Deloitte.

Fraunhofer SIT

Cyber Security
The perspective of information sharing

Cyber Security
The perspective of information sharing

Contents

Introduction

On February 7, 2013 the European Commission released the European Union's Cyber Security Strategy with the subtitle "An Open, Safe and Secure Cyberspace". The strategy defines five short and long term priorities and actions that involve EU institutions, member states, and industry:

1. Achieving cyber resilience
2. Drastically reducing cyber crime
3. Developing cyber defense policies and capabilities
4. Developing industrial and technological resources for cyber security
5. Establishing a coherent international cyber space policy for the European Union

One aspect that can be found in almost every priority and action is the sharing of cyber security information within and between the private sector, national entities, member states, and EU institutions like ENISA, Europol/EC3, and EDA.

In April and May 2013 Deloitte interviewed European private organizations from the Forbes Global 2000 list and selected European public organizations and research institutes from ENISA's Who-is-Who list in an online survey.

The German Fraunhofer-Institute for Secure Information Technology (SIT) supported the interviews and the evaluation of the survey results.

Objectives

Objectives were to identify the current state of cyber security information sharing within the countries of the European Union, addressing the following topics:

- Cyber incident capabilities and escalation behavior
- Rating of the importance of cyber security information sharing
- Existence and impact of current national cyber directives or regulations
- Frequency and sources of cyber security information collection
- Willingness and reality of sharing cyber security information
- Awareness of the EU Cyber Security Strategy and expected impacts

Approach

Participants were invited via email to take part in the survey and complete an online questionnaire. The answers were collected anonymously in order not to allow any response to be mapped to a specific participant. Accordingly, the survey results are anonymous as well.

Cyber security information sharing is already an European priority topic

Cyber Security – a new buzzword or a real challenge for companies and the public sector?

Mechthild Stöwer
Security Management
Fraunhofer SIT
Tel: +49 (0)2241 14 3123
mechthild.stoewer@
sit.fraunhofer.de

Peter Wirnsperger
Partner Cyber Security
Deloitte
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Absolute cyber security does not exist. The question is therefore not whether IT systems will be attacked, only when this will occur. Science, industry and the public sector need to take action in the sense of 'collective intelligence' against current and future threats. Deloitte and the Fraunhofer SIT maintain close cooperation and provide answers to questions around cyber security.

What does cyber security mean?

Deloitte
Cyber security is the logical development of what used to be known as information security. Today it is no longer about protecting particular data from individual attackers, but rather defending against many forms of attacks within a complex threat environment. Correspondingly, effective protection covers the whole range of available tools and technologies from the areas of Information Security, Operational Technology Security and IT security. Anyone who believes that having up-to-date quality software and implementing safety guidelines and standards is enough to be secure is confining their thinking to the short term. At the same time, organizations need to continuously review their infrastructures and applications for security vulnerabilities, and have access to intrusion detection systems and emergency plans in case of a cyber attack.

Fraunhofer SIT
The term 'cyber security' makes clear that all information and communication systems within the private, public or commercial environments which are connected to the internet or comparable networks are exposed to attacks from the world-wide network. The attacks are highly professional and are now managed by economic and geostrategic interests.

Is cyber security only an issue for large companies?

Fraunhofer SIT
No, quite the opposite. We observe a strong imbalance between the abilities of attackers, the sustained nature of their attacks, and the security standards and awareness within companies or even government organizations. In particular, medium-sized companies are lagging behind the attackers' potential. This is all the more critical since, with their innovations and technologies, they form the backbone of the German economy.

This urgency is further increased by the fact that medium-sized enterprises are also elements within value-adding chains across organizations. They are therefore required to have high security standards to ensure the confidentiality and integrity of information over the whole chain.

Deloitte
Cyber crime can affect anyone: from private individuals through government institutions and critical infrastructures to networked global corporations and medium-sized businesses.

Compared with large corporations, the lower capital resources in SMEs[1] hold higher risks: after all, monetary losses following a cyber attack could result in threats to the company's existence. In addition, SMEs are the target of cyber criminals more and more often. In 2012, malware attacks alone on this company segment increased by 86 percent.

What are the dangers? What should people prepare for?

Fraunhofer SIT
It is well known that cyber threats exist in many and varied formats. There are conventional forms such as online fraud during payment transactions or while shopping on the internet. A particular threat here is cyber espionage, which focuses not only on commercial enterprises, but also on government organizations.

Increasingly, production systems are also under cyber attacks. If critical infrastructure facilities such as energy supply systems or telecommunications infrastructures are under attack, then the cascading effects could impinge on whole areas of the economy. Particular challenges arise in the future by increasing the use of machine-to-machine communication. This offers large efficiency potentials in an environment of 4.0 concepts but also corresponding possibilities of attacks, provided that IT security is not thought along from the beginning.

Research institutions have already accepted some of the challenges sketched out. For example, Fraunhofer SIT, alongside some companies, has already developed forward-looking concepts and initial solutions.

Deloitte
In 2012, we experienced a number of attacks from botnets, malware, Trojans and phishing. The perpetrators count on the quality and quantity of their attacks and are acting significantly more professionally. Cyber criminals these days are better financed and increasingly organized in networks. Accordingly their attacks are better targeted, more sophisticated and harder to detect. Most spionage cases are only discovered by accident. So it is no surprise that the monetary damage from cyber espionage is huge for the German economy: it is estimated to be 50 billion euros per year.

[1] Small and medium enterprises (SMEs).

At the same time, cyber criminals are increasingly targeting innovative technologies: the utilization of personal mobile devices and cloud services in the business environment are making the IT landscape more vulnerable.

And not least, well-informed employees contribute to combating threats effectively. Clear guidelines, practical training courses and continuous information are the remedy.

What are the conditions for cyber security?

Fraunhofer SIT

Cyber security requires attack-resistant, robust systems with integrated and cooperative attack detection and defence concepts. Security must be anchored within hardware and software architectures. Research and industry need to implement joint projects in the medium term that deal with topics such as Security by Design, new risk models, the resulting information security management concepts and protecting mobile systems or security for industry 4.0.

In any case, however, companies need to analyse and evaluate their security requirements and their safety needs. The selection of solutions should then be in alignment with the actual threat situation. Tests and audits, but also the integration of security metrics in their security management, are examples of tools to improve the safety level within the company in the long term.

Deloitte

The key is to think of cyber security in an integrated way. Companies have to prepare themselves, assess threats in real time and provide a coordinated reaction in an emergency. The starting point is their cyber strategy, which covers various aspects such as system security, web safety and password security and at the same time is geared towards the current trends.

Extensive preparation relies on companies being very familiar with the different threat scenarios for their processes and data. Existing measures must be reviewed for their effectiveness on a regular basis. Cyber simulations uncover technical and organizational weak points. Based on these, an integrated security architecture for the whole organization can be planned and implemented. Last but not least, employees need instruction on how to handle data correctly.

Monitoring is primarily concerned with detecting attempted attacks immediately and repelling them effectively. In an emergency, fast and coordinated action is necessary. Good crisis management limits the damage and secures the traces of the intrusion.

Which players are involved?

Deloitte

Cyber security is not just a topic for IT and security experts within the company. In view of its growing importance to the long-term success of the business, it has become a top management task. Support from executives is vital. On the one hand, security concepts and measures need a stable financial basis. On the other, it is important to effect changes in behavior on all levels of the business.

Fraunhofer SIT

Security policies and measures need a stable financial footing. Therefore, cyber security is (also) a management task. However, management also needs to control behavior changes at all levels of the company. As the highest level of security implemented is useless if the safety systems are consciously or unconsciously avoided at user level.

How can the parties concerned work together to increase cyber security?

Fraunhofer SIT

Among the players involved, there is a great degree of consensus that cyber security is strengthened by a multi-stakeholder approach. Both government institutions and business enterprises benefit from sharing information about current threats, events and corresponding countermeasures.

Deloitte

I am convinced that the changing threats in cyber space can be fought more effectively through closer cooperation between companies and security service providers on the one side and industry, science and politics on the other. We need a Collective Intelligence, which arises from the exchange of information about weak areas, threats and countermeasures.

Detailed survey results

Participants

Approximately 350 private and public organizations, research institutes, and industry groups were invited to take part in this online survey. The list of participants covered 31 countries across Europe.

Private organizations came from different industries such as manufacturing, healthcare and life sciences, financial services, or technology, media, and telecommunications. Public organizations included ministries, authorities for information technology and communications, police forces, and intelligence and secret services. Research institutes included universities, institutes, and laboratories for information technology and communications.

Results

Out of all respondents who provided feedback, about 31% came from private organizations, 54% from public organizations, and approximately 15% from the research institutes.

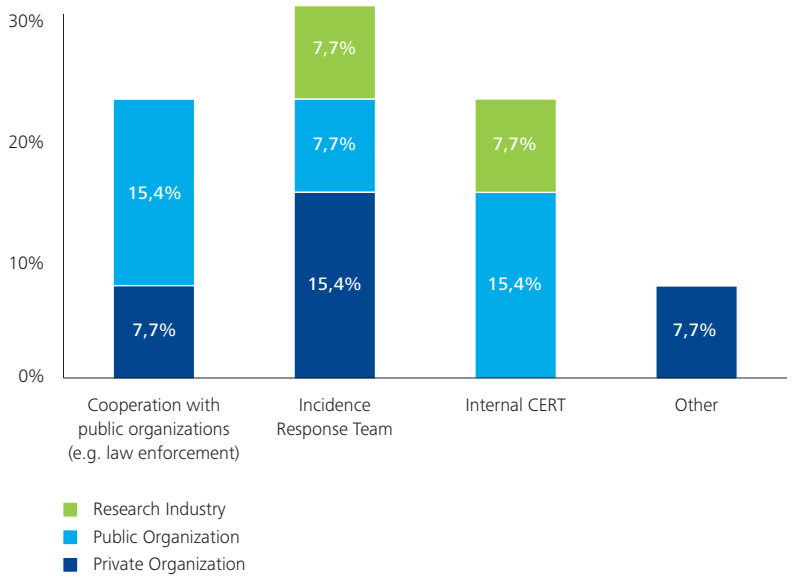
Eighty-five percent of the respondents are organizations sized between 1 and 499 employees.

Due to the unexpected low response rate, we do not consider the results to be representative, but they still allow for a solid comparison between private and public organizations with additional insights into the research institutes. Industry groups are not specified in the results.

Cyber incident capabilities and escalation behavior

Thirty-one percent of the respondents stated they have a local incident management team, 23% have an internal CERT, and another 23% would ask for support from local public organizations[1]. In the event that they were not able to handle a cyber incident themselves, the majority of respondents would request support from public organizations. In most cases national or federal CERTs would be asked for support, whereas only in a few cases would national/federal police forces be included (fig. 1).

Fig. 1 – Cyber incident capabilities and escalation behavior per sector



[1] The remaining 23% either did not respond to this question or are a CERT on their own

Rating of the importance of cyber security information sharing

There is a very definite awareness of the importance of information sharing within the group of respondents: 92% rated the priority of cyber security information sharing as high, 8% as medium, and 0% as low (fig. 2 and 3).

Existence and impact of current national cyber security directives or regulations

Across all sectors 64% of the respondents stated they are currently not affected by any existing regional/ national or EU cyber security directive or regulation. The 36% affected by existing directives or regulations mentioned for example the EU Directive 2009/140/ CE, the Portuguese Electronic Communications Law No. 51/2011, the Swedish regulation SFS 2006:942 on Emergency Preparedness, and other national laws regarding cyber security or cyber crime. The biggest impacts of information sharing are related to information security governance, followed by technology and business processes.

Fig. 2 – Responses per sector and size

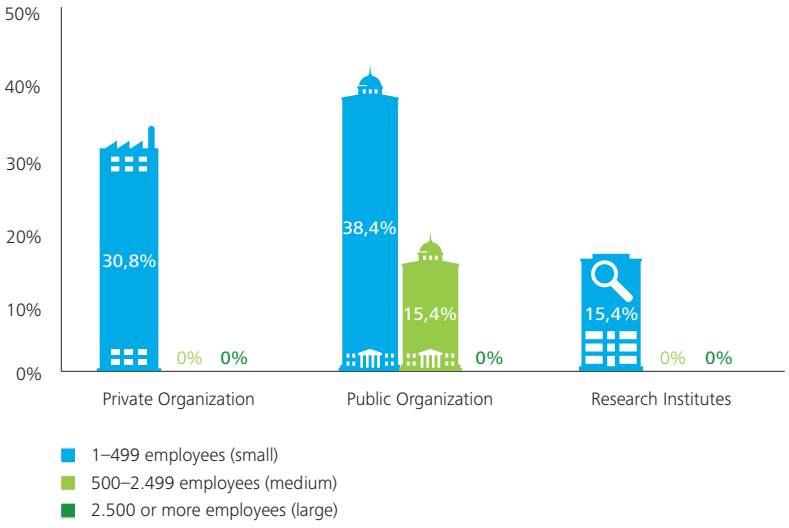
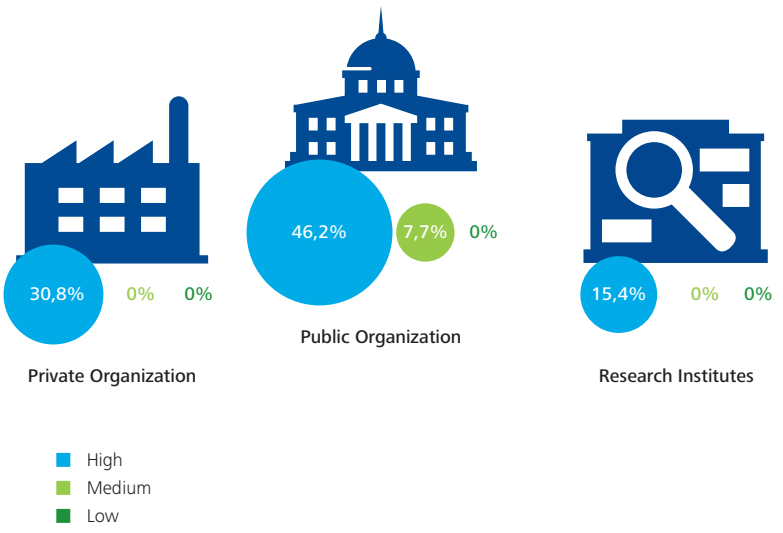


Fig. 3 – Rating the importance of cyber security information sharing per sector

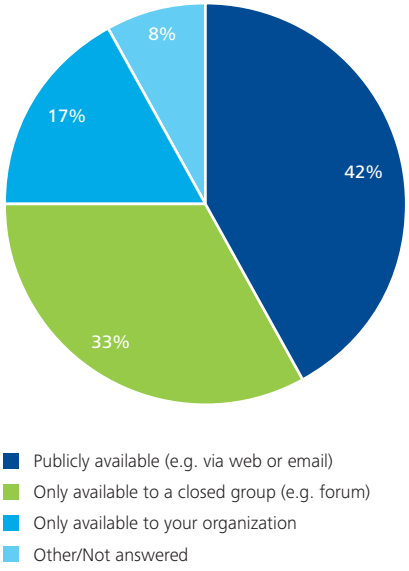


Frequency and sources of cyber security information collection

Sixty-two percent of all respondents regularly use[2] available cyber security information. Sources from public and private organizations account for 24% each, followed by sources from the research institutes with 15%. Other sources, e.g. industry groups, play a minor role.

In the use of sources no preferences have been identified. Public and private organizations equally use sources from public and private organizations. Most organizations prefer publicly available information (42%), but about 50% use information that is either only available to a closed group or only to the respondent's organization (fig. 4).

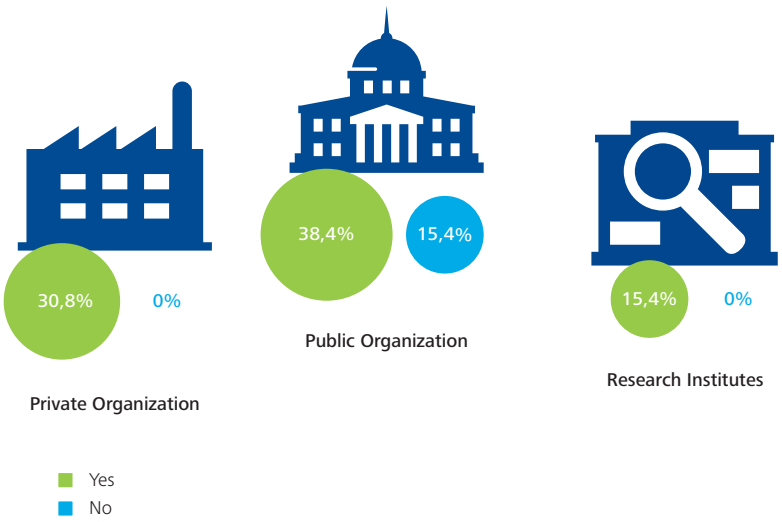
Fig. 4 – Sources of cyber security information sharing



Willingness and reality of sharing cyber security information

Eighty-five percent of all respondents are willing to share cyber security information. The 15% who reject sharing information are all from public organizations. Two-thirds of the 85% willing to share would do it on a voluntary basis, whereas one third state they would only share when required to and if regulated by law (fig. 5).

Fig. 5 – Willingness to share cyber security information per sector



[2] Monthly, daily or even more frequently

Asked whether organizations are at present sharing cyber security information, the picture is slightly different. Only 57% are currently involved in sharing activities; within this group public organizations account for 50%. Of sectors not involved in any sharing activities, 60% are private organizations.

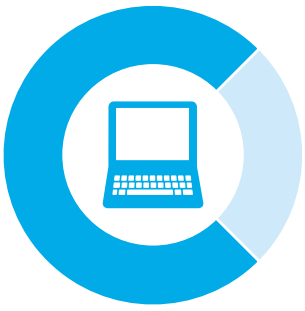
The information being shared is mainly about current cyber threats, followed by details of successful cyber attacks, indicators of compromise, and good practice controls. Most information is shared with public organizations.

Three quarters of the 57% currently sharing cyber security information use a dedicated software tool for it. Also there are some complaints about these tools (e.g. complexity, technical issues, or lack of qualified participants); the overall majority is satisfied with the system.

Awareness of the EU Cyber Security Strategy and expected impacts

Asked about awareness of the Cyber Security Strategy of the European Union, only 57% answered "Yes". Out of these 57%, one quarter have planned concrete action to comply with the strategy - they are all from private organizations. The biggest limitations to compliance with the strategy are budget and organizational challenges.

57%
are currently involved
in sharing activities



3/4 of them
use a dedicated software
tool for information sharing

Conclusions

Cyber security information sharing is widely seen as very important across all sectors and industries. The majority of participants is willing to share cyber information and would do this on a voluntarily basis. Yet presently about 43% are not sharing any information at all. The main reasons for not sharing are legal reasons or business concerns, and a lack of resources or adequate staff. Additional feedback we received during the invitation phase indicates that several organizations have not integrated cyber security information sharing into their overall cyber security governance framework.[3] So the low participation rate also gives an indication that many organizations might still not be ready even to consider sharing as an important source of improving security.

More than half of the participants are aware of the EU Cyber Security Strategy, and the proportional awareness of private organizations is much higher than for any other sector. This and statistics of planned actions indicate that private organizations are more concerned about cyber security law and regulations and their potential impact on their business.

The survey additionally shows that especially small to medium size organizations would not involve police forces in the event of a severe cyber incident. Reasons for this might be lack of trust, not being aware of potential support, or conflict of interests. However, this might be an interesting topic for additional studies.

[3] Potential participants – mostly medium and large sized – stated that their organizations lack a policy or roles and responsibilities for cyber security information sharing. They would therefore not participate in the study.

Our offices

10719 Berlin
Kurfürstendamm 23
Tel: +49 (0)30 25468 01

01097 Dresden
Theresienstraße 29
Tel: +49 (0)351 81101 0

40476 Düsseldorf
Schwannstraße 6
Tel: +49 (0)211 8772 01

99084 Erfurt
Anger 81
Tel: +49 (0)361 65496 0

60486 Frankfurt am Main
Franklinstraße 50
Tel: +49 (0)69 75695 01
Consulting:
Franklinstraße 46–48
Tel: +49 (0)69 97137 0

06108 Halle (Saale)
Bornknechtstraße 5
Tel: +49 (0)345 2199 6

20355 Hamburg
Dammtorstraße 12
20354 Hamburg
Tel: +49 (0)40 32080 0

30159 Hannover
Georgstraße 52
Tel: +49 (0)511 3023 0
Consulting:
Theaterstraße 15
Tel: +49 (0)511 93636 0

50672 Köln
Magnusstraße 11
Tel: +49 (0)221 97324 0

04317 Leipzig
Seemannstraße 8
Tel: +49 (0)341 992 7000

39104 Magdeburg
Hasselbachplatz 3
Tel: +49 (0)391 56873 0

68165 Mannheim
Reichskanzler-Müller-Straße 25
Tel: +49 (0)621 15901 0

81669 München
Rosenheimer Platz 4
Tel: +49 (0)89 29036 0

90482 Nürnberg
Business Tower
Ostendstraße 100
Tel: +49 (0)911 23074 0

70597 Stuttgart
Löffelstraße 42
Tel: +49 (0)711 16554 01

69190 Walldorf
Altrottstraße 31
Tel: +49 (0)6227 7332 60

Contacts

For more information

Peter Wirnsperger
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Thomas Donner
Tel: +49 (0)89 29036 8614
tdonner@deloitte.de

For more information please visit our website at www.deloitte.com/de/cyber

Issued 10/2013