. Six choices of definition were provided in Survey 1 asking "For me cybercrime is…?" In Survey 2 participants were asked to select a definition from the three top choices from Survey 1.



2.2 What activities are considered to be cybercrimes?

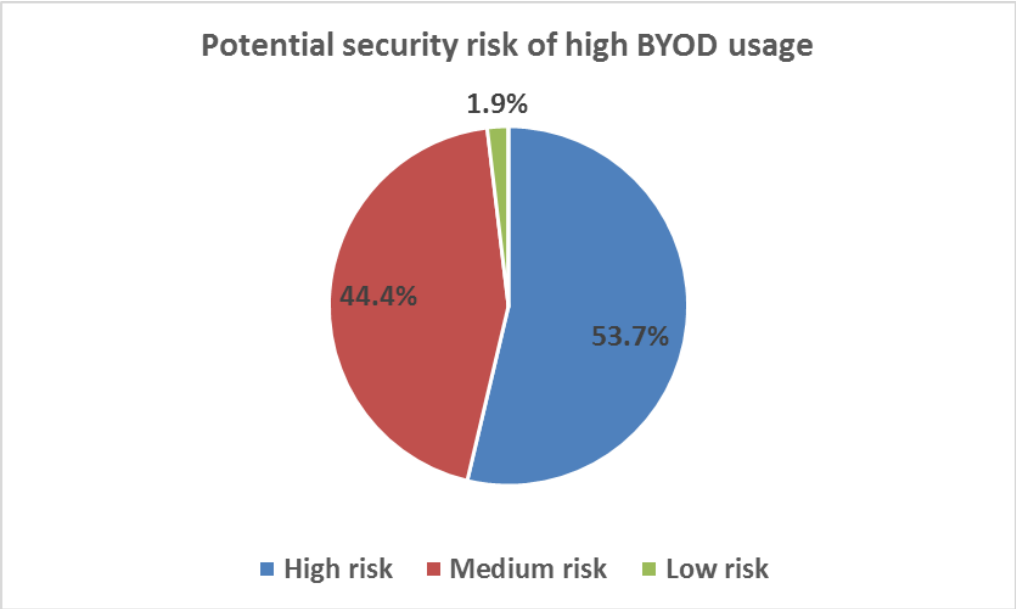
More than 62% of Survey 1 participants said they were either "Extremely Concerned" or "Very Concerned" about cybercrime. Participants expressed what they considered to be a cybercriminal act and what was considered by respondents as 'not' an act of cybercrime in Surveys 2 and 3.



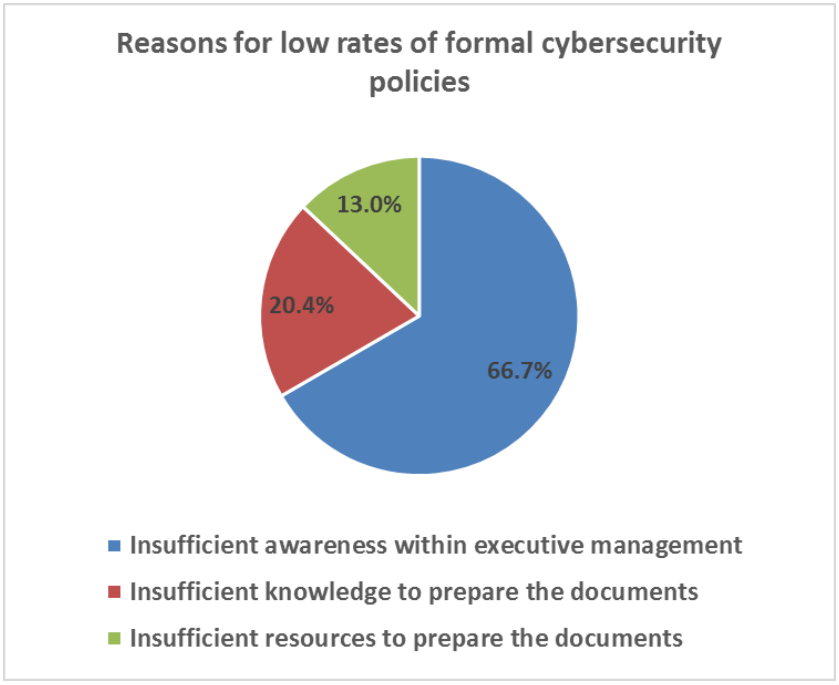


2.3 Best practices and workplace policies

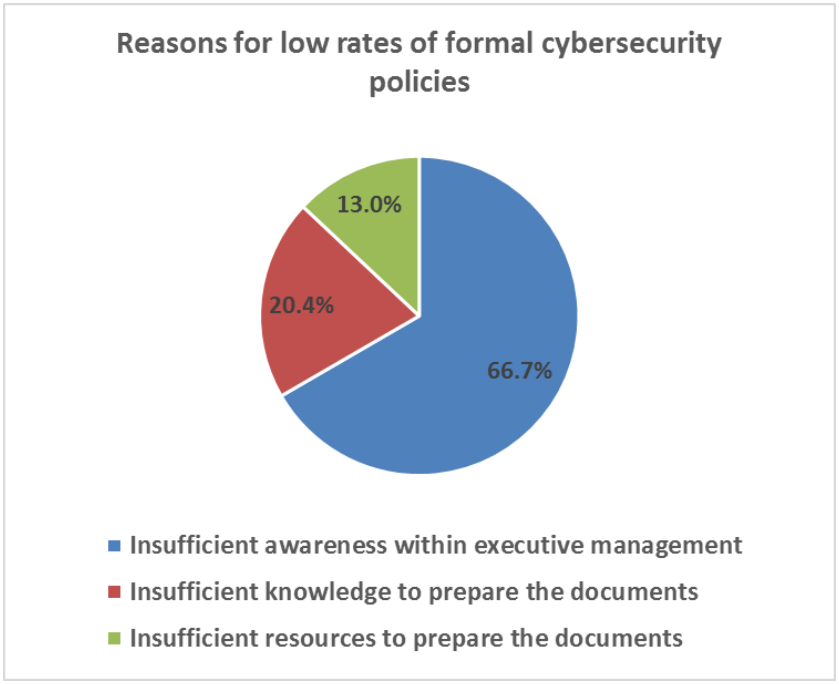
Survey 1 indicated that BYOD rates are high with more than 70% of participants using their own devices within the work-place. Rates for BYOD best practices are not following pace with only 26% these organizations having a BYOD best practices policy in place. Survey 2 participants were asked how highly this discrepancy rated as a potential security risk.

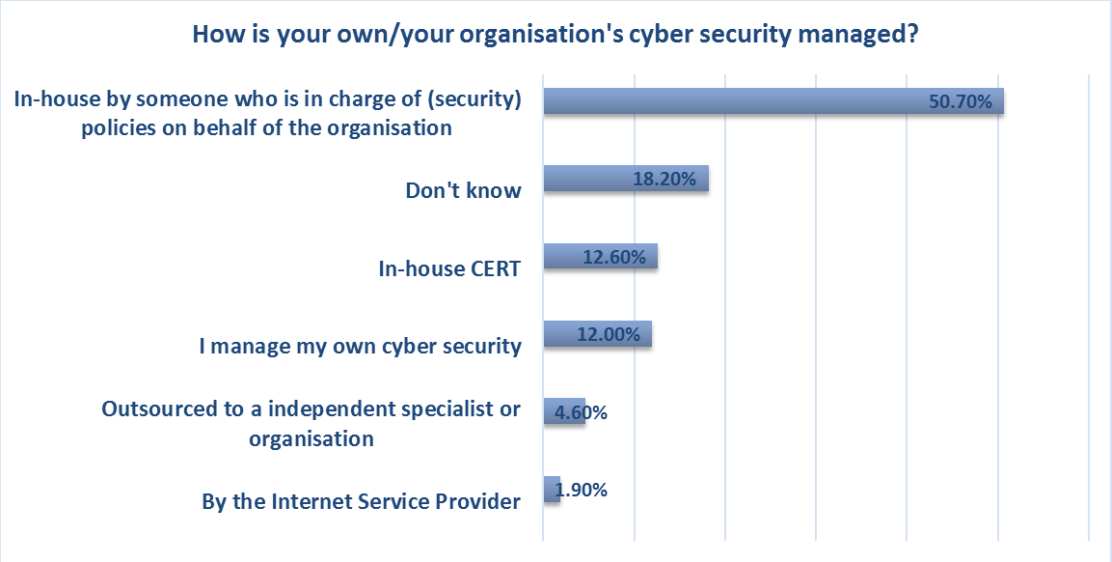


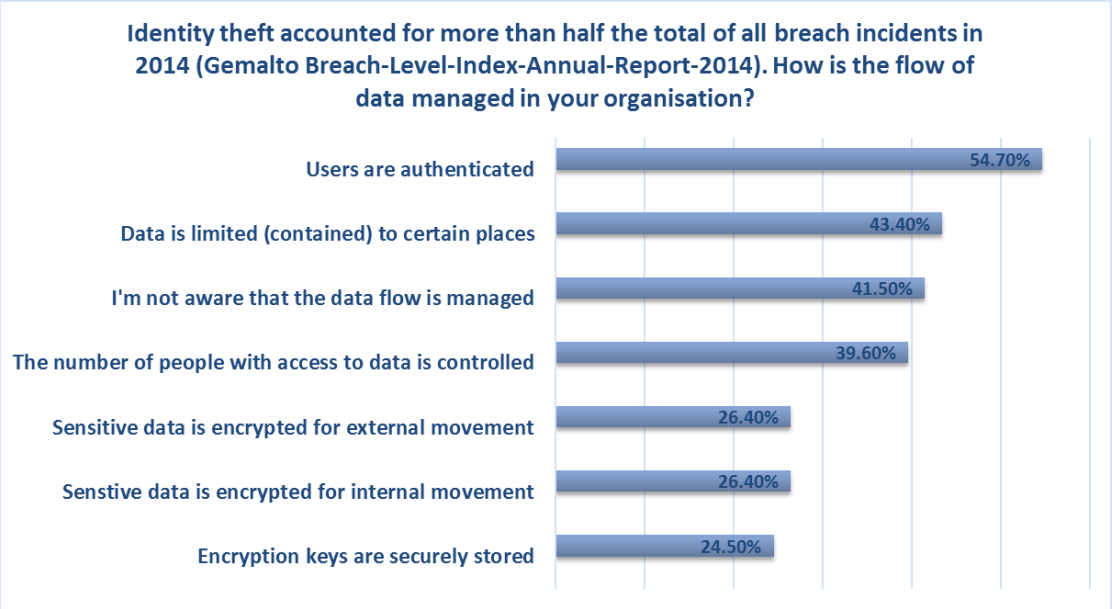
Survey 1 respondents indicated a lack of formal cybersecurity management policies in their place of work. In Survey 2 explored this theme further asking why they thought this was the case.



Participants were asked if there was a clear policy within their work place on how to escalate anything suspicious.

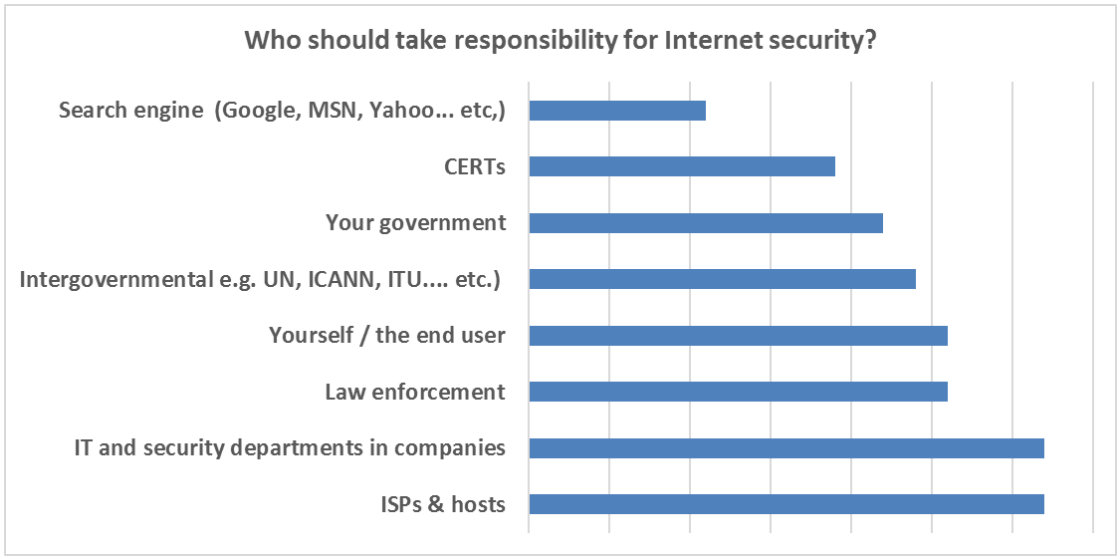



How is your own/your organisation's cyber security managed?
In-house by someone who is in charge of (security) policies on behalf of the organisation
50.70%
Don't know
18.20%
In-house CERT
12.60%
I manage my own cyber security
12.00%
Outsourced to a independent specialist or organisation
4.60%
By the Internet Service Provider
1.90%

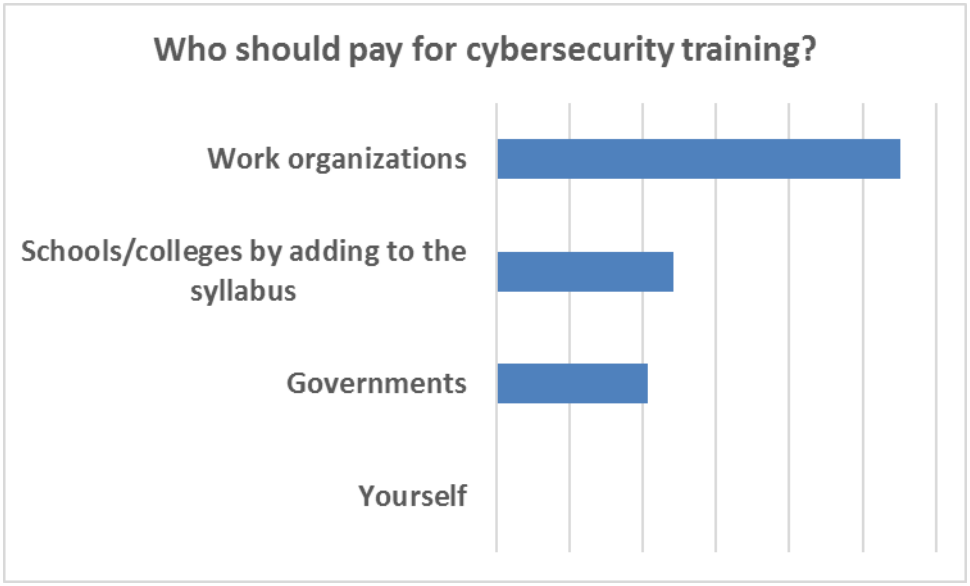

Identity theft accounted for more than half the total of all breach incidents in 2014 (Gemalto Breach-Level-Index-Annual-Report-2014). How is the flow of data managed in your organisation?
Users are authenticated
54.70%
Data is limited (contained) to certain places
43.40%
I'm not aware that the data flow is managed
41.50%
The number of people with access to data is controlled
39.60%
Sensitive data is encrypted for external movement
26.40%
Senstive data is encrypted for internal movement
26.40%
Encryption keys are securely stored
24.50%

2.4 Cyber security responsibility

Respondents were asked how much responsibility they felt for cyber security in their work place. Nearly 69% said they felt a shared responsibility while 31% felt their responsibility was only small.

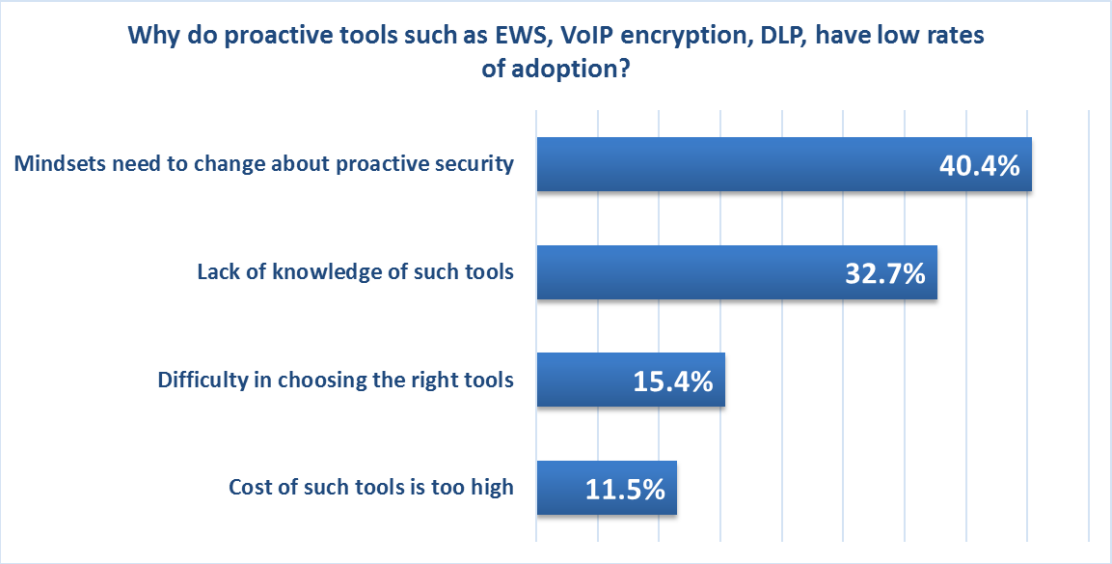


Survey 1 indicated low levels of training on cybersecurity within their workplace. Survey 3 respondents were asked who should be responsible for the cost of training.

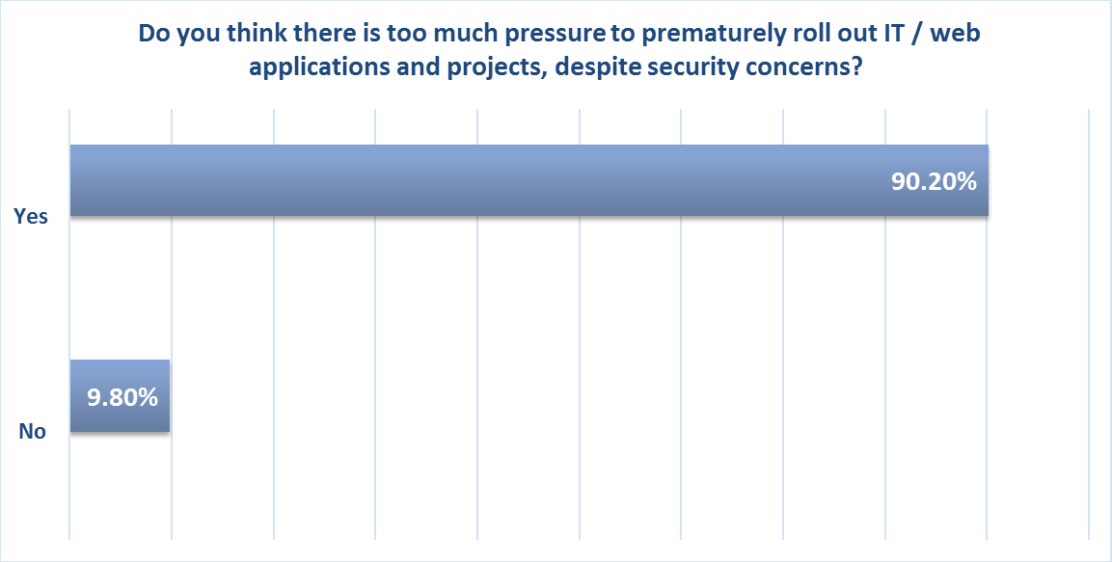


2.5 Security solutions

Survey 1 indicated a reliance on firewalls and antivirus as cyber security solutions while proactive tools such as EWS, VoIP encryption, DLP, have low rates of adoption. Survey 2 respondents were asked why that is the case. The results were:

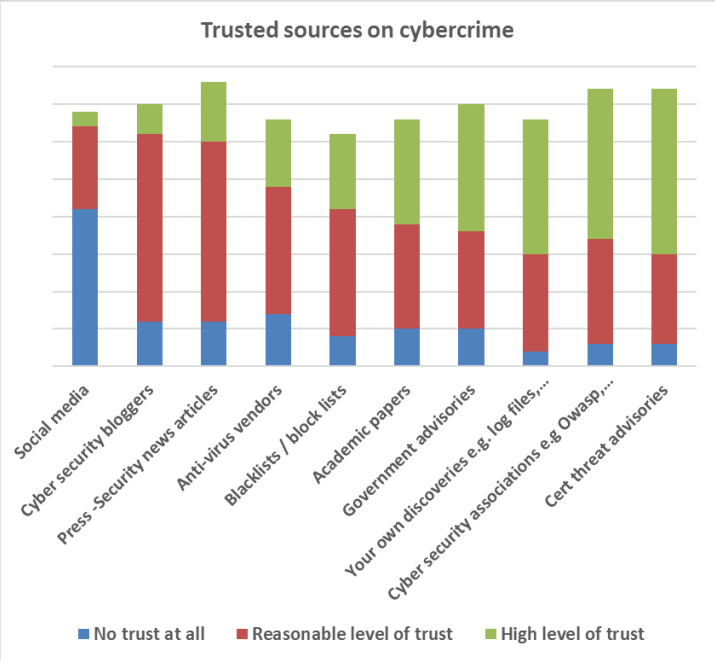


Over 90% of respondents of the more advanced Survey 2 – Technical and Organizational thought there was too much pressure to prematurely roll out IW/web applications and projects.



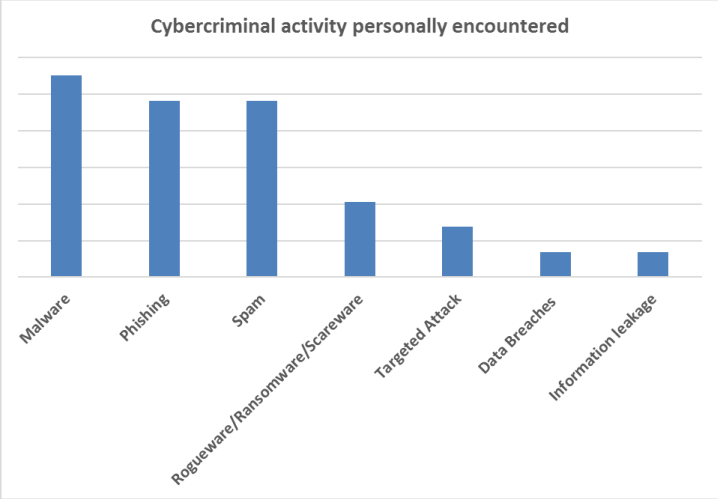
2.6 Sources of data and information on cybercrime

Participants were asked which sources of cybercrime data or information did they trust the most?

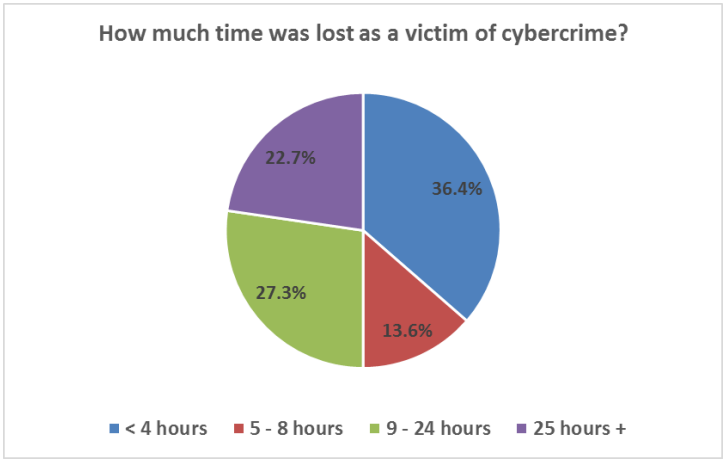


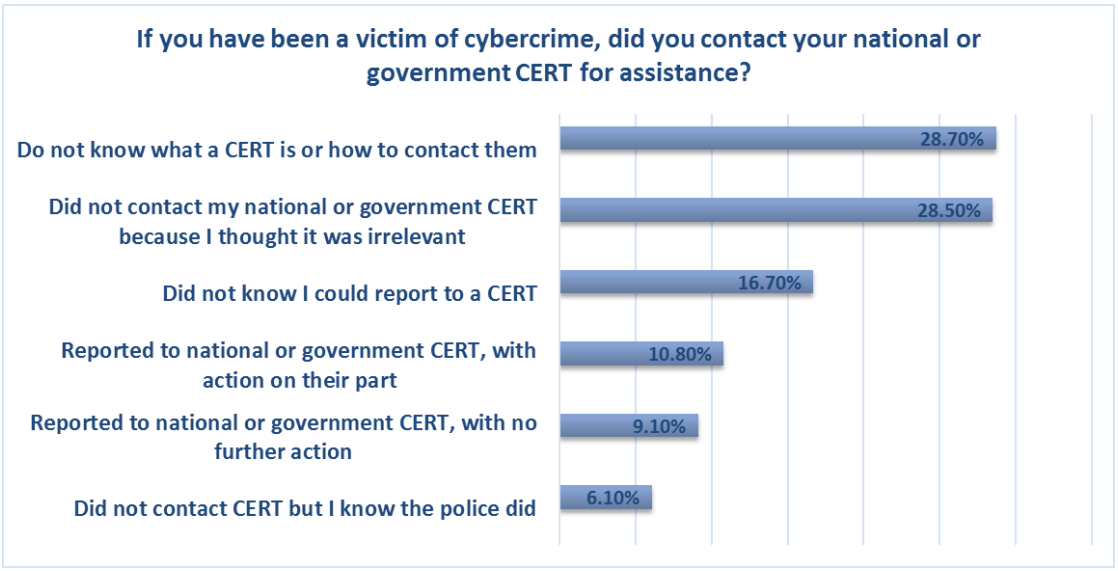
2.7 Personal experiences of cybercrime

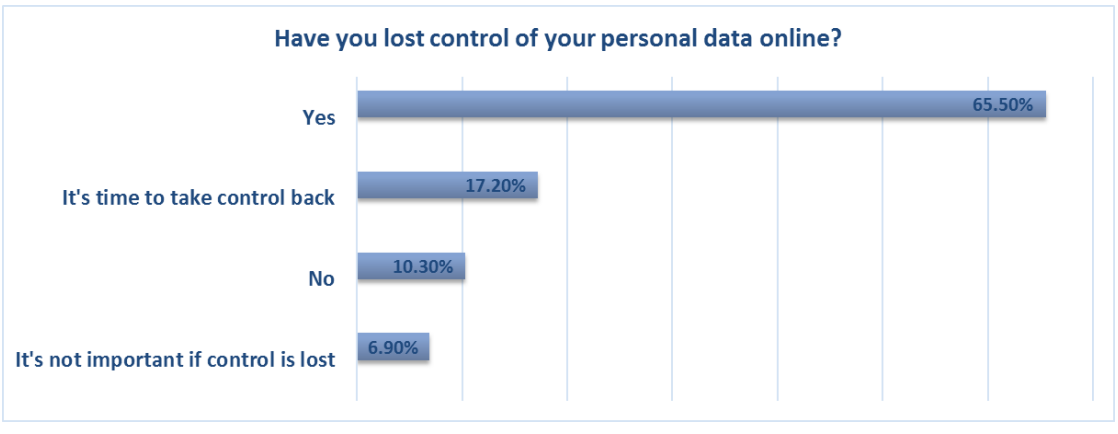
Participants were asked about their own personal experience of cybercriminal activity.



As previous respondents had indicated the two greatest effects of cybercrime had been “down time” and “inconvenience” respondents were asked how much time was lost as a victim to cybercrime.

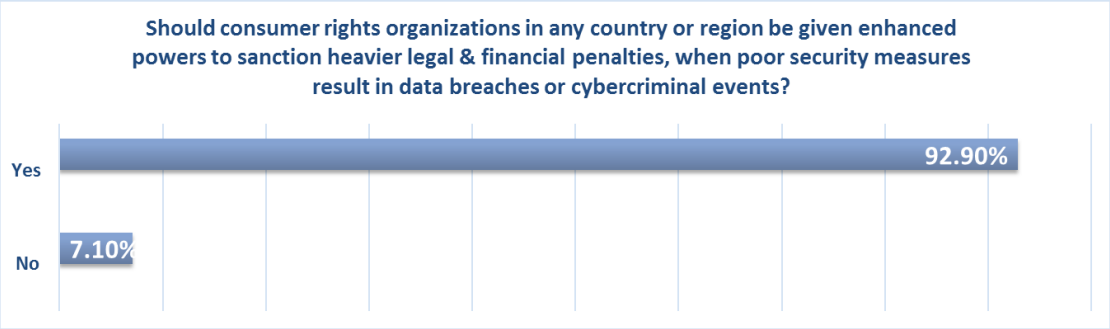

How much time was lost as a victim of cybercrime?
22.7%
36.4%
27.3%
13.6%
< 4 hours
5 - 8 hours
9 - 24 hours
25 hours +


If you have been a victim of cybercrime, did you contact your national or government CERT for assistance?
Do not know what a CERT is or how to contact them
28.70%
Did not contact my national or government CERT because I thought it was irrelevant
28.50%
Did not know I could report to a CERT
16.70%
Reported to national or government CERT, with action on their part
10.80%
Reported to national or government CERT, with no further action
9.10%
Did not contact CERT but I know the police did
6.10%


Have you lost control of your personal data online?
Yes
65.50%
It's time to take control back
17.20%
No
10.30%
It's not important if control is lost
6.90%

2.8 Consumer rights

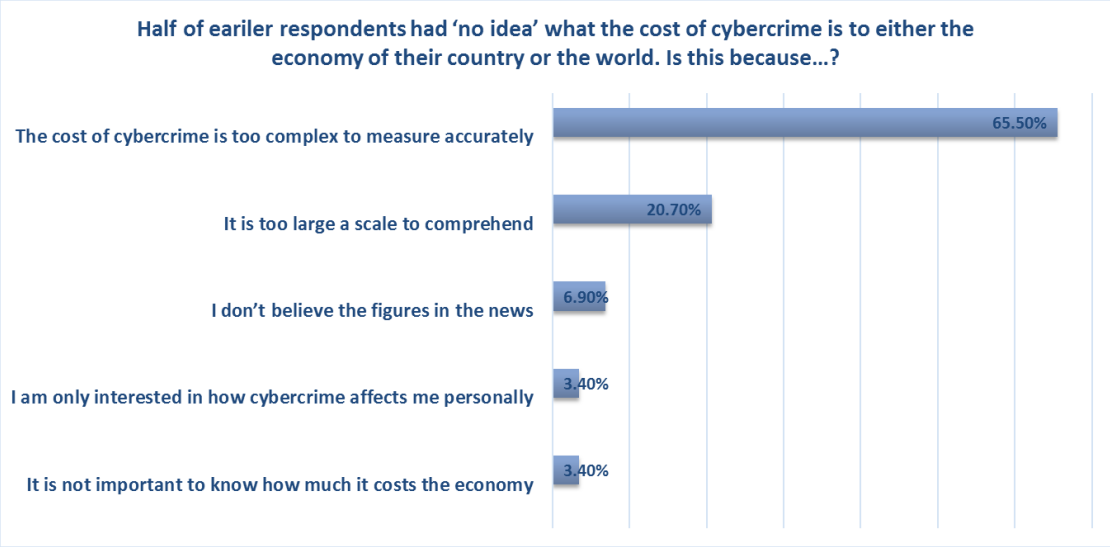
Over 92 % of respondents believe that consumer rights should be strengthened with more sanctions and heavier penalties available to appropriate organizations. Should consumer rights organizations in any country or region (e.g., the European BEUC, Bureau Européen des Unions de Consommateurs, or National 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?

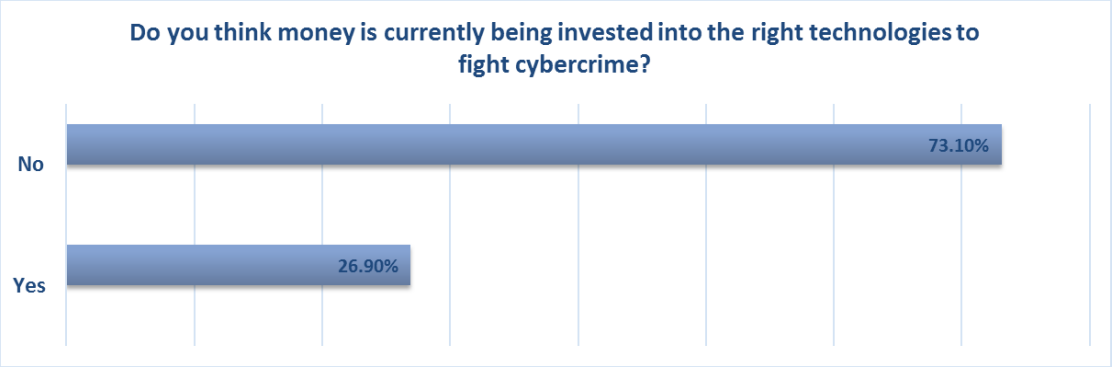


2.9 Cybercrime research – Return on Investment (ROI)

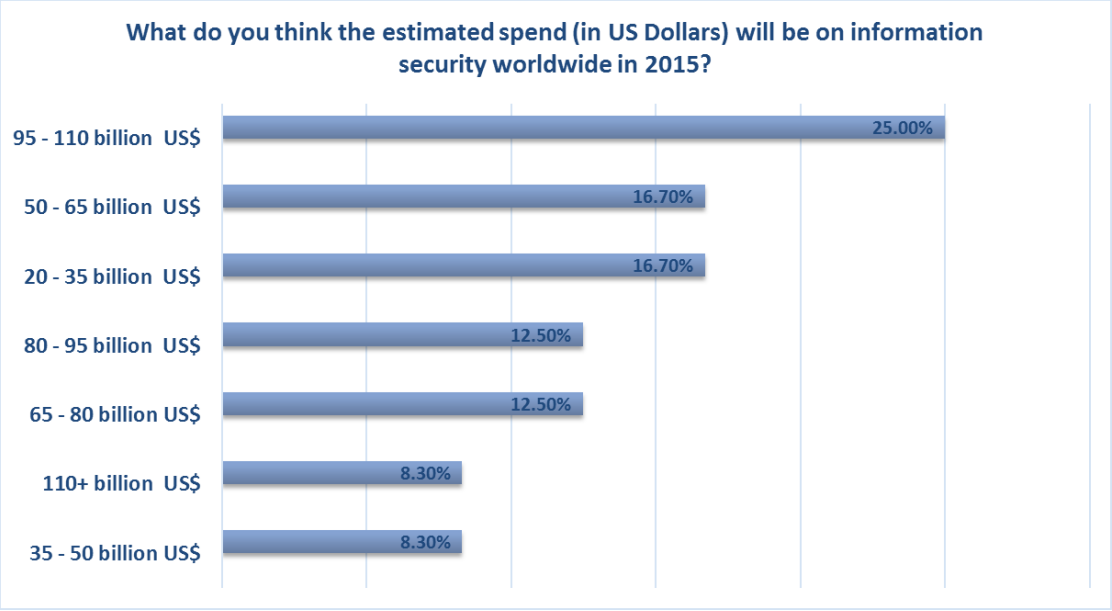
To improve cyber security, Return on Investment. Participants were asked where money should be spent in the future? Results in order of preference:

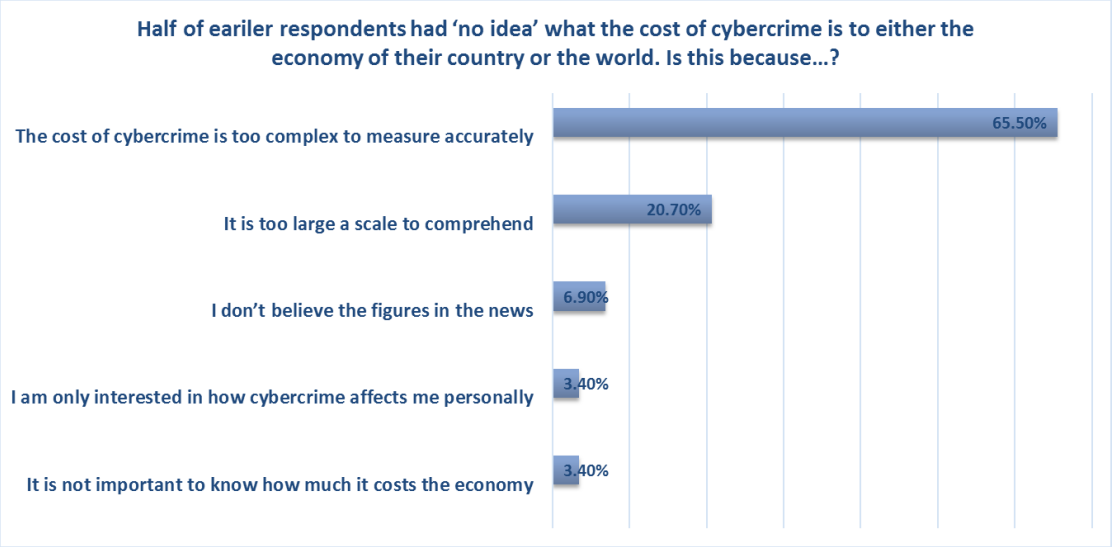
1. Education in cybercrime prevention
2. Cyber security management
3. Laws and policies on cybercrime
4. Risks & effects of cybercrime
5. Economic impact of cybercrime
6. Cybercrime definitions and classifications




Do you think money is currently being invested into the right technologies to fight cybercrime?
No
73.10%
Yes
26.90%


Would you spend more on your online security, if finance were not an issue?
Yes I would spend more if I could
57.10%
Free open source software does not fulfil my organisation's needs
10.70%
Free open source software fulfils my personal security needs
10.70%
Free open source software does not fulfil my personal security needs
7.10%
Free open source software fulfils my organisation's needs
7.10%
No I do not need to spend more
7.10%

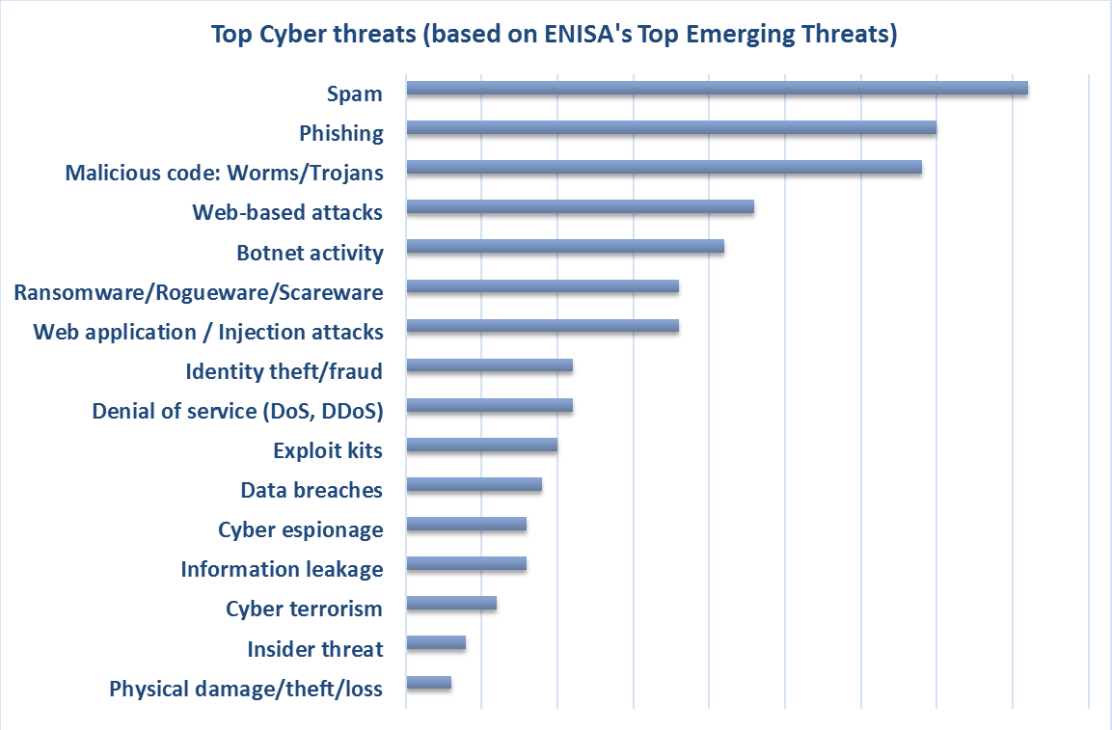

What do you think the estimated spend (in US Dollars) will be on information security worldwide in 2015?
95 - 110 billion US$
25.00%
50 - 65 billion US$
16.70%
20 - 35 billion US$
16.70%
80 - 95 billion US$
12.50%
65 - 80 billion US$
12.50%
110+ billion US$
8.30%
35 - 50 billion US$
8.30%

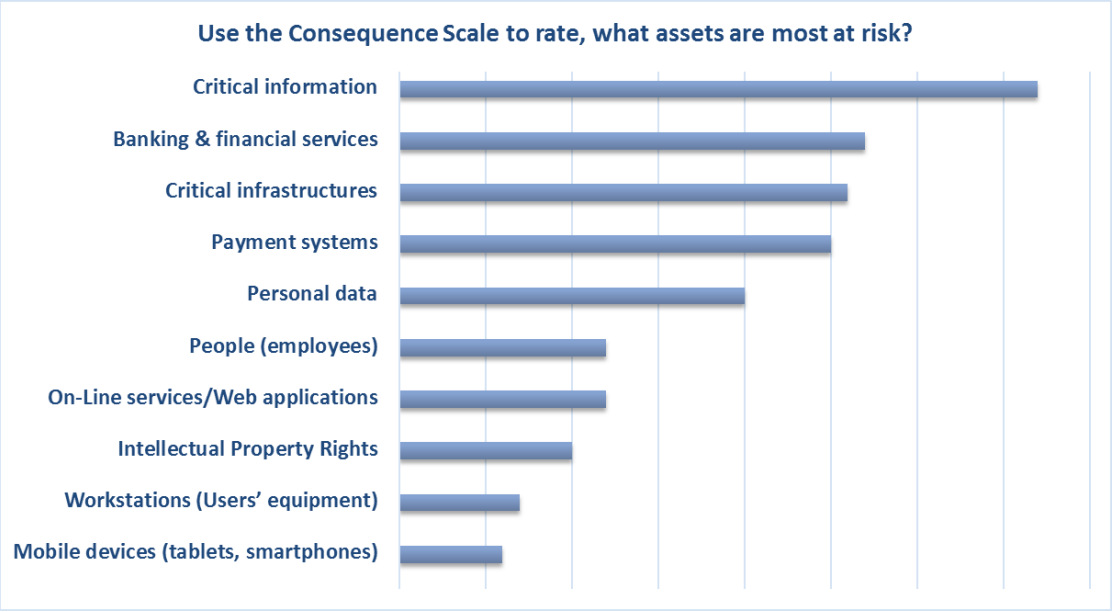


2.10 Information sharing

Results from Survey 1 indicated that sharing of information on cyber incidents is not common practice. Participants were asked why they thought this was the case.

2.11 Cyber Threats





3 Analysis from the stakeholder surveys – What are the research gaps?

3.1 Gap Analysis

Theme	Scenario	Consequences (actual view)	Defense (future view)	Research GAP
Definitions	Perceptions differ on what is an act of cybercrime	No standard definitions; Lack of international agreements; legal sanctions take place within national borders where perceptions may differ	Clear-cut definitions of cybercrime and cross-border co-operation to improve legal sanctions	How to achieve cross-border agreement and internationally agreed sanctions
Best Practices and Workplace Cyber Security Policies	High BYOD usage with low rates of best practice policies	High risk workplace environments	Compliance within the workplace. Effective measures in place.	Policies and best practices for the workplace
Cybersecurity Responsibility	Divided views on where responsibility for cyber security lays.	Ineffective cyber security measures due to inappropriate responsibilities	Responsibility boundaries are clear cut between governments, ISPs, service providers, law enforcement, end users and international organisations.	Cyber security as a shared responsibility. Where/what are the overlaps? Who should pay for cyber security training?
Cybersecurity Solutions	Inappropriate solutions to known cyber security issues	Breaches are not prevented	Proactive and appropriate solutions in place	Proactive security adoption from development to the workplace
Trusted Sources of Data	What sources of data can be trusted in the absence of industry benchmarking?	Lack of trust in data and security information. Inaccurate forecasting for budgets	Industry standards and benchmarking with data provided by trusted sources.	Industry standards and benchmarking. What determines a trusted source for data?

Stakeholder Experiences	Real-life vs assumed scenarios and consequences	Inappropriate solutions providing ineffective measures	Proactive security, fit-for-purpose measures	Fit-for-purpose solutions. Actual consequences of cybercriminal activity.
Consumer Rights	There are few consumer rights in the industry	Entities are not encouraged to raise standards to prevent incidents as the penalties, where they exist, are set too low	Consumer rights have a high profile with stiff penalties for breaches	Industry standards and consumer rights issues
Return on Investment & Economics	Research and development projects are not required to prove their cost-effectiveness.	Inappropriate solutions and ineffective measures as a result of inadequate research and development	R&D will provide appropriate return on investments	Where should research money be spent in the future?
Information Sharing	Stakeholders do not know who to share information with although they understand the value of doing so	Inaccurate collation of data and a barrier to legal action against perpetrators of crime	Incident and event information will be shared with trusted entities followed by appropriate legal action	What makes a trusted entity? How can information sharing be encouraged in a safe environment.

4 Conclusions

Stakeholder responses to the CyberROAD surveys provide a snapshot of personal experiences of cybercriminal activities and cyber security policies within the home and at work. The surveys illustrate the need for changes in perceptions and practices before cyber security solutions can be fully effective. Practices within the workplace fall short of what is desired leaving staff without proper guidance and at high risk to threats. Proper guidelines and processes within a comprehensive cyber security plan improves defenses against attack. More research on how these can be enacted is necessary.

Other problems areas highlighted are a lack of information sharing which limits the ability to collect and collate accurate cyber security data. Stakeholders often do not know where to report incidents or lack trust in the appointed entity. This limits the capacity to take appropriate action which is further hindered by the lack of cross-border cooperation between legal entities.

Industry standards are yet to fully evolve meaning that benchmarking is not commonplace. Consumer rights can be enhanced with appropriate best practices in place.

Reactive security is extensive with inappropriate measures in place that are not fit-for-purpose. Stakeholder experiences indicate that proactive security is not usual with attitudes to newer ideas slow to change.

The surveys highlight that research gaps are widespread and improved ROI could be achieved through funding being targeted in these areas.

WHY CYBER SECURITY RESEARCH MATTERS

Cyber criminal activities are reported to be continuously growing and are negatively impacting the development of the European society and economy, and are pervasively affecting all the aspects of our daily lifes. Even though the level of awareness of cyber threats has increased, and Law Enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. In addition to the economic reasons, however, cyber crime often hides other political and social motivations.

WHAT IS CYBERROAD?

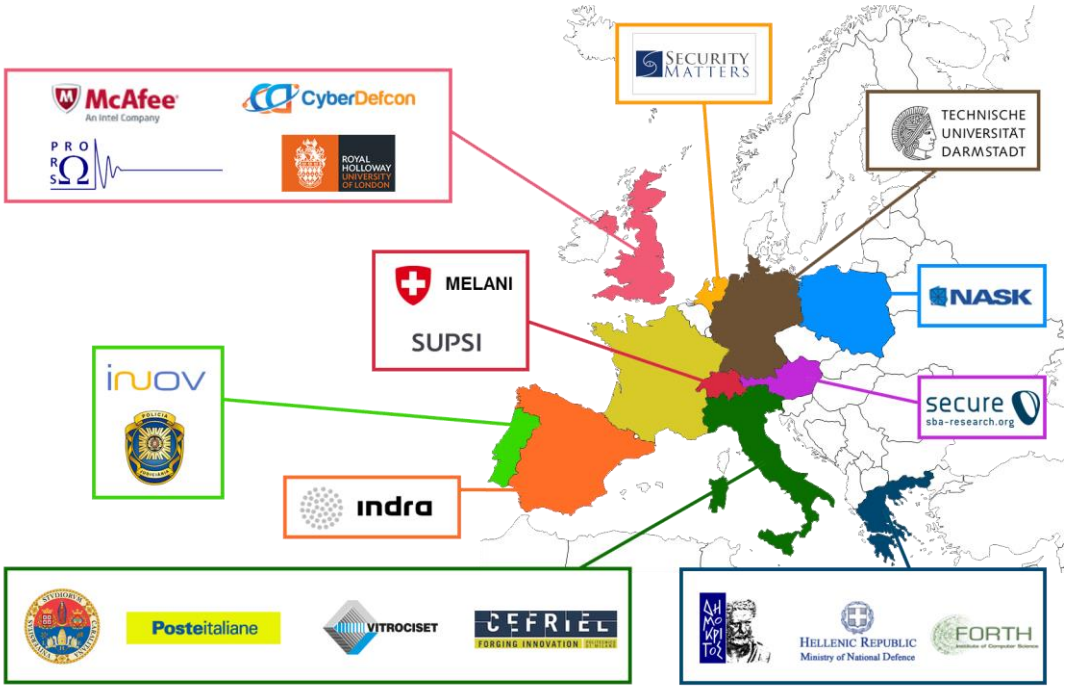
CyberROAD is a 24-month research project funded by the European Commission under the Seventh Framework Programme (with a total budget of 1.300.000 €).
In order to help coordinate the European efforts in the fight against cyber crime and cyber terrorism, the CyberROAD project has identified 19 research topics on which Europe should concentrate resources to increase its security and resilience, organizing them in strategic roadmap for Cyber Security Research.
The roadmap encompasses all the aspects which may contribute to reach this goal, from the development of better and more robust technologies for prevention, detection and mitigation of the attacks, to the legal and forensics aspects concerning the fight against cyber crime and cyber terrorism, up to the need of developing better methods to measure and to analyse the phenomenon and make the citizens more aware of it.
The roadmap is the final outcome of a process of information collection and analysis, during which the existing literature has been deeply analysed, public events and interviews with the relevant stakeholders have been organized in order to grasp the future challenges which our society will be called to face in the forthcoming years.
A ranking methodology has been also applied to the devised research topics which allows to obtain different views of the research roadmap tailored on the needs of the different stakeholders which may be interested in the project outcomes.

WHO PARTICIPATES IN CYBERROAD?

The CyberROAD project has been implemented by a consortium of 20 international partners, involved in the fight against Cyber Crime and Cyber Terrorism. Members include representatives from Academia and Research, Industry, Government and NGOs across Europe:

- PRA Lab, University of Cagliari, Italy (Project coordinator).
- CEFRIEL - Forcing Innovation, Italy.
- CyberDefcon, UK.
- National Centre for Scientific Research “Demokritos”, Greece.
- FORTH - Institute of Computer Science, Greece.
- Governo de Portugal - Ministério da Justiça, Portugal.
- Hellenic Republic - Ministry of National Defence, Greece.
- Indra, Spain.
- INOV - Inesc Inovação, Portugal.
- McAfee, UK.
- MELANI - Reporting and Analysis Centre for Information Assurance, Switzerland.
- NASK, Poland.
- Poste Italiane, Italy.
- PROPRS - Professional Probabilistic Risk Solutions, UK.
- Royal Holloway - University of London, UK.
- SBA Research, Austria.
- Security Matters, Netherlands.
- SUPSI - Scuola Universitaria Professionale della Svizzera Italiana, Switzerland.
- Technische Universitaet Darmstadt, Germany.
- Vitrociset, Italy

THE CYBERROAD CONSORTIUM



VISIT OUR WEBSITE

http://www.cyberroad-project.eu/en/

JOIN US IN SOCIAL MEDIA

https://twitter.com/cyberroad_eu

https://www.facebook.com/cyberroadproject

https://www.linkedin.com/groups/CyberROAD-8184478

CONTACT THE COORDINATOR

Prof. Fabio Roli
Department of Electrical and Electronic Engineering
University of Cagliari - Piazza d'Armi 09123, Cagliari, Italia.
E-mail: roli@diee.unica.it, **Phone:** +39 070 675 5779, **Fax:** +39 070 675 5782