INFORMATION SECURITY IN SWISS COMPANIES

A survey on threats, risk management and forms of joint action

Zurich, August 2006

CSS
An ETH Center

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contact:
Center for Security Studies
Seilergraben 45-49
ETH Zentrum / SEI
CH-8092 Zurich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch

Contents

List of Figures

Foreword

Computer-related criminality has existed ever since the computer ousted the pen and paper from our desks. And, with the global networking of computers, Internet crime has steadily gained ground. Still, the full extent of the threat this poses remains nebulous, lying somewhere between the world of fiction and virtual reality.

Aware of this problem, the Swiss Federal Council has taken two major steps to meet a broad spectrum of needs: first, by creating KOBIK,[1] a coordination centre against Internet crime, and secondly with MELANI,[2] a reporting and analysis centre for information security. Through this response, a range of dedicated and efficient structures have been established to protect society from cybercrime. What was missing, however, was a comprehensive current-state analysis of such measures and the threat level facing the Swiss economy. In other countries, particularly the United States, nationwide studies have been available for several years, such as the annual CSI/FBI Computer Crime and Security Survey.[3] The 2005 version, for instance, contains some well-supported data, such as the fact that half the US companies asked had experienced a computer security breach during the previous year, or that 95% had suffered some form of website defacement. More significant, however, is the sharp rise in the costs incurred per IT attack, from an average of some USD 51,000 to approximately USD 300,000.

Such findings are helpful in public outreach and awareness efforts. However, they also enable organisations to draw conclusions, appraise their own security breaches within a broader context, evaluate the efficiency of measures taken, and determine their own security needs. The task of conducting a nationwide study in Switzerland was entrusted to the Center for Security Studies at ETH Zurich.[4]

The findings are, on the one hand, as predicted, serving to confirm some known trends, but are also somewhat surprising in other respects, highlighting facts that were quite unexpected. Experts in the field will undoubtedly appreciate the contents of this report; however, due to its clearly written format, the survey will also be of interest to all those involved in information security – an issue that cannot be avoided over the coming years.

Mauro Vignati
MELANI Analyst, Project Manager

1 http://www.scoci.ch.
2 http://www.melani.admin.ch.
3 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005).
4 http://www.css.ethz.ch.

Key findings

A significant majority of respondents (72%) experienced at least one information security breach in 2005.
The most widespread incidents concerned viruses, worms, trojans and spyware. Another threat frequently encountered was the conventional theft of laptops or other hardware. Other, less frequent forms of computer-enabled crime were denial of service attacks, hacking, data theft and website defacement.

Large firms with over 250 employees and companies that buy and/or sell online are at a higher risk of such an incident.
In particular, large firms and companies operating in e-commerce are far more likely to suffer targeted attacks.

Almost all firms have instituted some form of technical and organisational security measures.
Of the various security technologies, anti-virus software and firewalls are used in practically all companies. In terms of organisational security, the most widespread preventative measure is back-up management. More complex technical and organisational security measures (such as crisis management teams) tend to be found in large firms and in companies operating in the IT sector.

The level of financial and human resources devoted to information security is low.
Only a minority of the firms that responded to the survey (32%) have a qualified IT specialist responsible for information security.

Many firms outsource the risk of an information security breach.
Outsourcing is particularly popular among medium-sized enterprises. In addition, companies often purchase insurance against cybersecurity risks.

A large number of companies would welcome intensified joint action.
The majority of these believe that new organisations would have to be created to implement such joint action. In any case, any such cooperation would have to address the fact that the different companies' needs are highly diverse.

1 Introduction

Information and communication technology (ICT) plays a central role in many Swiss firms and administrations. ICT enables us to work in a network, simplifying communication within and between organisations. The development of this new technology, however, also heralded the arrival of a new set of problems. Back in the 1980s, everyone was talking about the emergence of computer viruses; nowadays, these are a worldwide phenomenon and only one of many threats to information security.

Our increasing dependency on ICT in a wide range of activities and the laxity sometimes observed in its use have increased the risk of ICT failure, threatening the smooth running of the business world. A breakdown in ICT systems would have serious economic consequences for Switzerland. According to a study conducted by the Computer Engineering and Networks Laboratory (TIK) at ETH Zurich, a one-week Internet blackout in Switzerland would cost the economy CHF 5.83 billion. The study highlighted the importance of IT and the Internet in a modern society like ours, with 48% of Switzerland's 3.6 million jobs relying on ICT.5

In light of this situation, companies are now taking various precautionary steps, ranging from security technology and/or organisational changes to general staff awareness programmes – depending on their security requirements and available resources.

The objective of the present study is to provide an overview of the threats facing the Swiss economy in terms of information security and to learn how companies and administrations are tackling these. The study also examines the possibility of organised cooperation between companies and how State intervention might help the private sector protect its ICT systems.

1.1 Methodology

In order to ensure the broadest possible overview, a written survey was undertaken among firms and administrations of all sizes, from all parts of the country and in all secondary and tertiary sectors (i.e. industry and services). A total of 4,916 organisations were contacted by e-mail or by post.[6] For the sake of simplicity, the questionnaire itself was not sent; instead, it was made available online at the specified link via the given password. The questionnaire, with 36 questions, was accessible to survey participants for a period of four weeks (from 15 March 2006 to 13 April 2006).[7] During this time, it was completed 562 times, corresponding to a response rate of 11.45%, which is within the normal range for such surveys.[8]

1.2 Prior research and comparable studies

The problem with most previous studies in ICT security is that they only either address the technical factors or are written as in-house guidelines for IT security managers. No inventory of information security in Swiss firms has ever been drawn up before. The 2002 report *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz* ("Internet Use in Swiss

5 Dübendorfer, Thomas, Arno Wagner and Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Study by the Computer Engineering and Networks Laboratory of ETH Zurich, 2004), p. 4.

6 See Appendix 1 for details on the selection and composition of the sample pool.

7 Appendix 5 contains the questionnaire itself and details about the survey method.

8 See Appendix 2 for a detailed evaluation of the response.

SMEs") by the SME Task Force[9] was of use in the present study, however, as it is important to know how IT is viewed in the various firms when analysing computer security.

Some extensive studies on information security in the corporate world have previously been undertaken in other countries, allowing us to compare our results with international findings. In particular, "CSI/FBI Computer Crime and Security Survey 2005,"[10] "Hi-Tech Crime: The Impact on UK Business 2005" by the UK's National Hi-Tech Crime Unit,[11] and "The IT-Security Situation in Germany in 2005"[12] by the German Federal Office for Information Security (BSI) were important sources of comparative data.

1.3 Terminology

This section defines some of the terms frequently used in this report.

Information security
Information security (also referred to as computer security or IT security) aims to prevent unauthorised modification of or access to information or data. Maximum information security is achieved by combining technology with operational / organisational measures.

Objectives of information security
Authenticity: The authenticity of an object (e.g. data, systems, server, etc.) or a subject (user) refers to the genuineness of its identity, which must be verifiable by means of clear and unambiguous characteristics.
Data integrity: Data integrity is ensured when subjects and objects are unable to modify the data to be protected.
Confidentiality: A system ensures confidentiality if it prevents all unauthorised access to information, even during data transfer.
Availability: A system is said to be available when identified and authorised subjects can exercise their rights without any unauthorised restrictions.

Vulnerability
Vulnerability refers to the weaknesses of a system that could jeopardise the above objectives. Vulnerabilities can exist with respect to physical threats (fire, water, earthquake, power loss, etc.), inappropriate use, or, for instance, malware.

Threat
A system faces a threat when there are one or more vulnerabilities that could endanger the above objectives.

9 Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (study commissioned by the State Secretariat for Economic Affairs, Bern, 2002).

10 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005). http://www.gocsi.com

11 National Hi-Tech Crime Unit (NHTCU), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005). http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

12 German Federal Office for Information Security (BSI), *The IT-Security Situation in Germany in 2005* (July 2005). http://www.bsi.bund.de/english/publications/securitysituation/lagebericht2005_englisch.pdf

Risk

The risk defines the probability (or relative frequency) of a threat resulting in actual damage as well as the costs incurred by such damage. The risk is therefore also dependent upon the value of the items to be protected.

Attack / incident

An attack refers to an attempt, whether successful or not, to access a system without authorisation. A distinction is made between passive attacks (e.g. unauthorised information access, loss of confidentiality) and active attacks (unauthorised modification of data, loss of data integrity or availability).[13]

The term "incident" is used more generally in this study, however, to address the fact that inappropriate handling with no malicious intent can also result in information security breaches.

13 These definitions are adapted from: Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle*, 3rd edition, revised and expanded, Munich and Oldenbourg 2004, p. 4-17

2 Frequency of incidents

This first part of this study looks at the frequency of incidents, the information security threat from a company's own staff, and the risk of an incident by company type and form of threat. First, however, we need to clarify which security threats we are referring to and how these are defined. The following explanations of the individual threats are brief, with more specific details readily available online and in the literature.[14]

2.1 Information security threats

The participants were asked about the main known threats to information security. In essence, such threats relate to confidentiality, availability and data integrity. The questionnaire did not cover spam, i.e. unsolicited advertising sent via e-mail; although such junk e-mails may be very annoying, they usually do not pose a direct threat to information security.

2.1.1 Description of the threats covered in the survey

Viruses, spyware, worms and Trojan horses (known collectively as malware)
A *virus* consists of program instructions that tell the computer to perform certain actions. In order to spread, the virus attaches itself to what is known as a host application. This may be an application (e.g. downloaded software) or a document (e.g. Word file, Excel file). When the application is executed or the document is opened, the virus is activated, causing the computer to perform harmful actions. Viruses often infect a computer via e-mail attachments or infected files downloaded from the Internet to the computer. Once activated, they may spread via e-mail to contacts in the address book. External data storage devices are further means of distribution (e.g. CD-ROMs, USB memory sticks, etc.).

Spyware collects information without the user's knowledge and transmits this to a predefined address. The information collected depends on the spyware in question and can include anything from surfing habits and system settings to passwords or confidential documents.

Worms, like viruses, are programs that instruct the computer to perform certain actions. Unlike viruses, however, worms do not require a host program in order to propagate. Instead, they use security holes or configuration errors in operating systems or applications to spread by themselves from one computer to the next. Computers that have security holes or configuration errors and are connected to other computers (e.g. via the Internet, the local network, etc.) are possible targets for worms.

Trojan horses (often referred to as trojans) are programs that covertly perform harmful actions while disguised as a useful application or file. Trojan horses are often programs downloaded from the Internet. However, sound and movie files can also be Trojan horses. These use security holes in the corresponding player programs (e.g. Media Player) to install themselves covertly into the system. Trojan horses are also often distributed via e-mail attachments. They are mainly used for

14 Information at:
http://www.melani.admin.ch/gefahrenschutz/gefahren/index.html?lang=en&PHPSESSID=7163ed179ac94a817330beec749086a2. Numerous overviews of information security are available in the literature. For further details: Bidgoli, Hossein et al. (eds.), *Handbook of Information Security, Volume 3* (Hoboken, 2006).

spying on confidential data, complete takeover of a computer or for sending spam via the infected computer.

Denial of service (DoS)
Denial of service attacks aim to cause the loss of a specific service to users or at least to considerably restrict the accessibility of the service. A popular variant of DoS attacks in the IT sector is to send huge numbers of requests to a computer/service. Due to the flood of requests, the computer/service becomes so overloaded that a great deal of time is needed to respond or it crashes altogether.

Such attacks often originate from different computers that have previously been manipulated using malware. This is known as a distributed denial of service attack (DDoS). Such attacks are particularly effective when aimed at companies making online business transactions and are often accompanied by blackmail attempts.

With many computers unknowingly infected by malware, leaving them open to misuse by hackers, the threat of DDoS attacks is also on the rise. If several infected computers are linked up in a network (known as a botnet), this makes it easy to perform a DDoS attack. Experts are therefore warning of a possible increase in the frequency of such attacks.

System penetration (hacking) and data theft
The term "hacking" has several meanings, often being used to describe all forms of unwanted manipulation of other computers. Here, hacking refers to the unauthorised penetration of an organisation's IT system. This is often achieved through the targeted use of spying programs (spyware, trojans). Once they have penetrated a system, hackers can read, change or delete data. The most damage is caused by hackers with criminal intent who steal information from a company. Such attacks often target confidential customer data or new trade secrets on which a company's business survival depends. Data theft can therefore have some very serious consequences for a company. In most cases, this sort of attack is difficult to detect.

Website defacement
The defacement of a company's website (or of several websites in the case of mass defacement) is achieved via security holes in web servers, which enable attackers to change the website content and design. Sometimes, such attacks are politically motivated, carried out by so-called "hacktivists" as a form of political protest. Often, however, websites are defaced for fun by "script kiddies". Depending on how much a company relies on its website for business continuity, the consequences of such attacks can range from a tarnished image to substantial financial losses.

Abuse of wireless networks
Wireless Local Area Networks (WLANs) provide a straightforward means of accessing the Internet without the use of wires and cables. Such networks are often inadequately protected, however. Attackers can use such poorly protected access points to abuse the connection for a variety of purposes. The main problem with this sort of incident is the fact that the abuse is usually noticed well after the event or sometimes not at all.

Conventional theft of laptops and other IT devices
Among all the new threats that emerge, we should not forget that computers and IT equipment can still be simply stolen in the old-fashioned way. Apart from the loss of the material value, this

may also result in huge additional losses, for example, in the case of sensitive data stored on a stolen laptop.

2.1.2 Frequency of incidents

The questionnaire asked whether the organisations had been affected by the above threats during the year 2005. The results show that information security incidents are frequent. 72% of respondents said that at least one of the threats described above had led to an incident in their information infrastructure. It should be noted, however, that the survey pool does not reflect a proportional image of reality. For example, 15% of respondents are large companies with over 250 employees, whereas only 0.4% of all firms are that size in reality. Also, some business sectors are more heavily represented among respondents than in reality.[15] Because of this disproportionate composition of respondents, the average findings in the survey cannot be said to directly represent the average of all Swiss organisations in the manufacturing and service sectors. However, as we want to estimate the actual frequency of incidents, the statistical process of weighting is applied. This helps us to simulate reality by assigning different weightings to the company characteristics.[16] Once we apply this process, the proportion of Swiss organisations that noted at least one of the above-mentioned incidents in 2005 is estimated at 63%.

Because the various threats have very different consequences, it is important to find out how often the individual threats actually occur. Figure 1 shows how many of the respondents were affected by the various types of incident.

15 See Appendix 2 for further details on the response by size category and business sector.

16 All data are multiplied by a weighting factor. See Appendix 3 for more details about the weighting process.

Figure 1 Frequency of incidents

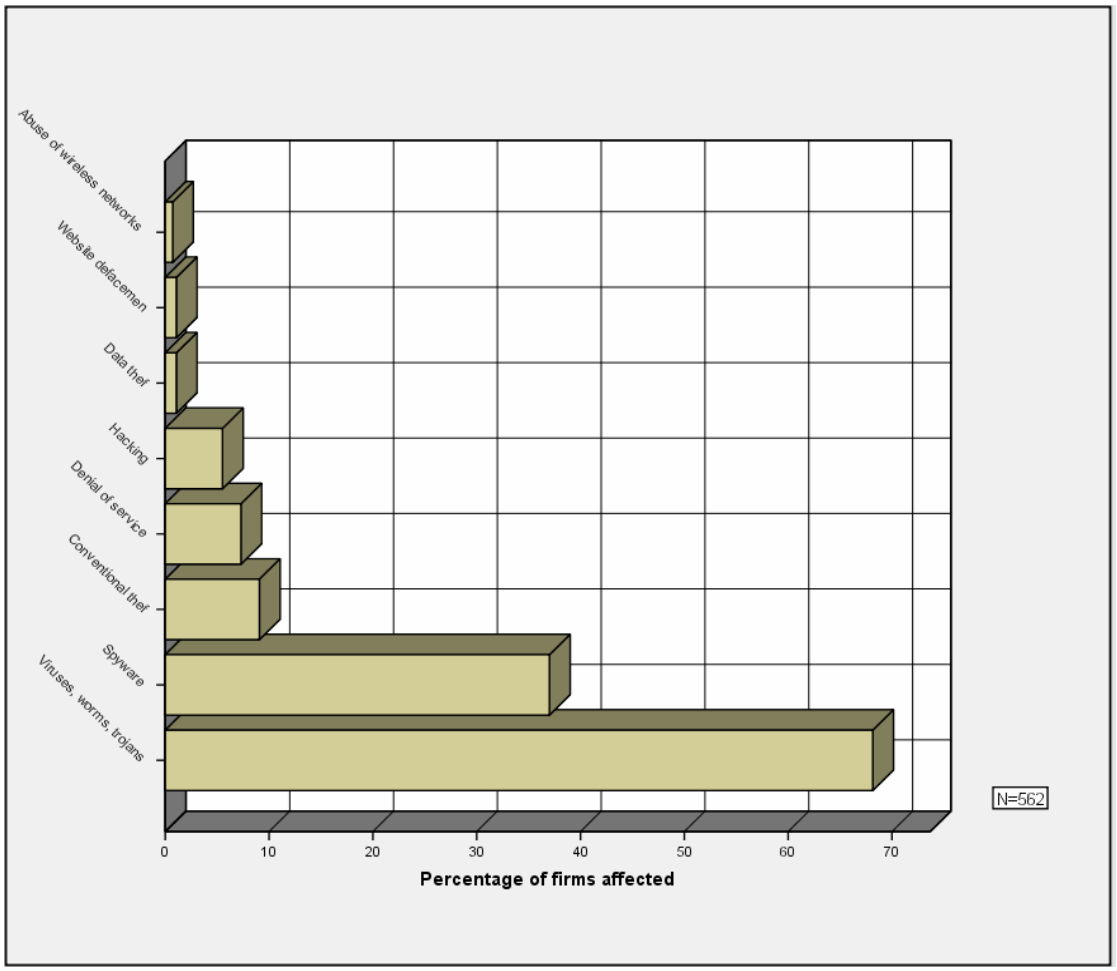


Figure 1 clearly shows that the most widespread threat comes from the various forms of malware (viruses, worms, trojans and spyware). Conventional theft of IT equipment is in third position. The more sophisticated attacks in technical terms, which also have a more serious impact, are encountered far less often.

2.1.3 Insider threats

Findings on the frequency of incidents are helpful in making a better estimate of the risk facing companies. It is important to know, however, where these incidents actually originate. In particular, it is interesting to find out how many such incidents are caused by an organisation's own staff.

Employees can jeopardise their company's information security for a number of different reasons. Often, they are the ones who enable malware to penetrate the system or facilitate such attacks by neglecting to follow the security guidelines. At other times, however, they are actually the perpetrators of the attack, for example to make money or take revenge on a superior. Many

experts believe that employees are directly responsible for a high number of incidents.[17] The UK study "Hi-Tech Crime: The Impact on UK Business 2005" also found a high proportion of incidents were employee crimes. According to this study, 37% of incidents recorded in UK companies are caused by acts of sabotage by dishonest or disgruntled employees.[18] In the present study, only 10% of respondents found this to be the case, which is a far lower percentage than might be expected. However, no direct comparison can be made with the UK study, as this also covered other threats and was conducted only on firms with over 100 employees.

Nonetheless, we can conclude that those incidents directly caused by employees are something of a rarity in Switzerland. Only in very rare cases is the damage by employees done deliberately. The threat posed by unintentional breaches is likely to be much higher.

2.1.4 International comparison of the frequency of incidents

So how do these levels of frequency compare with the studies conducted in other countries? The FBI's extensive survey "Computer Crime Survey 2005" found that 87% of respondents had fallen victim to computer-related criminality. However, the survey only covered companies with more than five FTEs. To compare like-for-like, the micro firms with fewer than five employees would have to be omitted. Thus, of the organisations in Switzerland with more than five employees, 79% have encountered such an incident. This figure is somewhat below that of the FBI study, but it should be noted that such incidents were more broadly defined in the FBI study. For instance, the discovery of pornographic material on a computer was also classified as such an incident.

The above-mentioned UK study "Hi-Tech Crime: The Impact on UK Business 2005" also shows that Switzerland encounters similar information security problems as other countries. That survey found that 89% of firms with over 100 employees had encountered an incident in 2004. If we consider only firms with over 100 employees in the present study, the figure for Switzerland comes in at a similar 85%.

Concerning the type of incidents, our findings are roughly the same as those in international studies. The FBI study also found that viruses and spyware were by far the most frequent breaches noted, that conventional theft was quite common, and that targeted attacks tended to be rare.

Therefore, we can conclude that Swiss companies are not facing any more or less computer-related criminality than organisations in other countries. In fact, it is precisely because of global networking that companies throughout the world face more or less the same level of threat to information security.

2.2 Risk by company type

Although the geographical location of companies does not appear to have any decisive impact on the risk of an incident, the size and business field of a company could be expected to affect the

17 One Gartner report even estimates that 70% of misuse of information systems is committed by employees. Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Summary of findings available at: http://www.csoonline.com/analyst/report3317.html. The German Federal Office for Information Security also believes that a large proportion of such breaches are internal: Federal Office for Information Security, *The IT-Security Situation in Germany in 2005* (July 2005), p. 29.

18 The National Hi-Tech Crime Unit (NHTCU), *Hi-Tech Crime: The Impact on UK Business 2005* (2005), p. 20.

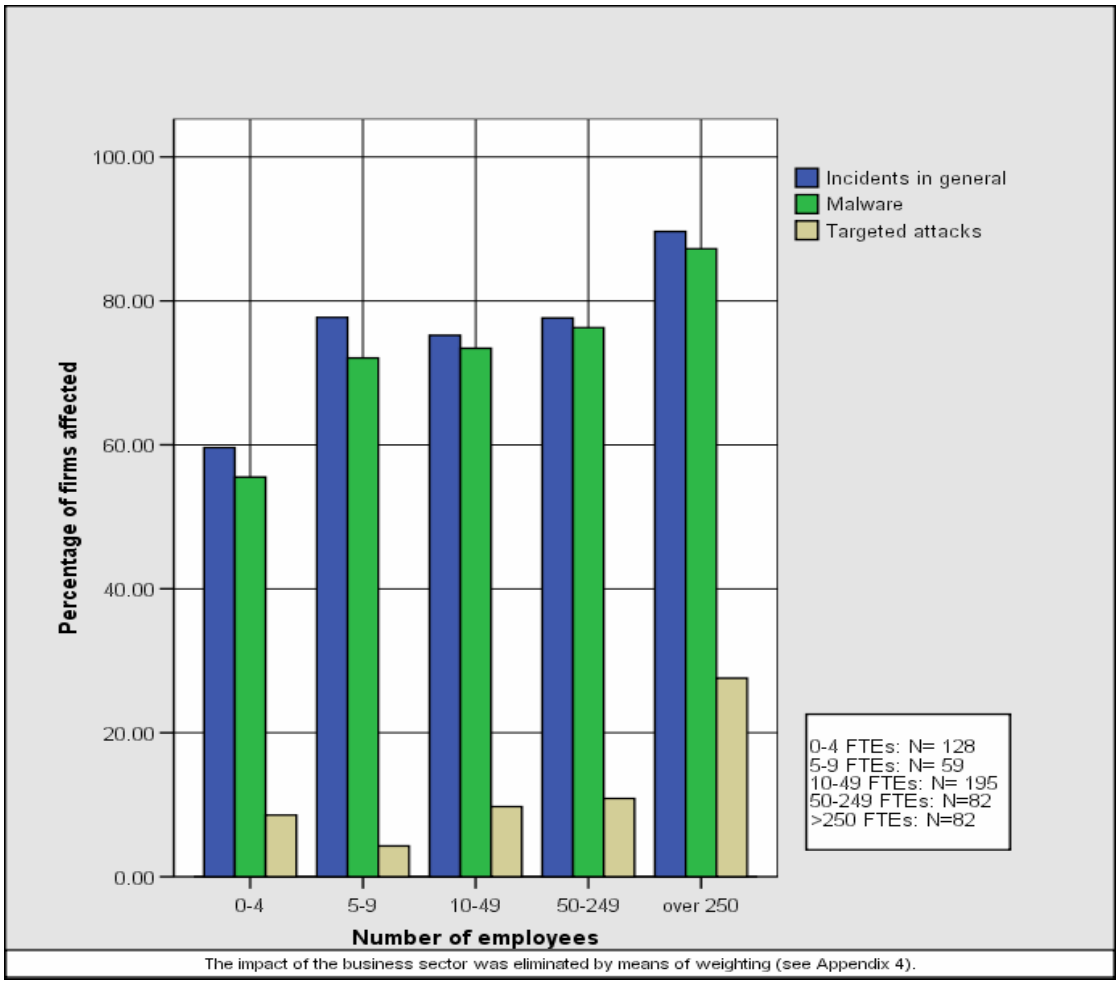
probability of it encountering malware and targeted attacks. The following paragraphs look at which types of firms are most frequently affected by such incidents.

2.2.1 Risk by number of employees

The study conducted by the SME Task Force on IT and Internet use in companies showed a direct relationship between company size and IT use: the bigger the firm, the greater the importance it places on IT and Internet technologies.[19] However, more intensive use of these resources also raises the risk of incidents. For instance, the more employees there are sending and receiving e-mails, the greater the likelihood of viruses finding their way into the corporate network. Apart from that, larger firms are more attractive for targeted attacks. From a hacker's point of view, carrying out such targeted attacks is only really worth the effort if the company in question generates sufficient revenues or has sufficient assets to be targeted or appropriated. Obviously, more money can be taken from bigger companies than from smaller ones.

Figure 2 shows how the probability of an incident rises with the size of the organisation.

Figure 2 Risk of incidents by number of employees



19 Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: Von der Einführung 1999 zur Entwicklung erster geschäftskritischer* Anwendungen (Berne 2002), p. 19.

Figure 2 clearly shows that micro firms with fewer than five employees had the lowest number of incidents as a whole. The small and medium-sized organisations (5-9, 10-49 and 50-249 employees) form quite a homogeneous group: they all clearly have more problems with malware, but do not encounter substantially more targeted attacks than the micro firms. Targeted attacks mainly affect large firms with over 250 employees, of which 28% have suffered such attacks. Malware also affects large firms more frequently than small and medium-sized organisations.

These findings thus largely meet expectations. The difference between micro firms and large organisations is quite distinct. What is perhaps more surprising is the negligible difference between small companies with 5 to 9 employees and medium-sized firms with up to 249 employees.

2.2.2 Risk by business sector

To differentiate organisations by their business activities, the usual approach would be to look at the sector in which they operate.[20] It is assumed that organisations operating in the same sector conduct their business in a similar manner. This study now also looks at the different risks of the various sectors.

Like company size, business sector also plays a role in the importance assigned to IT and Internet technologies within an organisation.[21] It could also be suspected that all sectors do not run the same risk of suffering a targeted attack, given that such attacks are more likely to be encountered in sectors where high revenues are generated or in sectors that tend to have access to large assets, which could be seized in a computer-based attack. Thus, it is to be expected that, for instance, companies operating in the financial services sector and those in IT, which use IT heavily and generate high revenues, will encounter such incidents more frequently than, for instance, construction firms or hotels and restaurants.

However, such expectations were not confirmed in the survey. Although IT companies did see many incidents, financial services companies did not fall victim to them any more often than the hotels and restaurants in the survey.[22] Perhaps the findings did not match expectations due to the fact that the individual sectors do not use protective measures to the same extent.[23]

Probably, however, a distinction by sector is not necessarily a reliable indication of the risk incurred by a particular business activity. Within an individual business sector, the significance of IT and Internet technology can differ very greatly from one company to another. If a business-related criterion is to have a greater impact on the risk level, it must be more closely related to the use of IT and Internet technology. One such criterion is online trading.

20 A distinction is made between 12 business sectors. For details on the sector division, see Appendix 1.

21 The survey findings in this respect correspond to the results of the SME Task Force. Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Bern 2002), p. 20.

22 When the findings by company size are weighted, 71% of financial firms and 73% of hotels and restaurants have encountered an incident. The sector that encountered the most incidents was that of business services (86%), with the trading sector reporting the lowest frequency (61%).

23 The next chapter goes into further detail about risk management.

E-commerce has become a very important phenomenon for Swiss firms. 77% of respondents said that they purchase goods or services online.[24] A much lower proportion (19%) sell goods or services via their website.[25] The assumption is that companies operating in e-commerce are more likely to encounter an incident, with a higher number of targeted attacks expected.

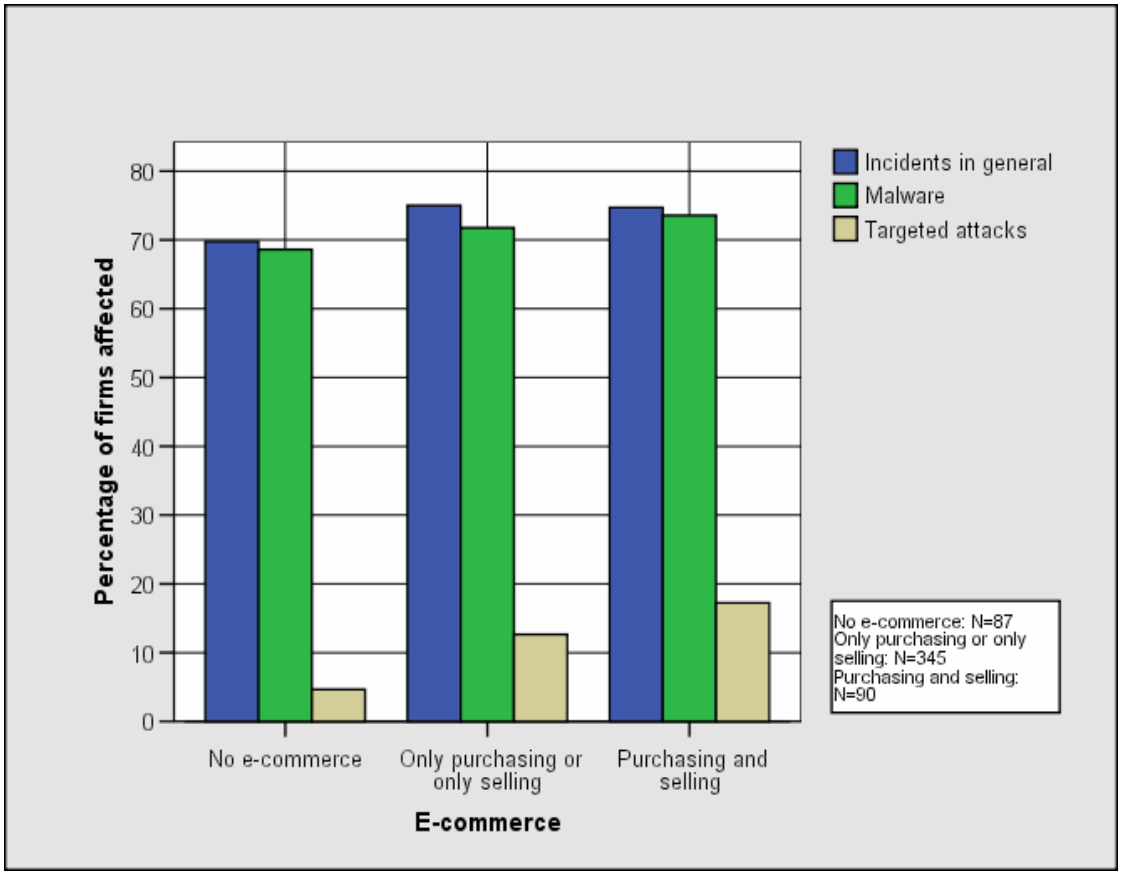


Figure 3 clearly confirms this assumption. Organisations that use e-commerce are at a much higher risk of a targeted attack. 12% of firms that either buy or sell using the Internet, and 17% of those that do both, reported being a victim of a targeted attacked. Meanwhile, the frequency of general malware with no specific target increases only slightly. Although organisations not using e-commerce record almost as many incidents, these are very rarely targeted attacks (only 5% of such firms have had such an attack).

Hence, the supposition that targeted attacks are more frequent among e-commerce firms is true. On the other hand, whether or not a company uses online trading has no bearing on the risk of general malware. As generic viruses, worms, trojans and spyware, which are not programmed for a specific, individual use per se, are much more widespread and therefore affect any vulnerable systems, regardless of the firm's commercial activities, malware is just as like to affect firms that do not use online trading.

24 Even after statistical weighting (see Appendix 3), the figure is still 73%. This very high figure corresponds to previous studies conducted in e-commerce. *Netzreport 2* (2001) found that 60% of firms purchase online. However, the study by the SME Task Force reported a figure of only 29% for SMEs. Information from: Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Bern 2002), p. 32.

25 14%, using the weighting procedure (see Appendix 3) to estimate the proportion among all Swiss firms.

2.2.3 Conclusion and other possible risk factors

The findings show that certain organisations run a higher risk of computer-related criminality than others. The size of the organisation and the use of the Internet for online trading play an important role.

Apart from the number of employees and the business activity, other factors can also influence the risk of an incident, such as the Internet connection type, the level of technical innovation and how well known the company is. More detailed studies would have to be made to predict the threat facing individual firms in this respect.

This may not even be possible, however. When analysing the risk by company type, we have to remember that the respondents only mentioned those incidents of which they were actually aware. The problem with targeted attacks is that these very often remain undetected for quite some time.

It should also be noted that the firms respond differently to threats to their information security. Technical and organisational measures can be taken to lower the likelihood of an incident occurring by averting the threat at an early stage or reducing any vulnerabilities, thereby lowering the actual risk for the same threat level. Improved protective measures within companies also help detect incidents at an earlier stage. The following chapter therefore takes a closer look at risk management within the organisation.

3 Risk management

With a wide range of threats facing information security, the protective measures available are just as varied. Risk management comprises not only numerous security technologies but also strategic and organisational issues. In order to maintain a clear overview, the various aspects of risk management are outlined individually in this chapter.

We begin by looking at the technical and organisational measures available and how these are used in organisations. Then we examine the extent of financial and human resources devoted to risk management in information security. Given that companies tend to want to spend as little as possible on safeguarding information security, it is interesting to see whether there are any significant differences between the firms. We conclude the chapter by looking at the frequency with which Swiss companies delegate the task of information security to external experts and whether they seek to cover this risk by purchasing appropriate insurance.

3.1 Technical and organisational security measures

When it comes to risk management, a company's main objective is to ensure that the measures it takes are the most appropriate for its specific circumstances. This section identifies which security measures are most used by which types of firms. A distinction is made between technical and organisational measures, so as to maintain a clear overview.

3.1.1 Definition of technical security measures

Before we discuss the extent of the various measures, a brief definition of each is given below (more detailed descriptions are readily available online and in the literature).[26]

Anti-virus software
Anti-virus software (or a virus scanner) is a basic technical measure in information security. This application detects malware on the computer and blocks or destroys it. In order for it to work, however, the malware pattern must be known. As new viruses and worms emerge every day, anti-virus software has to be updated on a regular basis.

Firewalls
Firewalls are used to protect computer systems from unauthorised access and the threat of malware. They do this by monitoring incoming and outgoing connections and rejecting them if necessary. Companies usually place firewalls at the interface between the Internet and their own network, forming another standard component of security technology.

Encryption
Whenever sensitive data is stored on computer networks, there is always the risk of unauthorised access to this information. The same threat exists in the transfer or communication of confidential data (e.g. by e-mail). This is where encryption programs come in. These use a specific encryption procedure, known as an algorithm, to convert data into a "secret text", which can then only

26 http://www.melani.admin.ch/gefahren-schutz/schutz/index.html?lang=en. These measures are also described in detail in Bidgoli, Hossein et al. (eds.) *Handbook of Information Security, Volume 3* (Hoboken, 2006).

be deciphered with the right code. Although this creates additional work for users, it is worth the effort when confidentiality is of crucial importance.

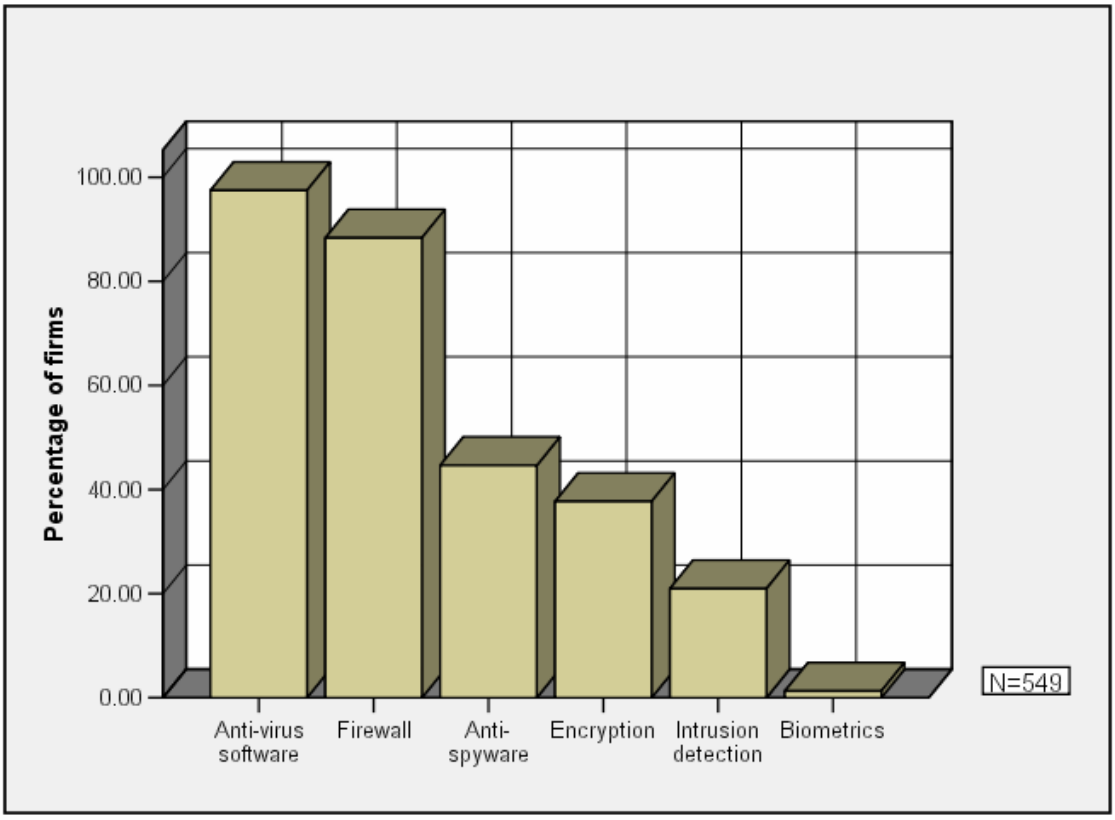
Intrusion detection
An intrusion detection system (IDS) is a program that monitors, stores and analyses activities on a computer or networks. Once a certain activity corresponding to a typical attack is detected, the system raises the alarm. However, making the best use of an IDS requires considerably more know-how than for firewalls or anti-virus software.

Biometrics
Biometric technology can be used to restrict physical access to computers. For instance, users have to identify themselves by means of fingerprints, face recognition or optical scanning systems. Such technology is generally relatively expensive.

3.1.2 Use of technical security measures

Figure 4 shows the extent to which the above measures are actually used in Swiss companies.

Figure 4 Use of technical security measures



Practically all respondents (99.6%) said they use at least one form of security technology. Anti-virus software and firewalls are used in 80% of organisations.

However, although most firms have taken some of the most basic technical security measures, the more complex technologies such as IDS and biometrics are rarely used. This is hardly surpris-

ing, corresponding more or less to the findings of the CSI/FBI survey of US firms.[27] Clearly, the additional costs involved mean that fewer companies opt for such technically and indeed financially demanding measures. For some companies, such measures would not make much sense. It is therefore worthwhile to more closely examinelook at which companies use these more complex measures.

Such measures are mainly used by large firms. For instance, encryption technology is used by 60% of large firms but only 25% of micro firms. Comparing the different business sectors, it is clear that the more complex technologies tend to be in greater use among companies in the IT and financial services sectors.[28] Again, such results were to be expected, given that larger firms, and in particular those in the financial services sector, rely heavily on having a secure IT infrastructure. Given that those in the IT business have the necessary know-how, it is quite understandable that the level of complex technical measures is higher here.

3.1.3 Definition of organisational security measures

Apart from the security technologies, companies can also tighten their information security by introducing various organisational measures. The survey asked about some of the main types of such measures; the results are outlined below.

Security policy
An organisation's security policy forms the underlying concept of its information security. This policy lays down objectives with respect to the firm's approach to security, specifies the responsibilities and defines the resources that are to be made available. These issues must be clearly defined if the various units within the company are to successfully work together in information security.

Incident response
Incident response means being prepared for an information security attack. This involves the use of technical as well as organisational and legal measures. Such management aims to ensure that the IT system is restored to normal service as quickly as possible after an incident occurs.

Back-up management
Back-up management is used to protect against all forms of data loss. This entails making a copy of the data (back-up) and keeping it in a safe place. In devising a back-up management strategy, the main issues to be clarified are how often a back-up is to be made, who is to be responsible for it, what data is to be backed up (all, only the most important, or only the most recent), and how to manage the backed-up data.

Updates / vulnerability scan
Given the complexity of operating systems and all the possible applications, new security holes emerge all the time, and hackers or malware waste no time in exploiting these to the full. It is therefore particularly important to detect any such vulnerabilities as soon as possible and close

27 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), p. 5.

28 63% of respondents in finance use encryption technologies, 42% use intrusion detection, and 5% use biometrics. Among the IT companies, 57% use encryption technology, 41% intrusion detection and 5% biometrics. These companies are therefore clearly the leading users of such complex and expensive technologies.

them with programs known as patches. The responsibilities for update management must be clearly assigned to ensure that it is carried out on a regular basis.

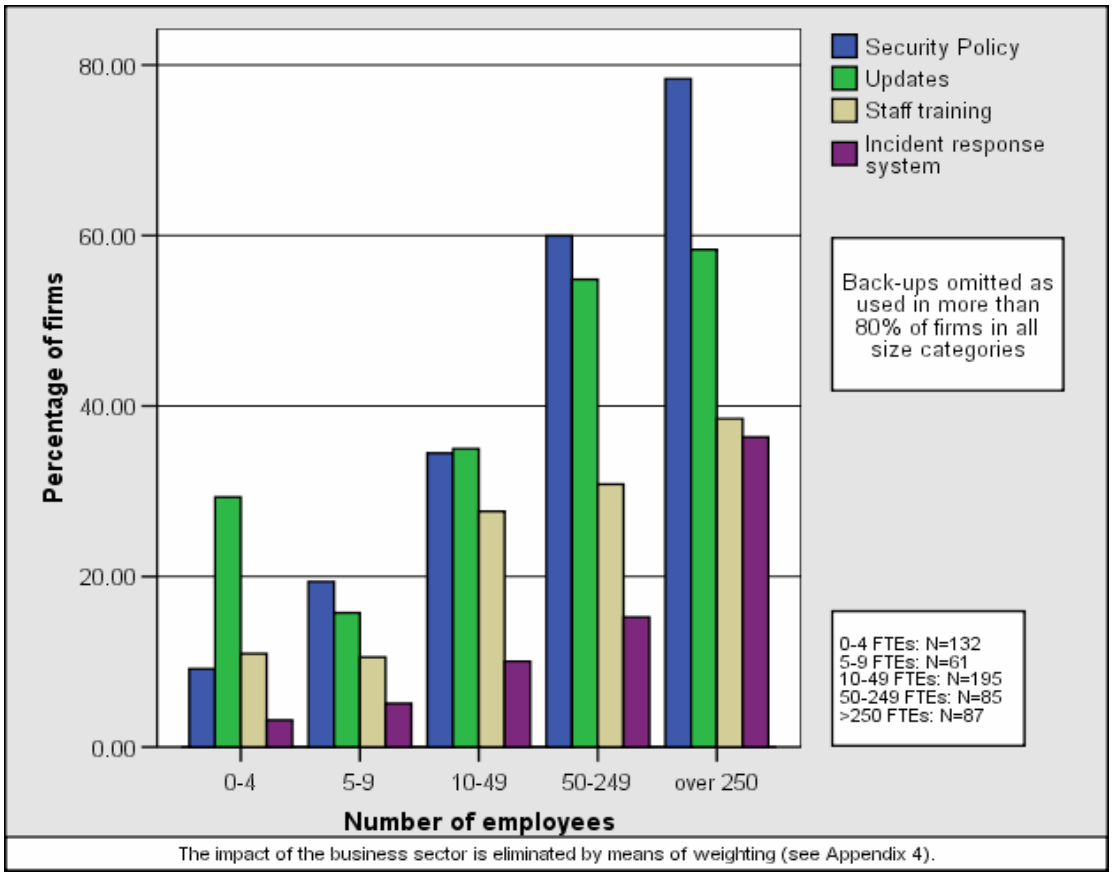
Staff training
Regular staff training in information security can help to minimise the risk of incidents by clearing up any incorrect conduct in this respect. Such training can be provided in the form of internal or external courses, or it may be limited to regular information campaigns.

3.1.4 Use of organisational security measures

Our study of the extent to which the various organisational measures are used in Swiss companies shows that the issue of most concern among respondents is back-up management. Almost all (91%) have implemented a back-up concept. The other measures are not so frequently used. 39% have a security policy, the same proportion use update management, 26% provide their staff with information security training, and 13% have an incident response system.

Here too, we sought to find out whether the measures are used to different degrees in the various companies. Figure 5 clearly shows the impact of company size.

Figure 5 Use of organisational measures by company size



We can see here that the larger firms tend to use more organisational measures than the small or medium-sized companies. Also, larger firms place more importance on assigning clear responsibilities and drawing up clear instructions for all employees. In particular, the level of incident response shows a marked increase according to the size of the company. 36% of large firms have such management. This shows that it is a lot more important for large firms than for their smaller

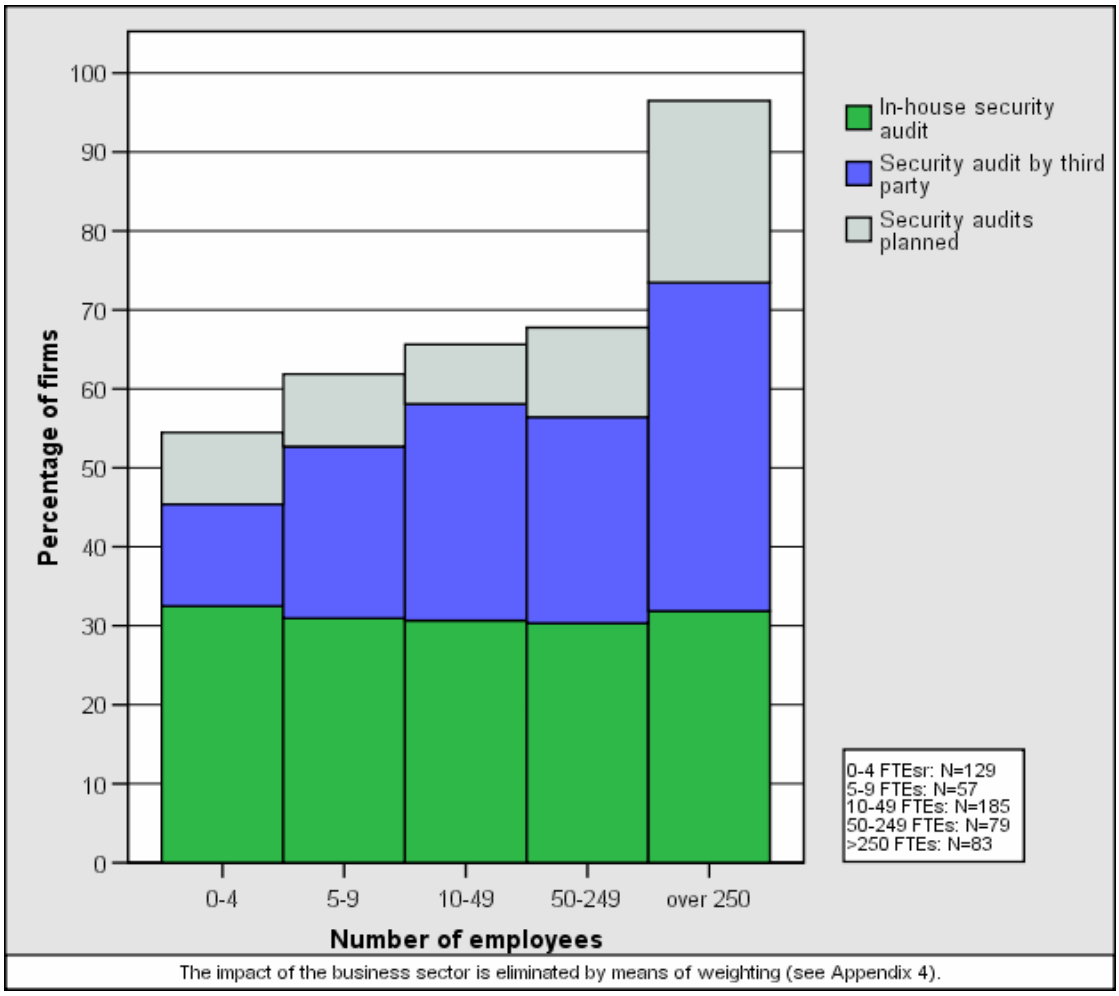
counterparts to get their IT systems up and running again after an incident. Nonetheless, a relatively large proportion of these (64%) do not use any form of incident response.

3.1.5 Monitoring of security measures

One important security aspect is the ongoing monitoring of measures that have been implemented. Only if such security measures are analysed on a regular basis can their weaknesses be rapidly detected, allowing for an early response before such weaknesses become a real problem. 56% of respondents conduct such an audit on a regular basis (32% do this in-house, with 24% calling in an external provider to check their security level). Another 11% of respondents plan to introduce such security audits in the future.[29] One-third of firms do not perform any regular audits and have no plans to do so.

A more detailed look at the results shows that the large firms are more consistent in monitoring their security measures. As Figure 6 shows, 72% of large firms already conduct security audits and another 13% have plans to do so.

Figure 6 Security audits by company size



29 After weighting of these results by size and sector (see Appendix 3), the proportion of Swiss firms that conduct a security audit can be estimated at 47%, with another 8% planning to introduce a regular security audit in the future.

The high proportion of large firms that conduct a security audit is in stark contrast to the rather low level of SMEs. The large firms are obviously aware of the importance of such ongoing monitoring and/or have the necessary resources to do so.

These results correspond to those of the "Hi-Tech Crime" study. This survey of UK companies with over 100 employees showed that 33% did not carry out any security audits whatsoever.[30] Thus, when it comes to security audits, large firms in Switzerland are comparable to those in the UK (28% of large companies in Switzerland do not yet audit their security measures).

3.2 The costs associated with information security breaches

Some of the measures described above are quite expensive to implement. And, as the threats are constantly changing, organisations have to adapt their technical and organisational measures on a regular basis. On top of that, employees have to be made available and trained in the use of such measures. Naturally enough, companies try to keep their costs in information security as low as possible. Thus, the budget they actually devote to information security is a good indication of how important it is to them. The same goes for the human resources they devote to information security, although this relates to not only the number of staff but also the degree of training of those responsible for information security.

3.2.1 Financial resources allocated to information security

Very few organisations can place a precise figure on the amount of money they actually spend on information security; for this reason, the questionnaire divided the spending budget into four bands (CHF 0 to 5,000; CHF 5,001 to 20,000; CHF 20,001 to 100,000; over CHF 100,000). The responses show that many companies devote only limited financial resources to safeguarding their information security. 62% of respondents said they spend less than CHF 5,000 for this purpose. Only 5% spend more than CHF 100,000. A more detailed analysis distinguishes the firm type and the level of investment in risk management.

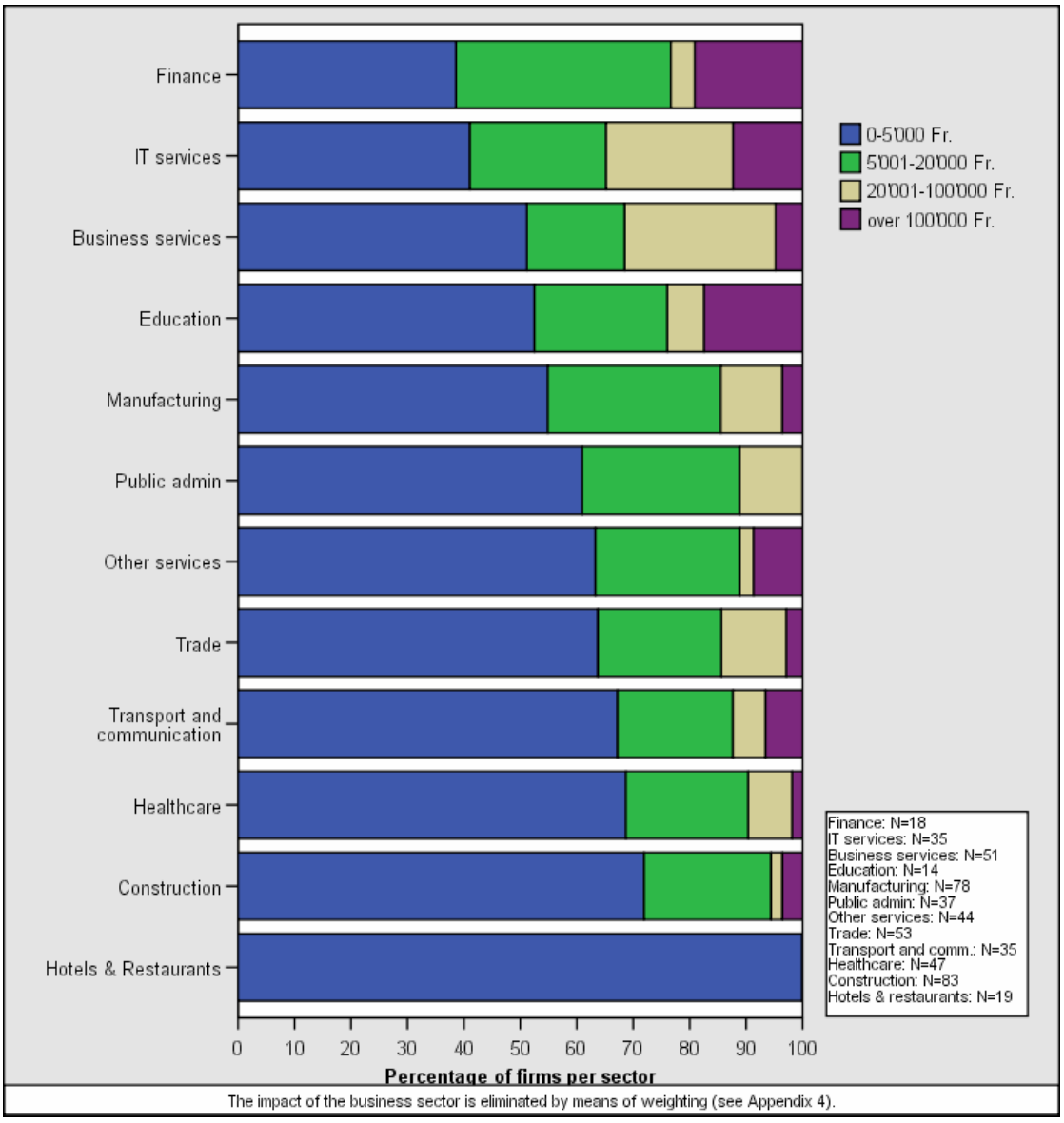
The close relationship between a company's size and its spending in this respect is hardly surprising: the bigger the company, the more it invests in risk management.[31] With bigger budgets, the larger companies have more resources to devote to information security. Of course, this additional spending is justified; as shown in the previous chapter, large firms face far more incidents than SMEs.

Apart from company size, the business in which a company operates can also influence its financial commitment to information security. In studying the frequency by business sector, we have already mentioned that the only reason why companies in the financial services sector have as few recorded incidents as hotels and restaurants is because of their better protective measures. Banks and other companies operating in finance usually place much more importance on data protection than hotels and restaurants. Figure 7 shows the information security spending of companies in the different sectors.

30 National Hi-Tech Crime Unit (NHTCU), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005), p. 29.

31 The close relationship between company size and prevention costs can be expressed with the correlation coefficient Gamma. Gamma can be between 0 and 1 for a positive correlation (the higher the number, the more spent). The relationship in question works out at a high 0.791.

Figure 7 Financial resources allocated to information security by business sector



As expected, substantial differences exist between the various sectors. Companies in the two sectors mentioned above form the upper and lower extremes: no hotel or restaurant spends more than CHF 5,000 on information security, while 19% of financial services providers invest more than CHF 100,000. Thus, as a rule, we can say that companies in those sectors that place less importance on IT also invest less in information security.

3.2.2 Human resources allocated to information security

The survey asked the organisations two questions about their information security staff. First, they were asked to specify the number of FTEs devoted to this area,[32] and then to indicate the level of qualifications of the person in charge of the information security team.

The answers to the questions about the size of the information security team show that most companies have only a small number of staff allocated to this issue. At 13% of the respondents,

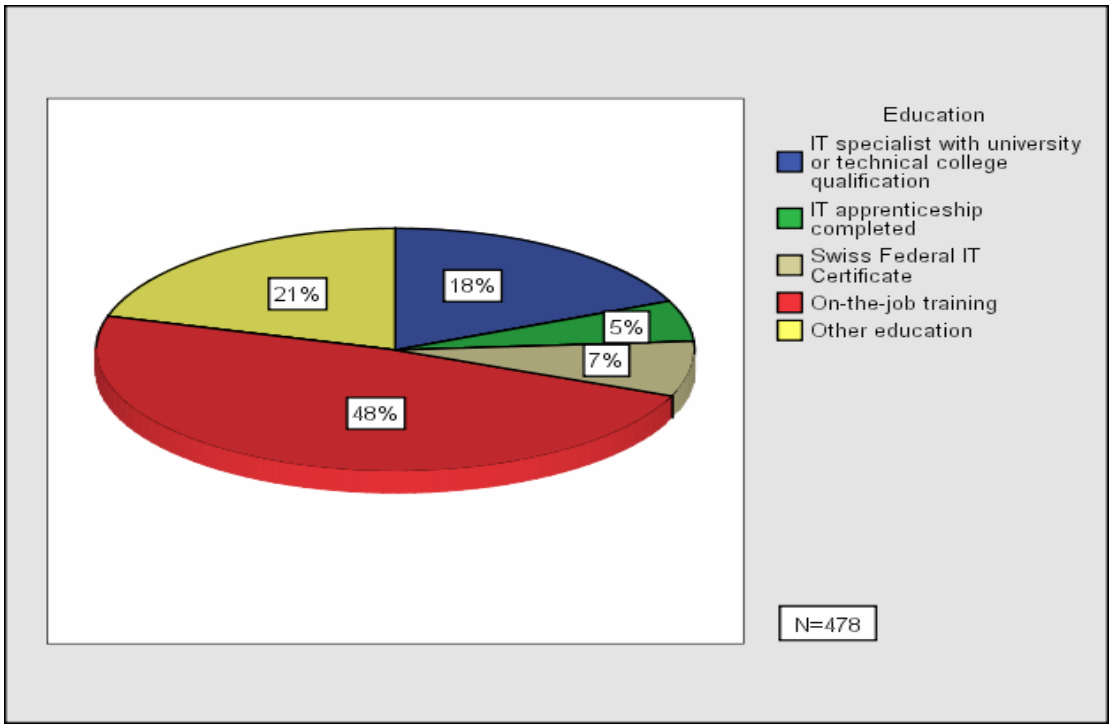
32 Once again, for the sake of simplicity, a range of bands was given to choose from: none; 0-1; 2-5; 6-10; over 10.

no particular individual is responsible for information security. Another 60% said they had no more than one FTE available for information security. Just under one-quarter of respondents (24%) employ small teams of 2-5 people, and very few (3%) devote more than five people to this task.[33] Thus, information security is seldom defined as a separate role in corporate HR policies. Often, this is due to a lack of financial resources, but sometimes companies opt for more flexible solutions (such as external consulting and outsourcing) than having a dedicated team on the payroll.

As with the financial resources, the level of human resources also increases according to company size.[34] Again, this can be attributed to the fact that larger firms have more human and financial resources at their disposal. However, the availability of more financial resources does not necessarily lead to more human resources. When we look at the staffing levels by sector, we see that, although companies operating in the financial services sector invest more money in information security, they devote relatively little staff to such concerns.[35] It is clear from this that certain sectors are more likely to use outsourcing solutions. We will talk about this in greater detail later chapters.

First, let us look at the level of qualifications of those responsible for information security. When it comes to ensuring effective protection, this factor can be just as important as the team size. However, specialists are expensive to hire and not very flexible within the company, which is why not every company can afford a specialist.

Figure 8 Qualifications of those responsible for information security



33 When making an estimate for all companies in Switzerland, it must be remembered that large firms and certain sectors are overrepresented among the respondents. After weighting (see Appendix 3), we can estimate that 22% of companies in Switzerland do not have anyone specifically devoted to information security and 68% have one FTE at most.

34 Once again, the relationship can be expressed using the correlation coefficient Gamma (see footnote 31). Gamma is 0.588 in this case.

35 As shown in Figure 7, financial services providers devote the highest budget to risk management. However, fewer than half of these companies employee more than two people in information security.

Figure 8 shows that less than one-in-three firms has a qualified IT specialist dedicated to information security. On closer inspection, it is clear that this proportion is likely to be even lower in reality. Large firms and IT companies employ a much higher percentage of qualified IT specialists. When we consider that the larger firms are overrepresented in the sample pool, the level of IT experts devoted to information security in Swiss firms is more likely to be around just 15%.[36]

Such a low proportion of formally qualified experts may become problematic as the threats become increasingly complex. Switzerland is no exception in this case, with the UK "Hi-Tech Crime" study also finding a lack of IT staff with formal security qualifications.[37]

To conclude, therefore, with respect to staffing levels in information security, most firms have only a few employees specifically allocated to this task, and only a minority of firms assign the principal responsibility for this to an IT specialist.

3.3 Outsourcing of the risk

As shown, some firms invest relatively large sums of money in information security but employ only a few members of staff for this purpose. It is clear that these companies hire external consultants, who offer a more flexible means of meeting their information security requirements. Outsourcing is not all without risk, however. As IT protection is, in many respects, a management issue as much as it is a question of security technology, a significant proportion of the tasks involved in information security are kept within the company itself. Apart from that, using specialists from outsourcing partners is a relatively expensive option.

Therefore, each company must decide for itself whether it makes more sense for it to outsource the task or form its own security information security team. As many companies see outsourcing as an important addition to their own security measures, the extent to which it is used is examined below. Following this, we look at whether companies are insuring themselves against the damage that might be incurred in such an incident. Taking out insurance is another way of outsourcing the risk, with any financial losses being borne by the insurance company.

3.3.1 The extent of outsourcing

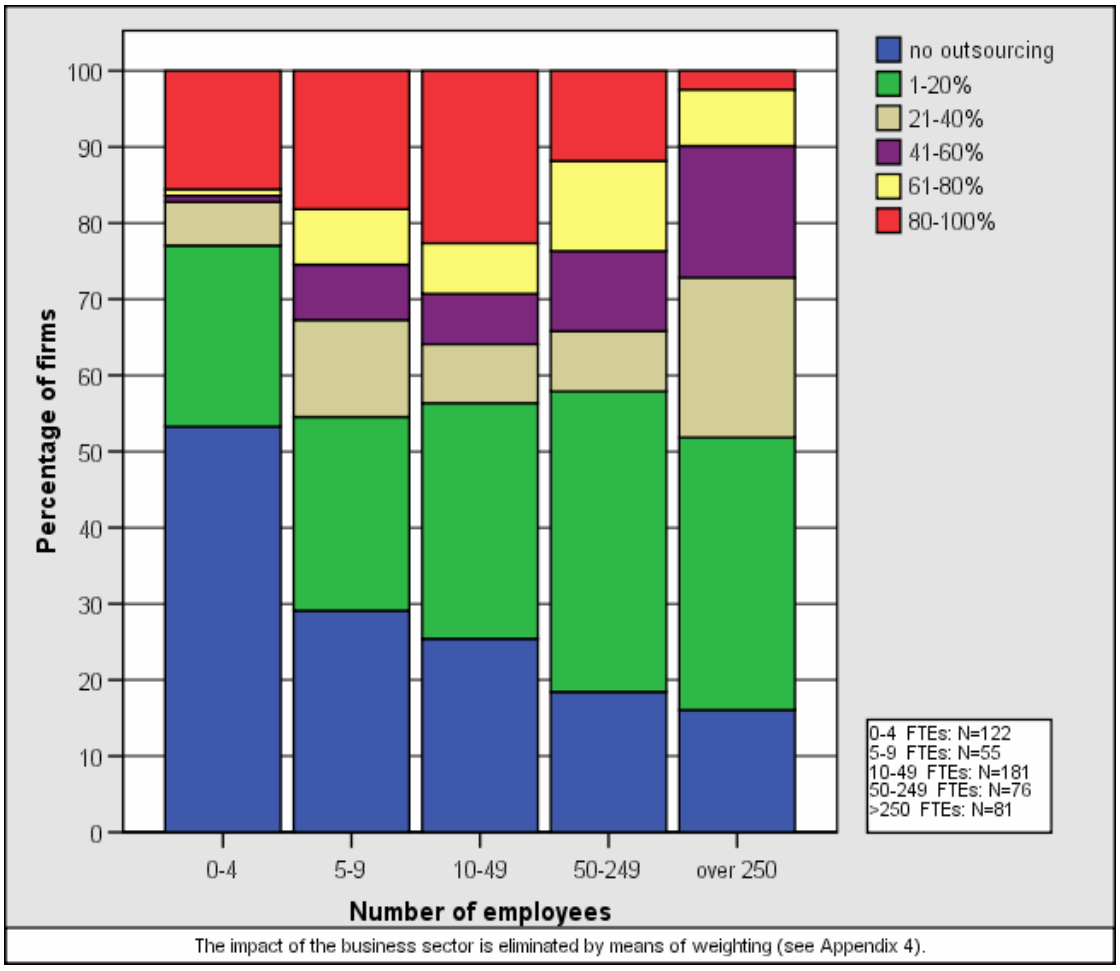
To examine the importance of outsourcing in information security in Switzerland, the participants were asked to state what percentage of their information security budget is used to pay their outsourcing partners.

30% of respondents said they did not use any outsourcing. Another 31% outsource up to 20% of their information security budget. Thus, more than half of the respondents delegate only a small proportion of their information security to specialists, with another 15% spending more than 80% of their information security budget on fees paid to outsourcing partners. The differences between the companies are enormous, making it even more interesting to examine which companies tend to favour outsourcing solutions. Figure 9 shows the extent of outsourcing by company size.

36 This is the estimate after weighting (see Appendix 3).

37 National Hi-Tech Crime Unit (NHTCU), *Hi-Tech Crime: The Impact on UK Business 2005* (2005), p. 30.

Figure 9 Outsourcing by company size



The micro firms with fewer than five employees seldom use outsourcing to any great extent. More than half of these firms take charge of their information security needs themselves. Probably, outsourcing is too costly a solution for such companies. The situation is quite different for the SMEs, which outsource a large proportion of their information security. More than one in five companies with 10-49 people outsource at least 80% of their budget earmarked for IT security. Some of these medium-sized companies rely heavily on IT but do not have the in-house capabilities to ensure security. Meanwhile, the large firms often use outsourcing partners but rarely delegate more than 60% of their information security (only 10% of large firms do).

Looking now at the extent of outsourcing by business sector, it is clear that banks and financial services providers, which spend a lot on information security and employ only a few people for this task, make above-average use of outsourcing. Clearly, IT companies themselves rarely call upon outsourcing partners for information security, given that they have the necessary know-how in-house.[38]

There are no comparable international studies available to determine whether Swiss companies' use of outsourcing can be said to be high or low. Compared with the annual "CSI/FBI Computer Crime and Security Survey 2005," Switzerland does appear to use a high level of out-

38 Only 9% of IT firms spend more than 40% of their information security costs on outsourcing.

sourcing. However, given the specific composition of the survey pool in the FBI study, the results cannot be directly compared.[39]

3.3.2 Insurance coverage

Insurance coverage represents a special case of outsourcing, whereby any costs or damages incurred through information security breaches are outsourced to a third-party. Insurance policies to cover Internet risks have been available in Switzerland since 2000.[40] The survey results show that these are rapidly gaining ground: 45% of respondents said they had purchased insurance against possible damage to their IT infrastructure. On this basis, we can estimate that around one-third of all companies in Switzerland make use of such insurance.[41]

Insurance is most popular among the medium-sized companies with 50-249 employees, of which 69% have purchased insurance to cover such risks. The figure is lower for micro firms (29%) and also lower for the large firms (54%). Public administrations were most frequently insured, followed by financial services providers and business services providers.

Among those firms that chose not to take out such insurance, cost was the main deciding factor. More than half (55%) said that such insurance would not make economic sense for them. Still, 29% were not aware that such insurance policies even existed. 15% said that they did not have the financial means for such insurance, and another 8% (especially large firms) thought the range on offer from insurance companies was insufficient.[42]

Once again, no international comparable data is available with respect to insuring such risks. However, even without comparable data, it is clear that such levels are surprisingly high. Although this insurance has only been available for a few years now, numerous firms have already taken out such a policy.

3.4 Conclusion on risk management by companies

Risk management can come in many different forms. The most basic security measures (anti-virus software, firewalls, back-up management) are found in almost all firms. For certain companies, particularly the smaller ones, these precautions are quite sufficient. Others, however, have higher security requirements, which they meet either themselves, with additional technical and organisational measures, or by outsourcing the task to third parties. Given that there are many ways of implementing risk management, some of which are extremely company-specific, the overall quality cannot be evaluated for Swiss companies as a whole. Neither is it possible to determine how such measures may impact the probability of a security breach. This is because those companies that have taken the most measures are also the ones that run a higher risk of incurring such an incident. There is also the fact that some of these incidents would go undetected without the existence of the security measures.

39 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 Computer Crime and Security Survey* (2005), p. 9. The participants of the FBI/CSI survey are members of the Computer Security Institute (CSI). It can therefore be assumed that their in-house efforts in information security are above average. Furthermore, that survey concentrated primarily on large firms.

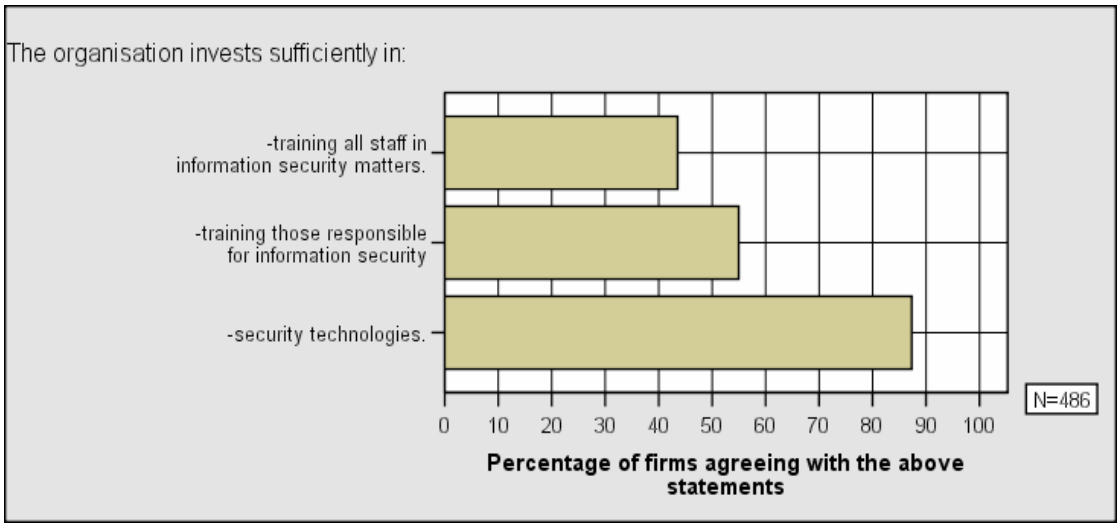
40 Haldemann, Lukas, V*ersicherung von Internet-Risiken* Term Paper submitted to the IT department ETH Zurich, 2001), p. 5.

41 Once again, this estimate is derived from weighting the survey data by company size and business sector (see Appendix 3).

42 More than one answer was possible for this question.

In any case, the organisations themselves appear to be satisfied with the measures they have taken. 87% believe that their company invests sufficiently in security technology. As Figure 10 shows, however, the level of satisfaction with security awareness training is by no means as high: only a slim majority are satisfied with their company's commitment in terms of training for those responsible for information security, and only a minority believe that enough is being invested in training general users within the company.

Figure 10 Assessment of company's own investment in information security



Of course, the firms' level of satisfaction with their own investment is not really any clear indication of the actual quality of risk management. Nonetheless, it is clear that many companies acknowledge that information security is not only a technical issue but one that also requires investment in terms of staff training.[43]

Thus, even if the quality of risk management cannot be accurately determined, we would like to conclude this chapter with a number of important points:

Swiss companies outsource a relatively high proportion of their information security (especially medium-sized companies). One reason for this is that information security is usually only allocated a low number of FTEs, and even these are often not qualified IT specialists. Medium-sized companies, in particular, cannot afford to implement all the measures that would be necessary. Given the scarcity of resources and the assumption that many of those responsible for information security need further training, the question is whether these companies would be interested in joint action in information security.

43 These results correspond with a KPMG survey of selected CIOs (Chief Information Officers) on how satisfied they were with their company's IT security. That survey also found a high level of satisfaction with the technical aspects but little satisfaction with the level of security awareness among the end-users. KPMG, *IT-Management 2005* (Zurich and Geneva, 2005), p. 26.

4 External help and joint action

The previous chapters have highlighted the importance of information security for many organisations. Most companies are increasingly confronted with incidents that threaten to compromise the security of their IT systems. Often they rely on external help when it comes to dealing with such incidents. Therefore, this chapter begins by looking at how often companies seek external help and where they find it.

Firms are often stretched beyond their own limits, not only in coping with such incidents but also in terms of risk management. An effective and efficient IT protection system is expensive to install and requires constant updating. With so many companies facing similar problems of this nature, it may make sense for them to share their experiences among each other. We therefore wanted to find out which companies would be interested in such joint efforts, who could possibly coordinate this, and how it should be funded. We also take a closer look at the role of the State and the contribution it could make to support the private sector in this respect.

4.1 External help in the case of an incident

One only need look at the proportion of firms using outsourcing partners to realise that Swiss companies often rely on the expertise of other providers for their risk management. This is particularly so whenever an incident occurs that threatens to compromise information security. However, some firms may be reluctant to seek outside assistance for fear of disclosing confidential in-house information or tarnishing the company's reputation. The question is therefore: do firms actually look for outside help when facing information security problems? And if so, from whom do they seek it?

The survey results show that 63% of organisations that have experienced such a security incident have actually sought external help.[44] Small companies with 10 to 49 employees are the most likely to seek external help. This corresponds to our previous finding that companies in this size category are most likely to use outsourcing. When we look at the extent by business sector, it is clear that the respondents in the public sector very often seek external help (75%), while IT companies, as to be expected, require far less additional support (36%).

It is also interesting to find out where companies find the help they are looking for. Most firms turn to their own outsourcing partners, software vendors or Internet provider. However, 40% said that they contact their counterparts in other firms and 25% get help online.

Thus, companies do not always choose to pay for help from the experts, often seeking instead an opportunity for mutual support. We now take a closer look at some of the possible forms of such joint action between companies.

4.2 Joint action between companies

A number of issues must be clarified in order to find out the type of joint action that might make sense for companies. First, we need to know what types of cooperation the firms themselves

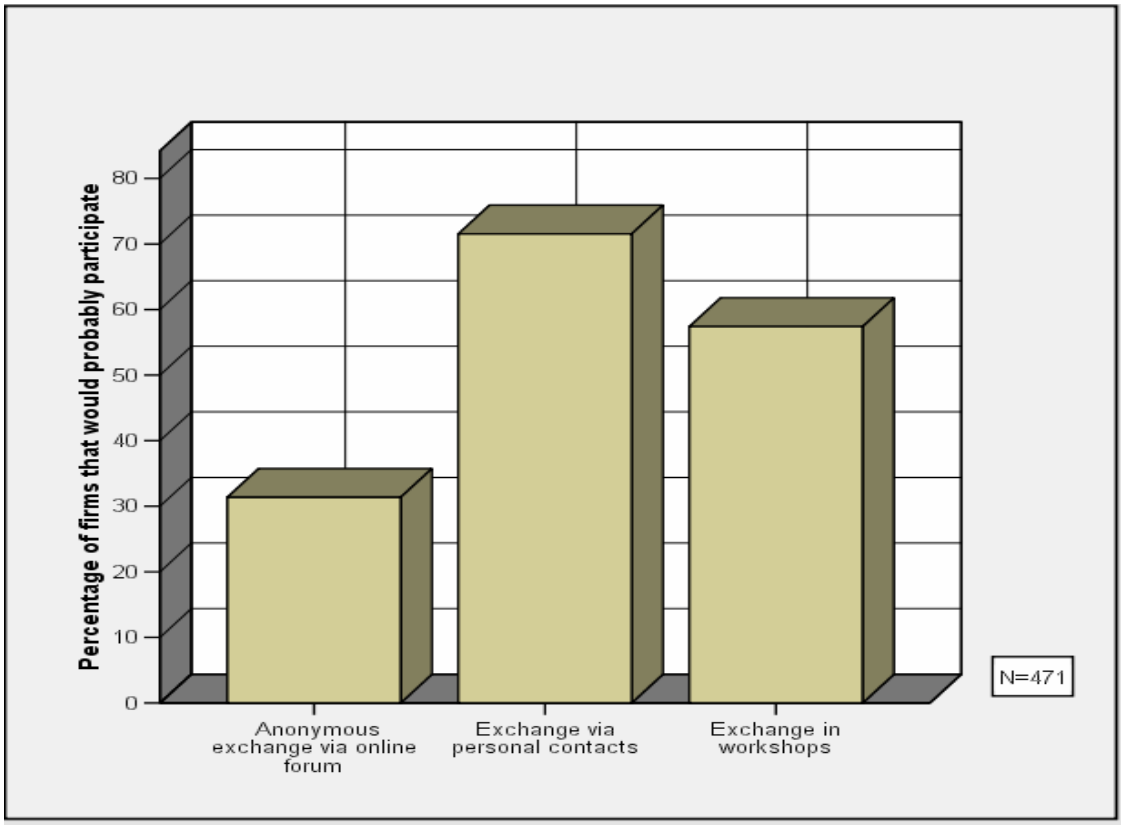
44 Once again, this result cannot be extrapolated to apply to all Swiss companies due to the fact that the respondents did not represent a proportional cross-section of all firms. Using the weighting procedure (Appendix 3), however, we can estimate that around half (47%) of Swiss firms that encounter such an incident choose to seek external help.

would be interested in joining. Then, there is the question of who could coordinate such joint action and whether firms are prepared to pay for this service.

4.2.1 Possible forms of joint action

To get an idea of the ways in which firms would be prepared to work together, the survey participants were asked which forms of joint action they would be interested in. The choices given were: anonymous exchange via an online forum, personal contacts, or workshops. Figure 11 illustrates the answers received to this question.

Figure 11 Willingness to participate in different forms of joint action



The most popular result was exchange via personal contacts, in which a clear majority would participate. The workshop idea was also quite popular.[45] The substantial interest in the sharing of ideas among colleagues is worth noting. Obviously, those responsible for information security realise that many firms are experiencing the same sort of problems and could benefit from each other's experience. Around one-third of respondents (31%) could envisage discussing issues of information security online.

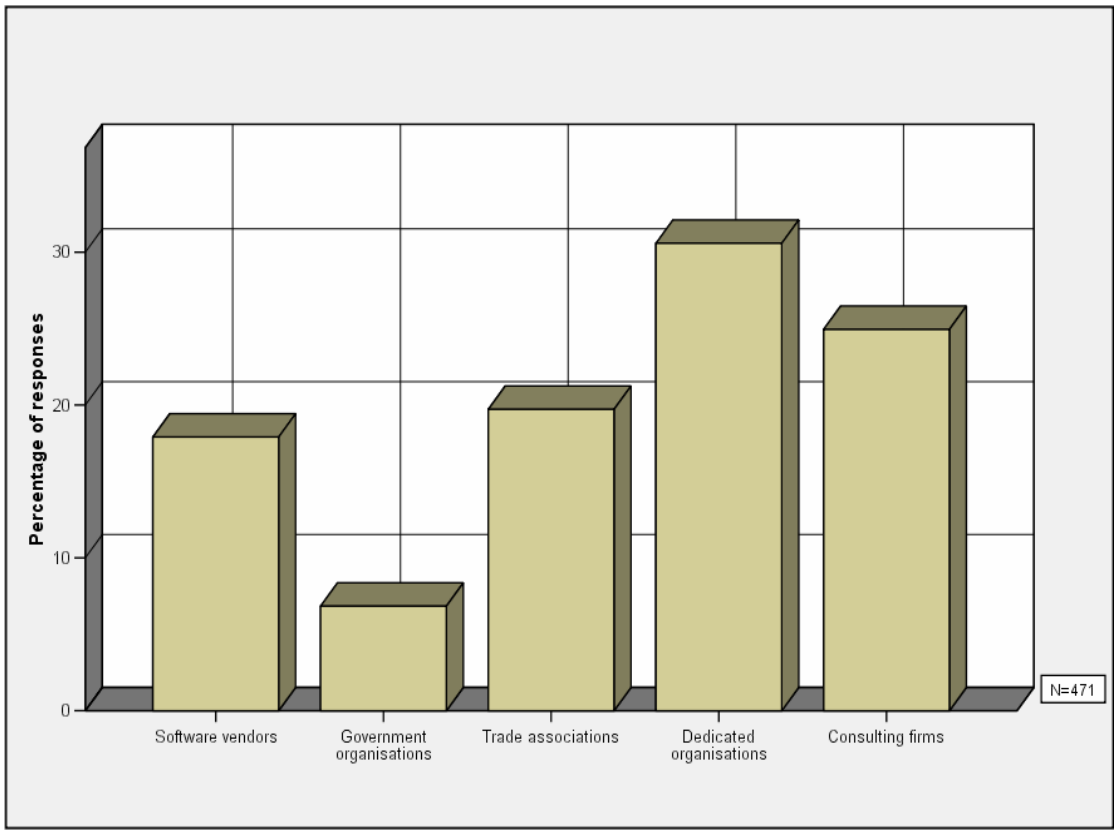
The need for joint action is evident. It is thus important to know who could coordinate this and whether participating firms would be prepared to offer financial support to such an organisation.

45 A distinction was made between workshops held by software vendors and workshops conducted by independent third parties. 41% said they would be prepared to participate in workshops by software vendors, while 50% would attend the independent workshops. The chart shows all organisations in favour of one or the other option.

4.2.2 Organising joint action

Even if there is no shortage of firms interested in such joint action, someone has to be prepared to take on the task of organising it. The participants were thus asked who, in their opinion, would be best suited to coordinate inter-company joint action in the manner of a centre of excellence. The possible answers were: software vendors, government-run organisations, trade associations, consulting firms, or dedicated organisations. Figure 12 shows the respondents' preferred options.

Figure 12 Possible organisers of inter-company joint action



It is clear that over 30% of firms believe that any joint action would be best coordinated by organisations specially created to serve this purpose. The structure of such dedicated organisations remains to be defined.

25% of respondents thought consulting firms should manage such joint action. Software vendors (18%) were probably also mentioned as they already work together with many companies. Trade associations were also quite popular (20%). The advantage of these is that they already have experience in the coordination and organisation of cooperative efforts.

The smaller firms tended to favour software vendors and consulting outfits, while more of the medium and large firms opted for trade associations and, in particular, organisations specially created for this purpose.[46] It is likely that smaller firms are more interested in consulting as a form of knowledge transfer. Medium and large firms, however, tend to seek joint action on the basis of mutual exchange.

46 29% of the small and micro firms with fewer than 10 employees chose software vendors to organise joint action, while 28% of these companies see consulting firms as the best option. 43% of large firms see dedicated organisations as necessary.

The findings also show that the direct consulting and coordination of joint action is not a job for the State. The next section goes into more detail about the role of the State. Before that, however, we look at whether companies would be prepared to contribute financially to the organisation of such joint action.

4.2.3 Funding joint action

The question as to how any joint action should be funded was formulated in a very general manner. Participants were asked whether they could envisage spending up to CHF 500 or up to CHF 2,000 a year on an organisation that provides advice and coordinates joint action in information security. The findings should give an indication of the respondents' willingness to contribute to the costs incurred in setting up such joint action.

As the wording was quite vague and some of the respondents were not in a position to decide on their company's financial commitments, a very high 36% of respondents did not answer this question. Of those who did answer it, 71% said that they would not be prepared to contribute financially; 22% said they would contribute up to CHF 500 and 8% up to CHF 2,000. It was mainly the large firms that were prepared to make such a contribution: a modest financial investment in such cooperation would not eat substantially into their generous budgets. 55% of large firms would be prepared to make a financial contribution. Among the micro firms, however, only 15% could imagine paying up to CHF 500.

It is hardly surprising that such an overwhelming majority rejected a financial contribution, given that most firms' budgets for information security are already quite stretched. Nonetheless, more than half of the large firms and one-third of medium-sized firms with 50 to 249 employees would be prepared to participate in the costs of setting up and running an organisation for joint action in information security. This once again confirms the need among medium and large firms for closer cooperation in information security.

4.3 Cooperation with the State

Considering that information security is an issue facing the entire economy, the question arises as to whether and how the State could or should support companies in taking protective measures.

The State is traditionally responsible for safeguarding various forms of infrastructure of central importance to the wellbeing of the population. Given that such wellbeing in our modern society relies heavily on the functioning of information and communication technology, the protection of information infrastructures has become an important task for the State. This task, referred to internationally as Critical Information Infrastructure Protection (CIIP),[47] can only be fulfilled by the State in cooperation with the private sector. It is therefore in the State's interest to cooperate with companies and to help them protect their IT systems. However, unlike the private sector, the State takes a more long-term view that extends beyond the issue of business continuity.

Given this different outlook, among other things, the question remains as to whether firms actually want to join forces with the State. As we have already seen, only very few firms view the State as the best player to coordinate inter-company cooperation. Thus, the role of the State is

47 Further details on Critical Information Infrastructure Protection can be found in: Abele-Wigert, Isabelle and Myriam Dunn, *The International Critical Information Infrastructure Handbook 2006* (Zurich, 2006).

viewed rather critically by the private sector. On this basis, it is important to find out how intensively companies have already been working together with the State.

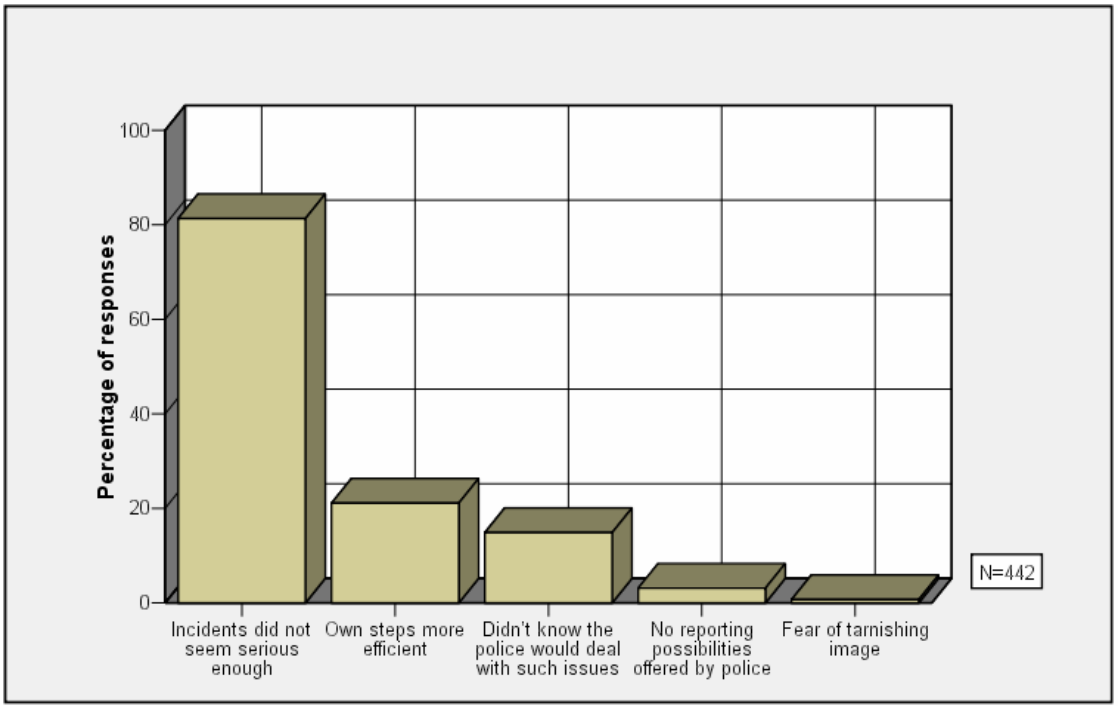
4.3.1 The role of the police

Whenever private individuals or companies fall victim to fraud or theft, they normally turn to the police. The State is responsible for protecting us from attacks on our property. But do companies also involve the police when it comes to IT attacks or data theft?

The survey asked whether firms had ever called in the police for an incident concerning information security. The results are unambiguous: only 34 of the 562 respondents (6%) said they had. Fifteen of these 34 are large companies. An international comparison confirms that firms very rarely involve the police for information security breaches. The FBI's "Computer Crime Survey" found that only 9.1% of US firms turn to the law enforcement agencies in such cases.

Of course, it is interesting to know why these figures are so low. Therefore, the survey also asked why the police had not been contacted. Figure 13 shows the frequency with which the various reasons were given (more than one answer was possible).

Figure 13 Reasons why the police were not involved



It is clear that many companies believe such incidents are not sufficiently serious to warrant filing an official complaint. Many see malware as everyday occurrences in the business world and therefore not worth reporting. Again, it is hardly surprising that one-in-five companies believes that its own measures are more efficient. The conduct of the police was less of a deciding factor. Only a small number of respondents said they did not report the incident because they thought the police would not be interested in such cases or did not offer any means of reporting such cases. It is also worth noting that the fear of tarnishing the corporate image did not prevent many firms from reporting such an incident.

Once again, these results are comparable with those found in the FBI's "Computer Crime Survey." Here too, the main reason why companies do not involve the police was that the incident was not regarded as being serious enough.[48]

4.3.2 MELANI

Thus, it would appear that companies see very little reason for police intervention. Indeed, many of the issues faced in information security could not even be solved by the conventional criminal authorities. This is why the State is now looking for alternative ways of supporting the economy in this respect. This was the basis for founding MELANI (Melde- und Analysestelle Informationssicherung), a reporting and analysis centre for information security. Working together with organisations in both the public and private sectors, MELANI strives to detect new risks and threats as early as possible and offer companies the possibility of reporting incidents.[49] MELANI became operational on 1 October 2004. Information on the current threat situation and warnings of new threats are regularly posted on the MELANI website.[50] Of course, this information is only of use if companies actually act upon it. It was therefore very important to find out how well MELANI is known among firms after just over one year of operation.

10% of respondents said they had heard of MELANI. It should be noted that MELANI works in close collaboration with certain large operators of critical infrastructures, but these did not participate in the survey.

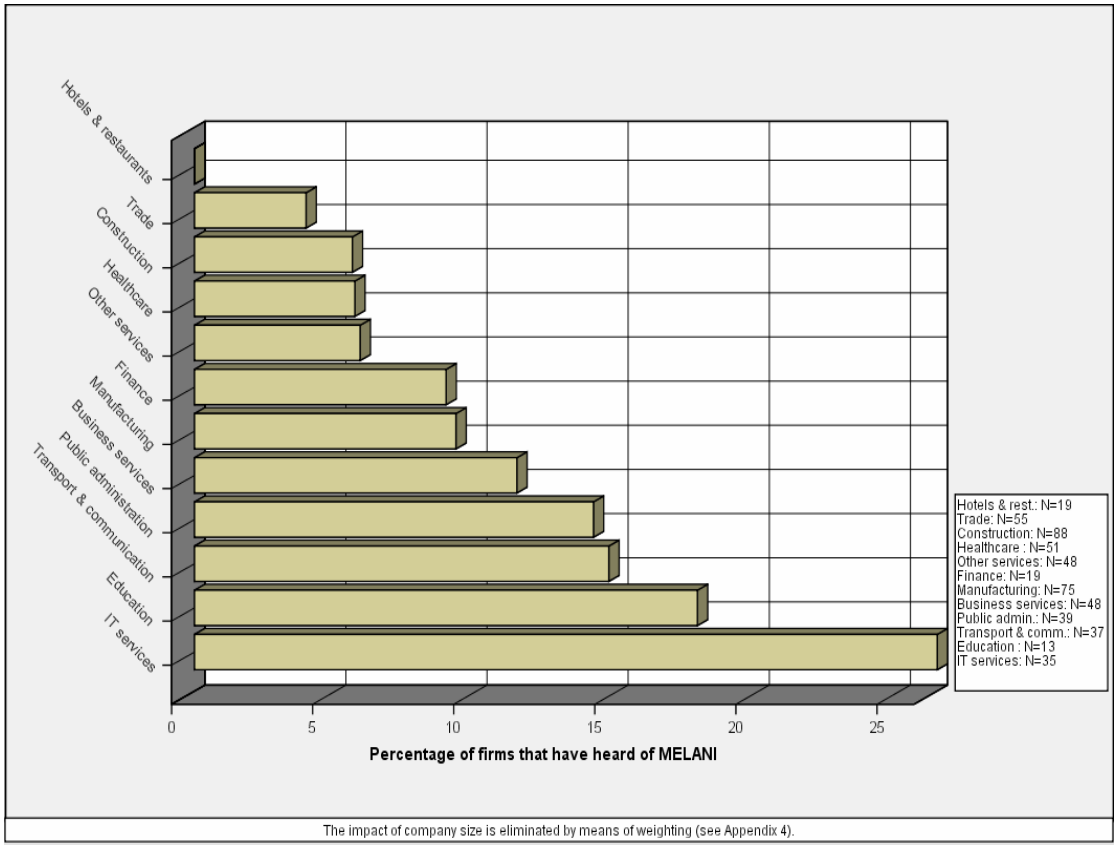
The proportion of firms familiar with MELANI increased according to company size. While only 4% of micro firms with fewer than five employees had heard of MELANI, the recognition level among large firms was 28%. As shown in Figure 14, considerable differences also exist among the different business sectors.

48 Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005), p. 12.

49 The leading partners are the FSUIT (the Federal Strategy Unit for IT), the Service for Analysis and Prevention of the Federal Office of Police, and the Computer Emergency Response Team from the Switch foundation (www.switch.ch).

50 www.melani.admin.ch

Figure 14 Recognition of MELANI by sector



IT companies were, by far, the most familiar with MELANI. Thus, in the first year of its existence, MELANI has become relatively well-known among companies that take a particular interest in information security (i.e. large firms and IT companies).

Given the wide range of information security problems in terms of both quality and quantity, depending on company size and the business sector, it is not easy for MELANI to cover all needs. Large firms need customised consulting from experts, whereas medium-sized companies are more interested in general tips and advice. The final chapter of this study now looks at some possible solutions to this problem.

5 Conclusion

The objective of this study was to provide an overview of the IT threats facing Swiss organisations and the security measures in place to deal with these. Our findings have shown that information security threats are widespread and that risk management is an important topic for all firms. However, it also became clear that substantial differences exist among the various organisations. This last chapter discusses the consequences of our findings.

5.1 Different threats – different risk management – different needs

The first main finding of the study is that the threats to information security can affect different companies to very different extents. The business sector in which a company operates does play a role, but the size of the company appears to be of more significance. Whereas small and medium-sized companies are particularly affected by malware, one in five large companies suffered a targeted attack on its IT infrastructure in 2005. Thus, in evaluating these results, a distinction must be made between large companies, SMEs and micro firms.

5.1.1 Micro firms

Micro firms with fewer than five employees are the least likely to be affected by information security threats. Such businesses are often less dependent on IT than larger firms, and they tend not to be of much interest to hackers. For this reason, they concentrate more on basic protection, with no great need for complicated security technologies or organisational measures. We can therefore assume that micro firms are relatively independent in terms of information security and can implement the required measures themselves. Nonetheless, practical recommendations, possibly with some training, would probably also prove useful in micro firms, given that few of them actually employ IT experts.

5.1.2 SMEs

Unlike in the micro firms, IT is a decisive factor in company organisation in SMEs. SMEs often depend on an up-and-running IT infrastructure. This, of course, also raises the security requirements for such firms. Technical protection against malware is simply not enough: these companies need to draw up directives and train their staff. However, SMEs are usually still too small to hire their own IT security experts. Hardly surprisingly, SMEs are the most interested in getting support against computer-related crime. They work the most with outsourcing partners, take out the most insurance in this respect and often are more likely than others to seek external help when an incident is detected. As many SMEs do not have a dedicated IT expert, yet still have to use some complex security measures, such companies would have a lot to gain from additional training and courses and an online forum for sharing experiences.

5.1.3 Large companies

The needs of large companies are different again. As they face the greatest IT threats, they have to turn to much more complex security measures. They invest more financial and human resources

in the problem, use more complex security technologies and often implement security directives. Nonetheless, given the more frequent targeted attacks on them, they also face more complex threats. Hackers are always quick to adapt their methods, so any organisation trying to outwit them has to keep up to date. Even in-house experts and IT teams are very quickly stretched to limits.

For this reason, large firms are particularly interested in specific expert consulting. They are not interested in general information security issues but the concrete implementation of highly complex and technically demanding security measures. Moreover, such firms often work in a network with mutual dependencies. Therefore, alongside consulting, there is a need to organise and promote joint action and mutual exchange. Working together with the police can also be an important issue for large firms in combating cybercrime.

Hence, the interests of large companies differ considerably from those of smaller and medium-sized companies. However, their requirements in terms of specific consulting and joint action have been recognised for longer and these have been addressed by offering close collaboration with MELANI. Given the high costs involved in terms of financial and human resources, however, such intensive cooperation can only be offered to a relatively small number of large companies.

5.2 Joint action despite different needs: Warning, Advice and Reporting Points (WARPs) as a possible solution

A second important finding to come out of the survey is the fact that Swiss companies would like to work in closer cooperation in combating computer-related crime. Many firms are facing the same difficulties and would benefit from an opportunity to share information. The problem with implementing this form of joint action is that, as we have seen, the different companies have different needs.

One possible solution to this problem is the creation of Warning, Advice and Reporting Points (WARPs). The National Infrastructure Security Co-ordination Centre (NISCC) set up by the UK government supports WARPs as an ideal platform for exchange and cooperation in information security.[51] Members of WARPs share information with each other, facing information security threats as a group. New threats are thus detected earlier and possible solutions made available to all members. The main point is that WARPs can be formed of companies operating in the same sector or the same region or of similar sizes, as required. Companies facing similar problems and with similar requirements can thus cooperate within such WARPs. The study shows that company size should be a major criterion in the formation of WARPs. For instance, large firms are more interested in specific consulting among experts, whereas SMEs have a greater need for general consulting and information sharing. WARPs may be of particular use to medium-sized companies, improving their information security through joint action, without raising the costs.

The State could provide the impetus for such WARPs and coordinate these in the early stages. In fact, when it comes to setting up WARPs, State support would appear to be necessary, given that firms tend to participate in such organisations only when they have proven their use. Coordination among the various WARPs would also be important, taking advantage of their areas of overlap. Thus, while companies concentrate on protecting their business in specialised WARPs,

51 http://www.niscc.gov.uk/niscc/warpInfo-en.html

the State, in coordinating such organisations, could help to safeguard the economy as a whole, a central objective of its security policy.

6 Bibliography

Abele-Wigert, Isabelle and Myriam Dunn, *The International Critical Information Infrastructure Protection (CIIP) Handbook 2006. An Inventory and Analysis of Protection Policies in Twenty Countries* (Zurich, 2006).

Bidgoli, Hossein et al. (eds.), *Handbook of Information Security Volume 1-3* (Hoboken, 2006).

BSI – German Federal Office for Information Security, *The IT-Security Situation in Germany in 2005* (July 2005). http://www.bsi.bund.de/english/publications/securitysituation/lagebericht2005_englisch.pdf

Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI), *2005 CSI/FBI Computer Crime and Security Survey* (2005). http://www.gocsi.com

Dübendorfer, Thomas, Arno Wagner and Bernhard Plattner, *An Economic Model for Large-Scale Internet Attacks* (Study by the Computer Engineering and Networks Laboratory of ETH Zurich, 2004). http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/WETICE-ES-duebendorfer-economic_damage_model.pdf

Eckert, Claudia, *IT-Sicherheit: Konzepte – Verfahren – Protokolle* (3rd ed. revised and expanded. Munich and Oldenbourg, 2004).

Federal Bureau of Investigation (FBI), *2005 FBI Computer Crime Survey* (2005). http://www.fbi.gov/publications/ccs2005.pdf

Gartner Research, *Enterprises and Employees: The Growth of Distrust* (2005). Summary of findings available at: http://www.csoonline.com/analyst/report3317.html

Haldemann, Lukas, *Versicherung von Internet-Risiken* (Term Paper, IT Department of ETH Zurich, 2001). http://www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf

KPMG, *IT-Management 2005: Standortbestimmung und Trends in der Schweizer Informatik* (Zurich and Geneva, 2005).

MELANI – Reporting and Analysis Centre for Information Security, *Information Assurance: The Situation in Switzerland and Internationally. Semi-Annual Report 2005/1* (2005). http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=en&PHPSESSID=d532e556dd85528bb64edb458d06d5de

MELANI – Reporting and Analysis Centre for Information Security, *Information Assurance: The Situation in Switzerland and Internationally. Semi-Annual Report 2005/2* (2006). http://www.melani.admin.ch/berichte/lageberichte/index.html?lang=en&PHPSESSID=d532e556dd85528bb64edb458d06d5de

National Hi-Tech Crime Unit (NHTCU), *Hi-Tech Crime: The Impact on UK Business* 2005 (2005).http://www.gfknop.co.uk/content/news/news/Impact%20of%20HTC%20NOP%20Survey%202005.pdf

Sieber, Pascal, *Einsatz und Nutzung des Internets in kleinen und mittleren Unternehmen in der Schweiz: Von der Einführung 1999 zur Entwicklung erster geschäftskritischer Anwendungen 2002* (Study commissioned by the Ministry for the Economy, Berne, 2002).

7 Appendices

Appendix 1: Composition of the sample pool / Breakdown of companies

- The **parent population for the survey comprises all Swiss companies** in the secondary and tertiary sectors.
- The survey excluded all large firms who are members of MELANI-Net.
- The survey sought to cover at least 500 participants. The estimated response rate was 10% of companies asked. This resulted in a **target sample size of 5,000 companies**.

- **Differentiating criteria of the firms:**
  a) **Size categories:**
     - Micro firms: 0-4 FTEs
     - Very small companies: 5-9 FTEs
     - Small companies: 10-49 FTEs
     - Medium-sized companies: 50-249 FTEs
     - Large companies: more than 250 FTEs

  b) **Sectors** according to the categorisation of economic activities by the Federal Office for Statistics.[52]
     - **Industry, manufacture of goods:** Organisations that convert materials or parts into goods by mechanical, physical or chemical means.
     - **Construction:** Building construction and civil engineering, construction installations and other extension work.
     - **Trade:** Wholesale and retail trade (onward sale with no further processing) of all types of goods and the furnishing of services in the sale of goods.
     - **Hotels and restaurants:** Provision of accommodation and/or preparation of meals, snacks and drinks for immediate consumption by guests.
     - **Transport and communication:** Activities associated with the scheduled or occasional transportation of goods and people by rail, road, sea and air as well as transportation in pipelines. Associated and secondary activities related to railway stations, ports and airports, parking spaces and car parks as well as freight transshipment, storage and also post and telecommunications. Rental of vehicles with driver or service personnel.
     - **Financial intermediation:** Acceptance and distribution of financial resources for purposes other than the obligatory retirement scheme, insurance and pension funds.
     - **Business services:** These activities mainly concern the corporate sector. However, practically all activities in this sub-section can also be used by private households, e.g. rental of consumer goods, databases, legal advice, detective agencies as well as security guard services, interior decorators, photographers and photo laboratories, etc.
     - **IT services:** Activities associated with hardware or software and general data processing.

52 NOGA: General Classification of Economic Activities. More details on this system can be found on the website of the Federal Office for Statistics:
http://www.bfs.admin.ch/bfs/portal/en/index/infothek/nomenklaturen/blank/blank/noga0/publikationen.html

- **Public administration:** Activities normally carried out by public-sector bodies. The legal or institutional status of the body *per se* is not decisive in this respect.
- **Education:** Public and private education at all levels and in all subjects in the various educational establishments of the regular school system, as well as adult education, literacy programmes, etc.
- **Healthcare:** Hospitals, doctors' surgeries, veterinary and social work (including retirement homes, nursing homes, youth centres).
- **Other services:** Services that do not primarily concern the corporate sector (e.g. culture, sports, laundrettes, hair/beauty salons).

- **Sampling plan:**
  The sample had to be stratified such that conclusions could be drawn for the different company sizes and individual business sectors. Therefore, a disproportionate sampling approach was taken (quota random sampling) whereby individual strata were over or underrepresented – something that had to be rectified subsequently by means of weighting. In many business sectors, a census or universal sample had to be taken for the 250+ FTEs category, where only a small number of large companies actually exist.
  The addresses of the companies were obtained from the Federal Office for Statistics on the basis of the following sampling plan:

Quota requirements for ordering addresses

NOGA sections (divisions)	Size categories (FTEs)		
	0-9	10-249	250+
D Manufacturing of goods (15-37)	330	420	250
F Construction (45)	300	390	C
G Wholesale and retail trade (50-52)	500	400	100
H Hotels and restaurants (55)	220	320	C
I Transport, storage and communication (60-64)	200	200	C
J Financial intermediation; insurance (65-67)	120	160	C
K Real estate; other business activities (70-74)	550	350	C
L Public administration and defence; compulsory social security (75)	60	130	C
M Education (80)	140	210	C
N Health, veterinary and social work (85)	270	220	C
O Other community, social and personal service activities (90-93)	310	200	C
Total	**3,000**	**3,000**	**~1,000**

FTE = Full-time equivalents
C = Census (i.e. all companies in this size category)

- A reserve of 2,000 addresses was kept on file. The survey was sent to 5,000 companies. As some of the addresses were out of date, the actual sample size was 4,916 companies.

Appendix 2: Response

- 562 companies participated in the survey, corresponding to a **response rate** of **11.45%**.
- No systematic analysis was made of the **non-participants**. As with all surveys, where only some of those asked actually complete the questionnaire, there is a risk of the respondents deviating from the average in some important areas. Moreover, it may be that the mere fact that a company responds to the survey is a sign that it takes the subject of IT security more seriously than others may do. Some indication of the reasons for non-participation in the survey comes from those companies who actively turned down the survey. Of the **44 rejections**, half cited lack of time or interest. Eight companies said they do not use any IT, another 10 said they were not competent to respond to the questions, and four companies did not want to complete the questionnaire for security reasons.

  Response by number of employees:

FTEs	Number	Percent
0-4	132	23.49
5-9	62	11.03
10-49	195	34.70
50-249	86	15.30
>250	87	15.48

  Response by business sector:

Sector	Number	Percent
Manufacturing	82	14.59
Construction	92	16.37
Trade	59	10.50
Hotels & restaurants	20	3.56
Transport & comm.	37	6.58
Finance	21	3.74
Business services	53	9.43
IT services	37	6.58
Public administration	42	7.47
Education	14	2.49
Healthcare	56	9.96
Other services	49	8.72

Appendix 3: Data weighting

- **The respondents do not reflect reality with respect to company size and the business sector in which they operate**. In reality, only 0.3% of all companies have a workforce of more than 250; however, such large companies made up 15% of the respondents to the survey. Among the various sectors, companies operating in construction are overrepresented, while the business services providers and hotels and restaurants are underrepresented.
- A disproportionate reflection of reality is necessary to ensure sufficient data for comparisons to be made. However, this also means that the average figures among respondents cannot be directly used to draw conclusions for the average of all Swiss companies in the secondary and tertiary sectors.
- In order to produce estimates for all firms in Switzerland, the data must be weighted.
- Weighting means that **all data are multiplied by the weighting factor w**. This is calculated as follows:

$$w = \frac{n_{Ri}/N_R}{n_{Si}/N_S}$$

n_{Ri}= Number of firms in category ***i*** in reality
N_R= Number of firms in reality
n_{Si}= Number of firms in category ***i*** in the sample
N_S= Number of firms in the sample

- There are a total of 60 categories (5 company sizes and 12 business sectors). The weighting factor ***w*** can be calculated for each of these categories by dividing the percentage in reality by the percentage in the sample.

Sector	Total (Reality)	Total (Survey)	Weighting	0-4 (R)	0-4 (S)	Weighting	5-9 (R)	5-9 (S)	Weighting
Manufacturing	12.82	14.59	0.88	8.17	1.43	5.72	1.86	0.71	2.61
Construction	10.91	16.37	0.67	7.11	2.50	2.85	1.88	3.39	0.55
Trade	22.60	10.50	2.15	17.36	3.21	5.41	3.08	1.07	2.88
Hotels & rest.	7.91	3.56	2.22	5.02	0.36	13.96	1.74	0.36	4.85
Transport & comm.	3.50	6.58	0.53	2.53	1.61	1.57	0.43	0.54	0.79
Finance	1.71	3.74	0.46	1.07	0.89	1.20	0.25	0.00	
Business services	19.39	9.43	2.06	16.39	3.21	5.11	1.78	1.25	1.43
IT services	3.52	6.58	0.53	2.90	3.04	0.95	0.30	0.54	0.56
Public administration	0.74	7.47	0.10	0.29	0.89	0.32	0.11	0.89	0.13
Education	2.21	2.49	0.89	1.28	1.07	1.20	0.25	0.00	
Healthcare	6.87	9.96	0.69	5.29	2.32	2.28	0.69	0.89	0.78
Other services	7.83	8.73	0.90	6.64	3.04	2.18	0.69	1.25	0.55
Total	100.00	100.00		74.06	23.49		13.08	11.03	

Sector	10-49 (R)	10-49 (S)	Weighting	50-249 (R)	50-249 (S)	Weighting	250+ (R)	250+ (S)	Weighting
Manufacturing	2.06	4.64	0.44	0.60	3.93	0.15	0.13	3.93	0.03
Construction	1.68	7.32	0.23	0.22	2.32	0.10	0.02	0.89	0.02
Trade	1.84	4.64	0.40	0.26	0.54	0.48	0.05	1.07	0.05
Hotels & rest.	1.03	2.14	0.48	0.10	0.36	0.28	0.01	0.18	0.05
Transport & comm.	0.43	2.68	0.16	0.09	0.89	0.10	0.02	0.89	0.02
Finance	0.30	0.54	0.55	0.06	0.18	0.34	0.03	2.14	0.02
Business services	1.05	2.32	0.45	0.14	1.79	0.08	0.02	0.89	0.02
IT services	0.27	1.96	0.14	0.04	0.36	0.11	0.01	0.71	0.01
Public administration	0.21	1.79	0.12	0.09	1.79	0.05	0.03	2.14	0.01
Education	0.49	1.07	0.46	0.16	0.18	0.91	0.02	0.18	0.14
Healthcare	0.59	2.86	0.20	0.25	1.96	0.13	0.06	1.79	0.03
Other services	0.42	2.86	0.15	0.06	0.89	0.07	0.01	0.71	0.01
Total	10.37	34.70		2.09	15.30		0.40	15.48	

Appendix 4: Weighting process to determine the influence of the business sector / company size

- In some cases, the impact of the company size or the business sector is analysed. Whenever the influence of either one of these is being examined, it is important to rule out the influence of the other in each case.

  Example: Among the companies asked in the financial sector, 57% are large companies with more than 250 employees. Therefore, compared with the proportion of large firms in the overall sample (16%), such companies in the financial sector are clearly overrepresented. Now, if the findings were to show that companies in the financial sector invest heavily in IT security, this could merely be due to the fact that large firms in this sector are overrepresented.
- This is why we use the weighting factor w_2, which weights the data in such a way that the size categories are the same in all sectors and the sectors appear with the same frequency in all size categories. The formula for calculating w_2 is as follows:

$$w_2 = \frac{n_i / n_{Bi}}{n_{Gi} / N} = \frac{n_i \, N}{n_{Bi} \, n_{Gi}}$$

n_i = Number of firms in category ***i***
n_{Bi} = Number of firms in the business sector of category ***i***
n_{Gi} = Number of firms in the size category of category ***i***
N = Number of firms in the entire sample

Calculation of w_2 using the percentages of the size categories per business sector:

Sector	0-4 (B)	0-4 (A)	Wgt	5-9 (B)	5-9 (A)	Wgt	10-49 (B)	10-49 (A)	Wgt	50-249 (B)	50-249 (A)	Wgt	250+ (B)	250+ (A)	Wgt
Manufacturing	9.76	23.57	2.41	4.88	10.89	2.23	31.71	34.82	1.10	26.83	15.19	0.57	26.83	15.52	0.58
Construction	15.22	23.57	1.55	20.65	10.89	0.53	44.57	34.82	0.78	14.13	15.19	1.08	5.43	15.52	2.86
Trade	30.51	23.57	0.77	10.17	10.89	1.07	44.07	34.82	0.79	5.08	15.19	2.99	10.17	15.52	1.53
Hotels & rest.	10.53	23.57	2.24	10.53	10.89	1.03	63.16	34.82	0.55	10.53	15.19	1.44	5.26	15.52	2.95
Transport & comm.	24.32	23.57	0.97	8.11	10.89	1.34	40.54	34.82	0.86	13.51	15.19	1.12	13.51	15.52	1.15
Finance	23.81	23.57	0.99		10.89		14.29	34.82	2.44	4.76	15.19	3.19	57.14	15.52	0.27
Business services	33.96	23.57	0.69	13.21	10.89	0.82	24.53	34.82	1.42	18.87	15.19	0.80	9.43	15.52	1.65
IT services	45.95	23.57	0.51	8.11	10.89	1.34	29.73	34.82	1.17	5.41	15.19	2.81	10.81	15.52	1.44
Public administration	11.90	23.57	1.98	11.90	10.89	0.92	23.81	34.82	1.46	23.81	15.19	0.64	28.57	15.52	0.54
Education	42.86	23.57	0.55		10.89		42.86	34.82	0.81	7.14	15.19	2.13	7.14	15.52	2.17
Healthcare	23.64	23.57	1.00	9.09	10.89	1.20	29.09	34.82	1.20	20.00	15.19	0.76	18.18	15.52	0.85
Other services	34.69	23.57	0.68	14.29	10.89	0.76	32.65	34.82	1.07	10.20	15.19	1.49	8.16	15.52	1.90

(B): Percentage in the business sector in question
(A): Average percentage

Appendix 5: Questionnaire

- The survey was conducted online, with the target firms receiving a password by post or e-mail. This password enabled participants to log in to the website www.unipark.de/informatiksicherheit.

- The survey was conducted between 15 March 2006 and 13 April 2006.

Start

Welcome to the online survey

"IT Security in Switzerland"

This survey is conducted by the Center for Security Studies (CSS)
at ETH Zurich.

Information on completing this questionnaire
This questionnaire is directed at companies and public bodies.
For the sake of simplicity, all participants are referred to in the questions as organisations.
All information is processed in complete confidentiality and anonymity.
If you have any questions, please write to:
suter@sipo.gess.ethz.ch
Please complete the questionnaire by 29 February 2006.

In which sector does your organisation operate (main business activity)?
Please select one only.

- ○ Industry, manufacturing of goods
- ○ Construction
- ○ Wholesale or retail trade (food and consumer goods)
- ○ Hotels and restaurants
- ○ Transport, storage and communication
- ○ Financial intermediation, insurance
- ○ Real estate
- ○ IT services
- ○ Other business services
- ○ Education
- ○ Healthcare and social work
- ○ Public administration
- ○ Other _____

How many people are employed at your organisation?
Including apprentices. Please convert part-time workers to FTEs. If applicable, include also employees based abroad.

- ○ 0-4
- ○ 5-9
- ○ 10-49
- ○ 50-249
- ○ Over 250

How high were your organisation's sales revenues in 2005?
Please state in Swiss francs.

- ○ below 1 million
- ○ 1-4.9 million
- ○ 5-9.9 million
- ○ 10-99 million
- ○ Over 100 million
- ○ Don't know

What percentage of people in your organisation use the following tools for their work?

	0%	1-20%	21-40%	41-60%	61-80%	81-100%	Don't know
○ Desktop PC							
○ Laptop							
○ Personal digital assistant (PDA)							
○ Mobile phone							
○ E-mail							
○ Internet							

Can your staff access your corporate network from home?

- ○ Yes
- ○ Yes, but only under certain conditions
- ○ No
- ○ Don't know

What kind of Internet connection is used at your organisation?

- ○ Modem
- ○ ISDN
- ○ DSL (xDSL, ADSL, SDSL, etc.) < 2 MB/s
- ○ Cable modem or other broadband connection
- ○ Other _____

Does your organisation use wireless networks?

- ○ Yes
- ○ No
- ○ Don't know

Does your organisation have a website?

- ○ Yes
- ○ No
- ○ Don't know

What does your website contain?
More than one answer possible.

- ○ Information about the organisation (contact details, mission, etc.)
- ○ Information on your products (advertising)
- ○ Product sales without online payment processing
- ○ Product sales with online payment processing

○ Other _____

Does your organisation use the Internet for any of the following purposes?

	Yes	No	Don't know
○ Information search			
○ Training and education			
○ Discussion forums			
○ Purchasing of products and services			

How would you evaluate the importance of the IT infrastructure for your organisation?

not very important ○ ○ ○ ○ ○ very important

How has the proportion of investments in IT infrastructure evolved over the past five years?

Decreased	Stable	Increased	Don't know
○	○	○	○

Did your organisation experience any of the following IT security breaches in 2005?

○ Viruses, worms, Trojan horses
○ Unauthorised access (spyware)
○ Denial of service
○ Hacking
○ Data theft
○ Theft of laptops or other IT equipment
○ Abuse of wireless network
○ Website defacement
○ Other _____
○ No breaches found

What was the source of these breaches?

○ The attacks came from outside the organisation itself.
○ The attacks originated with a member of staff.
○ There were both internal and external attacks.

How many people are in the IT security team at your organisation?
Please convert part-time positions to FTEs.

○ None
○ 0-1
○ 2-5
○ 6-10
○ Over 10

How qualified is the leader of this team?

○ Degree in IT from a university or technical college
○ Apprenticeship completed in IT
○ Swiss federal certificate in IT

- ○ On-the-job training
- ○ Other _____

How much was spent on IT security in 2005?
Please state amounts in Swiss francs. Include staff and structural costs.

- ○ 0-5,000
- ○ 5,001-20,000
- ○ 21,001-100,000
- ○ Don't know

Is your organisation likely to spend more or less on IT security in 2006?

- ○ More
- ○ Less
- ○ Same
- ○ Don't know

What percentage of the IT security budget is delegated to outside firms?

0%	1-20%	21-40%	41-60%	61-80%	81-100%	Don't know
○	○	○	○	○	○	○

Do you agree with the following statements: "In IT security, my organisation invests sufficiently in…

	Agree	More or less agree	Neither	Don't really agree	Don't agree	Don't know
… security technologies."	○	○	○	○	○	○
… training for those responsible for IT."	○	○	○	○	○	○
… training for all employees in the subject of IT security."	○	○	○	○	○	○

What security technologies do you use to safeguard the security of your IT systems?
Several answers possible.

- ○ Anti-virus software
- ○ Firewall
- ○ Encryption
- ○ Anti-spyware programs
- ○ Intrusion detection
- ○ Staff training in IT security
- ○ Biometrics
- ○ Others _____
- ○ None

Do you conduct regular IT security audits?

- ○ Yes, conducted by the organisation itself
- ○ Yes, conducted by an external company
- ○ Not yet, but such audits are planned
- ○ No
- ○ Don't know

Which of the following security concepts are used in your organisation?
Several answers possible

- ○ Back-up management
- ○ Security policy
- ○ Update management (vulnerability management)
- ○ Incident response management
- ○ Other _____
- ○ None

Does your organisation have insurance against potential damage from an IT security breach (hardware, software, data loss)?

- ○ Yes
- ○ No
- ○ Don't know

If not, why does your organisation not have any insurance against such damage?
Several answers possible

- ○ Not worth it
- ○ Didn't know that such insurance exists
- ○ No budget for that
- ○ Insurance offerings not satisfactory
- ○ Other reasons _____

Do you (or your organisation) look for external help in solving IT security problems?

- ○ Yes
- ○ No
- ○ Don't know

Where do you look for such assistance?
Several answers possible

- ○ Software manufacturer
- ○ Internet Service Provider (ISP)
- ○ Colleagues/ acquaintances in other companies
- ○ On the Internet (websites, Internet forums, etc.)
- ○ Other _____

Has your organisation ever contacted the police concerning an IT security breach?

- ○ Yes
- ○ No
- ○ Don't know

If not, why were the police not called in?
Several answers possible

- ○ Didn't know the police deal with such issues
- ○ The police do not offer any means of reporting such incidents.
- ○ Steps taken in-house are more efficient.
- ○ Fear of negative repercussions on the organisation's image

○ The incidents did not seem to be serious enough.

Would you use the services of a helpdesk providing advice on IT security matters?

○ Yes, in all cases
○ Yes, but only if it were carried out independent of the software vendors
○ No

Such a helpdesk could provide a range of different services. Which services would you find useful?

	helpful	not helpful
Telephone help	○	○
Help using e-mails or tickets	○	○
Personal help on-site	○	○

Sharing experiences and know-how with colleagues can be a useful source of information. In which type of exchanges would you participate?

	definitely	probably	probably not	definitely not
Anonymous exchange via Internet forums	○	○	○	○
Exchange via personal contact	○	○	○	
Exchange in workshops organised by the software manufacturer	○	○	○	○
Exchange in workshops organised by an independent third-party	○	○	○	○

Other services and documents could help you improve IT security. Please evaluate the usefulness of the following.
1 means "not very useful"; 5 means "very useful"

	1	2	3	4	5
Guidelines for reporting an offence	○	○	○	○	○
Basic staff training / awareness materials	○	○	○	○	○
Recommendations for best practices (e.g. ISO 17799)	○	○	○	○	○
Help in implementing best practices (e.g. ISO 17799)	○	○	○	○	○
Guidelines for coping with incidents	○	○	○	○	○

In your opinion, who would be the most suited to providing the aforementioned services (helpdesk, setting up information exchange platforms, drafting of documents)?

○ Software vendor
○ State-run organisation
○ Trade organisations/associations
○ Dedicated organisations
○ Consultancy firms

Would your organisation be prepared to participate financially in such an organisation?

○ Yes, up to a maximum of CHF 500
○ Yes, up to a maximum of CHF 2,000
○ No
○ Don't know

Are you familiar with MELANI, the Swiss Confederation's reporting and analysis centre for IT security?

○ Yes
○ No

If so, how helpful do you find MELANI in improving your organisation's IT security?

not very helpful ○ ○ ○ ○ ○ very helpful

Are the following MELANI services of use to you?

	yes	no	don't know
Warnings (news ticker)	○	○	○
Incident report form	○	○	○
General information on threats to and security of information systems	○	○	○
Demonstration and training programs for your staff	○	○	○
Checklists and instructions for your staff	○	○	○
Reports on the main trends and developments	○	○	○

Author

Manuel Suter, lic. phil. I, researcher at the Center for Security Studies (CSS), ETH Zurich

Project responsibility

Dr. Myriam Dunn, Head, New Risks Research Unit and CRN Coordinator (Crisis and Risk Network), Center for Security Studies (CSS), ETH Zurich

Dr. Victor Mauer, Deputy Director, Center for Security Studies (CSS), ETH Zurich