Information security surveys as instrument of risk analysis

To evaluate the threats to information security, it is essential to know the frequency and quality of breaches in companies. Such information can be derived from surveys. This article discusses the strengths and weaknesses of surveys.

A fundamental concern of risk analysis is the identification and quantification of threats. The questions “What can go wrong?” and “What is the likelihood of it going wrong?” have to be considered carefully. Thus, in the domain of Critical Information Infrastructure it is important to know the quantity and quality of threats to information security. But the data for these threats are hard to come by. One possible option for completing this task is to conduct computer security surveys.

There are currently plenty of such surveys available, however, most of them are conducted by commercial IT-security companies and exist for marketing purposes rather than as a scientific endeavor to clarify facts. To gain more independent knowledge, several national organizations responsible for information security have undertaken their own studies. The best known among them is the annual CSI/FBI “Computer Crime and Security Survey,” as well as the survey “Hi-Tech Crime – the Impact on UK Business 2005” by the UK’s NHTCU (National Hi-Tech Crime Unit) and “The IT-Security Situation in Germany in 2005” by the German Federal Office for Information Security (BSI). The latest example is the survey “Information Security in Swiss Companies,” conducted by the Center of Security Studies (CSS) at ETH Zurich at the request of MELANI (Melde- und Analysestelle Informationssicherheit) the reporting and analysis center for information security of the Swiss government.

Drawing on the experiences gained in composing the Swiss survey, I’ll discuss the strengths and weaknesses of information security surveys as instruments of threat evaluation.

The challenges of information security surveys...

First, it is important to clarify that surveys aren’t able to accurately map the current-state analysis of threats to information security. There are simply too many methodological obstacles such surveys have to confront: first, the willingness of the companies to provide information about their problems with security (information that may be restricted for obvious reasons). This can make it difficult to build a sample big enough from which one can make generalizations. Another difficulty is the great diversity among companies. Threats to information security affect different companies to very different extents. Therefore, accurate statements about threats to information security of companies in general are extremely difficult to make.

I will discuss the methodological obstacles and requirements at length later in this article. But, it’s enough to emphasize that exaggerated expectations on information security surveys are exaggerated.

Often, expectations on information security surveys are exaggerated.

<table>
<thead>
<tr>
<th>Manuel Suter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)</td>
</tr>
<tr>
<td><a href="mailto:suter@sipo.gess.ethz.ch">suter@sipo.gess.ethz.ch</a></td>
</tr>
</tbody>
</table>
present results that can only be weakly confirmed. For example, despite the difficulty, surveys often aim to precisely assess the average losses that companies suffer as a result of computer crimes.

…and their potential
But even though surveys aren’t able to quantify threats precisely, investigations on information security in companies are still worthwhile. Actually, for the purpose of risk analysis, there is little need to tally the cost of threats, it is more relevant to discover or confirm trends and probabilities. It is also more important to investigate the type and frequency of incidents detected in a given type of company, instead of extrapolating the costs of threats. Findings on the frequency of incidents are essential for the setup of early-warning approaches. Furthermore, because many current threats originate in so-called botnets (infected computers linked in a network), threat estimations must also take into account the level of ICT-protection and risk management in companies. A common assumption is that companies tend to spend as little as possible on safeguarding information security, which could possibly result in insufficient protection, and would in turn increase the risk of attacks originating from infected computers. Again, one shouldn’t expect surveys to accurately determine the overall quality of risk management in companies. Still, it is possible to examine some indicators, such as the diffusion of technical or organizational security measures, the financial and personal resources allocated to information security, or the outsourcing of risk.

Such basic facts for threat estimation are only available through broad surveys among companies. In addition, conducting surveys may strengthen a company’s awareness of security issues. By completing a survey, information security officers possibly gain new insights into the state of measures taken in their companies. The results of the survey may also help the officers to convince company management of the importance of additional measures. Thus, indirectly, surveys may play a role in risk management.

Finally, a survey is also a suitable instrument for testing the acceptance of innovative ways of solving the IT security problems. The survey participants could be asked, for example, which forms of joint action interest them. With questions of this type, it is possible to appraise (in advance) the chances of success of new solutions to the problem of information security.

In short, while surveys cannot quantify the threats to information security precisely, they can deliver important insights into problems facing the companies, preferred security measures, and new possible solutions.

Methodological requirements
The quality of survey results depends on the accurate application of methodological requirements. The biggest methodological challenge is the definition of the sample pool. Not only must the size of the sample pool be considered carefully, but its composition should be as well. There are many significant differences between firms that may potentially influence a firm’s risk management approach. Common differentiating criteria included in information security surveys are company size and business sector. Depending on whether conclusions should be drawn from company size and individual business sectors, the size of the sample pool has to be converted, or a disproportionate sampling approach should be taken (e.g. quota random sampling, whereby individual strata are over- or under-represented – something that has to be rectified subsequently by weighting).

Of course, the response rate is also crucial for the quality of the results. To avoid the danger of too small a representation of categories, it is helpful to set a numerical target for each category in advance. In addition, the mere fact that a company responds to the survey may be a sign that it takes the subject of IT security more seriously than others do. Thus, if the respond rate is low, it may be necessary to properly compare the respondents with the non-respondents.

A further methodological challenge is the creation of the questionnaire. As mentioned, it is disadvantageous to ask questions of great complexity. Respondents will abandon the survey if they don’t understand many questions, or worse, they will give false answers. Also, the questions shouldn’t be too sensitive as some companies won’t give an answer for security reasons. In short, the simpler the questions are, the better the interpretation of the results will be.

The methodological requirements for such a survey are rather substantial and it is almost impossible to fulfill all of them completely. However, to assure the quality of the results, these requirements should serve as guidelines for every survey.

The results of recent surveys
The most recent surveys strive for somewhat different goals, but they have
important commonalities. In particular, the similarities among the results are interesting for risk analysis, as they indicate global trends in information security threats. Therefore, it is interesting to compare the most important results of the US, British, German and Swiss surveys.

As expected, all the surveys show that viruses, spyware, trojans and other malware are by far the most frequent breaches noted. Because the sample pools of the surveys are different, it is rather difficult to compare the percentages of companies affected. However, it can be clearly stated that malware is the most widespread threat. Another interesting finding is that in all the country surveys (except for the German survey, in which the question wasn’t included), the conventional equipment theft is one of the most frequently cited incidents. In addition, the comparison also shows that the most sophisticated attacks in technical terms (that also have a more serious impact) are less frequently encountered in all countries surveyed.

The findings about the technical security measures are analogical. All of the surveys analyzed indicate a nearly uniform use of firewalls and antivirus software across companies. Meanwhile, more complex technologies such as intrusion detection and biometric systems are rarely used.

These examples show that most of the results in the surveys aren’t astonishing. Nevertheless, they are valuable because they serve to confirm trends. But above all, the results constitute the basis for further investigations and provide a global perspective on IT-security threats.

Suggestions for future surveys
Some of the cited surveys are already a tradition. For example, the FBI/CSI “Annual Computer Crime and Security Survey” is in its 11th year. This is remarkable since continuity is a precondition for all research into developments. Surveys don’t have to be repeated annually and the questionnaires don’t have to always include the same questions. Though, it would be interesting if future surveys could highlight trends by formulating questions in the same manner as current surveys. Therefore, the first suggestion for future information security surveys is that they should include some similar standard questions. This would ease the comparison of survey results, whether international or chronological. In my opinion, standard questions should be rather basic, such as questions about the frequency of incidents. Detailed questions about the amount of losses sustained and losses by type of attack, for example, are hardly comparable, as respondents’ answers may change over time and may vary between the different countries. Unfortunately most current surveys concentrate too much on these kinds of questions.

The second suggestion concerns the composition of samples. The Swiss survey showed significant differences between the various companies. It is important to note that the size of the company has a great impact both on the frequency of incidents, as well as on the use of security measures. It would be beneficial to design future surveys to take this into account and differentiate between categories of size.

Furthermore, surveys should distinguish between the business sectors of companies surveyed, since in all likelihood, companies of some sectors (e.g. the financial sector or IT services) are much more affected by incidents than firms in other sectors, such as the hospitality (hotels and restaurants) or the manufacturing sectors.

Finally, as a third suggestion, I would propose to include more questions referring to the needs of companies. Granted, such questions go beyond the scope of risk analysis, but they are indispensable to evaluate new solutions to the problems of information security.

Conclusion: The prospects of information security surveys
We can conclude that information security surveys are not a panacea for risk analysis. However, they are an applicable instrument for gathering information on the nature of threats. In order to be effective, the surveys must be conducted in a methodological manner and the interpretation of the results must be consistent and reliable.

Finally, it should also be mentioned that information security surveys do not yet tap their full potential as instrument for risk analyses. Comparing the results of different international surveys could provide a better overview, and with chronological comparisons it could be possible to identify new developments with regard to threats.

See www.crm.ethz.ch for an online version of the Swiss survey.