IT Security Governance—A Slow Start to a High Maturity Level

By Peter R. Bitterli, CISA

One of the leading reinsurance companies of the world expanded its IT security organisation between 1999 and 2003 from 1.5 to 27 full-time employees, from 11 to 32 part-time employees and from a budget of about CHF 1.2 million to approximately CHF 18 million. This article is based on the keynote speech delivered by Bruno Porro at ISACA's EuroCACS 2004 conference. Bruno Porro is the chief risk officer of Swiss Re and also heads the business information security committee (formerly, group IT security committee) of Swiss Re.

About Swiss Re

Swiss Re is one of the world's leading reinsurers and the world's largest life and health reinsurer. The company, which was founded in 1863, operates through more than 70 offices in more than 30 countries. In 2003, premiums earned increased to CHF 30.7 billion and the net income was CHF 1.7 billion.

The core business segments risk transfer, risk finance and asset management are covered by a variety of products to manage capital and risk. Traditional reinsurance products, including a broad range of property and casualty as well as life and health coverage, and related services are complemented by insurance-based corporate finance solutions and supplementary services for comprehensive risk management.

There are approximately 8,000 people working in the three business groups (property and casualty, life and health, and financial services) and the corporate centre. The corporate centre exercises global functions on behalf of the Swiss Re group and plays a vital role in managing the group's resources. Key global information technology functions form part of the corporate centre while each business group employs its own IT personnel for specific (local) developments and support.

The Evolution of IT Security at Swiss Re

The First Step

Back in the 1990s, the use of information technology was not that important for Swiss Re. Security requirements such as confidentiality or availability were rated low—as was typical at that time probably for any reinsurance company. Therefore, IT security was handled in an isolated and more or less intuitive way. A loose network of IT security officers managed security-related problems and possible solutions and informally exchanged specific security know-how.

In about 1997 and due to the increased use of information technology as the enabling factor in almost every business process in Swiss Re, information security became an important business function. This importance was further increased by the adoption and heavy dependence on the Internet as a business channel and communication medium as well as the need to comply with a number of new data privacy and other laws in many parts of the world.

This is one of the main reasons why in 1998 a new Swiss Re IT security policy (a three-to-four-page high-level document) was set up and approved by the company's executive board. The IT security policy contained nine fundamental IT security principles and made clear that all employees, contractors and suppliers have certain responsibilities in regard to ensuring information security.

As part of the IT security policy, a formal IT security organisation was set up, consisting of the group IT security committee, the group IT security office and the IT security officers network:

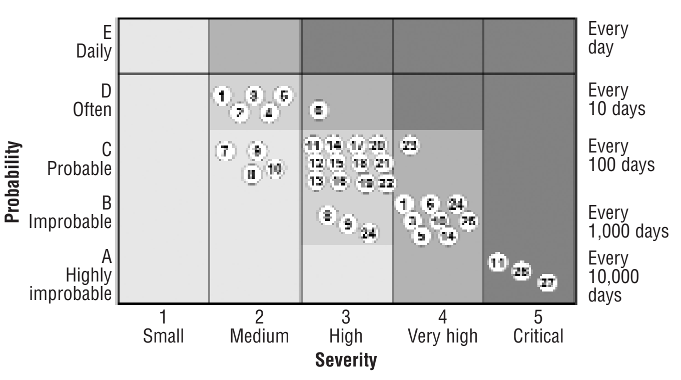
- Group IT security committee (now the business information security committee)—Provides groupwide management direction in IT security and ensures that IT security is consistently addressed as a business issue. It consists of nine business and IT representatives and is led by the group risk officer, who is a member of the executive board of Swiss Re. The name change from group IT security committee to business information security committee in 2003 reflects the changed focus.
- Group IT security office—Develops and co-ordinates all aspects of IT security groupwide. Activities include the development and implementation of groupwide IT security policies and guidelines, awareness programmes and training, support for IT security officers (in divisions and major legal entities), and the handling of any IT security incidents affecting the organisation as a whole.
- IT security officers in divisions and major legal entities—IT security officers manage and co-ordinate IT security activities within their units. Activities include the assessment of risks, consulting and support relating to IT security measures and their implementation, heightening IT security awareness, managing training activities, handling IT security incidents, and organising regular IT security status checks. Currently, Swiss Re has 27 full-time and an additional 32 part-time IT security officers (as of spring 2004).

Although the IT security organisation was formally set up in 1999, it took time and other events before security was firmly established.

Assessment of 2000

The intensive use of IT starting in 1999 opened up a new field of crime and fraud threats to Swiss Re that could cause severe damage to vital electronic assets and have a negative impact, including but not limited to the disruption of core business processes. This is why in 2000, as a basis for systematic IT risk management, Swiss Re started to collect, evaluate and rate possible IT risk scenarios according to their respective probability and severity and place them in what Swiss Re calls "The IT Security Risk Landscape." It came as no surprise to the IT security experts that many of the collected risk scenarios (see example scenarios 11, 26 and 27 in **figure 1**) had to be placed in areas on the risk landscape that were considered to be "not acceptable" (marked in dark shaded areas in **figure 1**), as the possible impact could result in severe losses to Swiss Re.

Figure 1—The IT Security Risk Landscape (2000)



Some of the numbers are actually shown twice in the IT security risk landscape shown in **figure 1**. In these cases, a scenario has been split into two similar subscenarios, which are differentiated only by their specific probability and severity level. An example of such a double scenario is where a user's password is misused for unauthorised access: there are "normal" users with typically uncritical access privileges vs. system administrators and other users with almost unrestricted access privileges. The probability of the scenario password misuse for a "normal" user is far higher whereas the related severity is lower.

In parallel to the scenario-based risk assessment, Swiss Re performed an IT security self-assessment, based on the British Standard BS7799 ("Code of Practice for Information Security Management"). As the standard did not (and still does not) provide help to rate the compliance of a company, Swiss Re adopted a maturity model that had been developed during 1996-1999 by the author of this article for use in control self-assessment. The maturity model is described in **figure 2**.

The result of this assessment is provided in **figure 3** (the numbers around the circle refer to the chapters of the "old" BS7799). **Figure 3** clearly shows, that although a few topics of the standard had been rated as acceptable (2 or higher) using the ratings from the maturity model, the vast majority of the topics were unacceptably low. (Note: The peak of topic 6.3 is for the antivirus defense, a topic that Swiss Re handled exceptionally well). Swiss Re decided that the overall target level should be "level 3," i.e., all best practice procedures contained in BS7799 are formalised, documented and implemented.

Figure 2—Maturity Model Used for Control Self-assessment

Level	Comments
4	Requirements fully covered, improvements proactively sought
3	Procedures formalised, documented and implemented
2	Well-structured and repeatable procedures, some topics not sufficiently covered
1	Very little implemented, instinctive action, informal and not repeatable
0	Almost nothing implemented, spontaneous action

According to the Information Security Forum (ISF), a strong correlation exists between the adherence to good practice standards (e.g., BS7799) and the probability of major IT security-related incidents. It therefore makes sense to measure the maturity level of a series of good practices and by that define a "risk exposure."

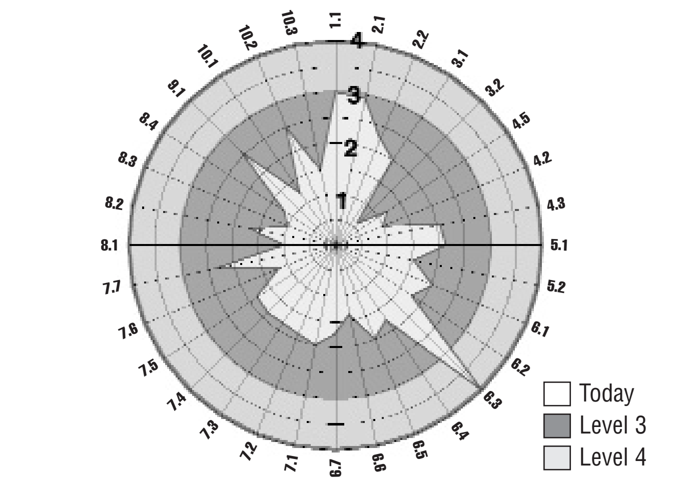
Based on the actual IT security risk landscape and the IT security radar chart (**figures 1** and **3**), the group IT security committee charged the group IT security office with defining an immediate action plan for improvement.

IT Security Strategy Approved in 2001

Because of the two-fold risk management approach with both a classical risk analysis (i.e., the scenario-based IT risk landscape) and a baseline approach using BS7799 as a reference (i.e., the IT Risk Radar Chart), it was not too difficult to derive and devise a clear IT security strategy.

In spring 2001, the executive board of Swiss Re approved the IT Security Strategy 2001-2003, consisting of a set of four concurrent IT security initiatives (shown in **figure 4**).

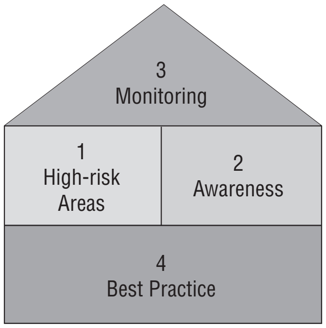
Figure 3—IT Security Radar Chart (2000)



Initiative 1: High-risk Areas

The first IT security initiative addressed existing high-risk technical issues, covering a wide range of topics such as a secure single point of access for all e-business users, a standardisation and reduction in the numbers of Internet access

Figure 4—The "House" of the Four IT Security Initiatives



points, encrypted secure remote access for Swiss Re employees from any place in the world, encryption of the hard disks of laptops, the hardening and improvement of the outer network perimeter, and a further improvement of the antivirus measures. Over time, antispam measures were also developed.

Initiative 2: Awareness and Training

Swiss Re recognised from the beginning that in IT security—as probably in most other areas, too—people make the difference. Swiss Re therefore specifically focused on a programme to foster the required change of behaviour. The long-term goal of the second IT security initiative was the internalisation of security-conscious behaviour in all aspects of work. This initiative was targeted (mainly) at managers, IT staff and all other users of IT.

The awareness campaign started with a video shown at the annual meeting of the 150 top executive managers of Swiss Re, followed by a new brochure, articles, an IT security web site, pop-ups, etc. During 2002 and 2003, every employee underwent a 90-minute classroom-based training showing the most important security aspects of the use of the Internet, e-mail and passwords. These trainings consisted of a mixture of video, slides, classroom discussions and question and answer sessions and were very well received. The analysis of a detailed feedback form clearly showed that 89 percent of the participants intended to adapt their behaviour after the course. Similarly, every laptop user underwent a 45-minute training, covering the major risks related to traveling with a laptop and using it in public places. Managers in all business groups received individually tailored presentations, explaining their vital role in the ongoing awareness campaign.

In 2004, Swiss Re started with e-learning targeted at specific groups in all IT departments, e.g., developers, administrators, supporters/help desk, and other IT staff. For the two highly important target audiences, developers and operators/administrators, an e-lab is currently being set up, where successful passers of the preceding e-learning modules can gain hands-on experience in protecting their systems from hacker attacks and other threats. These e-labs run on dedicated systems, enabling the participants to use real tools to analyse security deficiencies.

Lessons Learnt

The known and unknown threats are still growing and speeding up. They are becoming more aggressive and leaving less time to react. In some cases, just staying at the achieved high maturity level is already a very good result. The constantly changing technology needs proactive involvement of security experts with the best technical skills available to handle today's variety of security issues.

The vast progress of Swiss Re in IT security over the last few years is mostly due to having the necessary skills available—internally and externally—to implement the four strategic IT security initiatives. In retrospect, these initiatives, with their combination of technological and organisational measures, enabled Swiss Re to focus on medium-term security goals while also handling the countless day-to-day security issues.

The two-pronged risk management approach—with 1) benchmarking against a set of good security practices (i.e., baseline controls) based on the British Standard BS7799 and 2) handling recognised risk scenarios individually—proved its worth. As many of the problems to solve were (and still are) technical in nature, it was also very helpful for the group IT security officer to report to the chief information officer (CIO) as well as to the group IT security committee led by the chief risk officer (CRO).

—Bruno Porro, chief risk officer, Swiss Re

Initiative 3: Monitoring, Intrusion Detection and Incident Management

One of the overall objectives of the third IT security initiative is measuring and verifying the effectiveness of IT security controls. This was mainly handled by setting up an intrusion detection and response capability and the performance of security penetration tests as well as other security reviews of networks and platforms.

Since 2003, all network entry points and major network hubs are logged and continuously monitored by a "virtual team." For example, in December 2003, more than 2.4 million attack attempts were detected and successfully blocked. And, learning from a virus incident that started because an external consultant attached a virus-infected laptop to the Swiss Re network, any foreign hardware connected to the network will now be immediately detected, localised and removed. One of the latest additions is a third layer of spam filters, which has enabled the detection of more than 95 percent of all unsolicited e-mail.

Initiative 4: Best Practice in All Other Areas

The fourth IT security initiative is targeted to achieve an overall best practice level in all areas of BS7799, but focusses on operational aspects. Where the other three IT security initiatives consist of clearly defined projects, the fourth initiative is more a collection of countless small and medium tasks and activities—all aimed to improve operational effectiveness.

Emphasis is placed on the improvement in documentation and control of IT internal processes (e.g., with service level agreements). Today, business-critical servers are all redundant and situated in highly protected environments (i.e., data centres or server rooms). Although Swiss Re runs a duplicate data centre, business-critical information is backed up to an additional remote site.

The Planned Evolution of Security Over Time

Of course, the implementation of the four IT security initiatives should improve the overall level of security dramatically. **Figures 5** and **6** show the planned improvements over time. Whereas the IT security radar chart "only" shows the general improvement in complying with best practice, the IT security risk landscape shows the individual improvement for each risk scenario. Generally, the goal for most scenarios was to move down left toward the light shaded areas shown in **figure 6** —as far as this could be achieved in a cost-effective way.

Figure 5—IT Security Radar Chart
(Improvements After Implementation of All IT Security Initiatives)

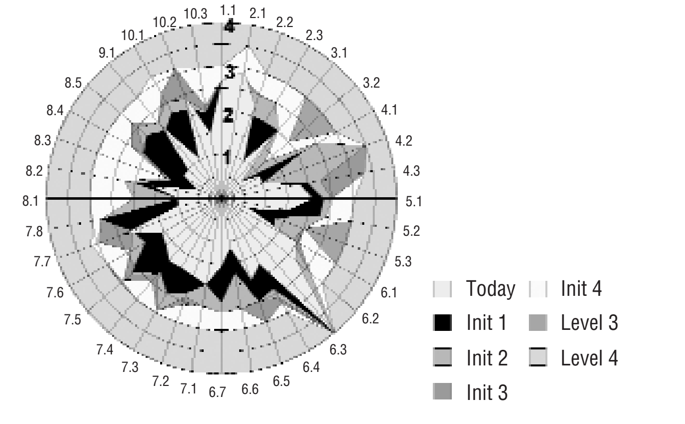
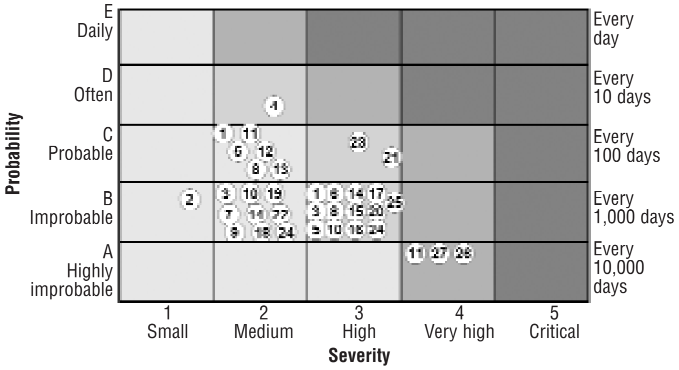


Figure 6—IT Security Risk Landscape
(Improvements After Implementation of All IT Security Initiatives)



Where Does Swiss Re Stand Now?

By implementing the four strategic IT security initiatives, Swiss Re was able to achieve the planned improvements as shown in **figures 5** and **6**—though it took some time to build up sufficient momentum. The slow start was due mostly to organisational issues, e.g., finding and hiring skilled staff, and the time it generally takes before security measures are developed and implemented.

During the past years, Swiss Re regularly performed reassessments of the maturity level of implemented good practice (i.e., the IT security radar chart) and the risk scenarios (i.e., the IT security risk landscape). These self-assessments showed that in some cases achievements were partly offset by the changes in information technology and business issues.

To counterbalance the home-grown self-assessment, in 2003 Swiss Re took part in a security benchmark of the Information Security Forum, where Swiss Re ranked 31 of 98 ISF participating members. (ISF is an international association of more than 250 leading organisations and offers a wide range of IT security standards, guidelines, tools and checklists.) This proprietary ISF benchmarking methodology also allowed the presentation of the results based on BS7799, so these results could be compared with the internally performed self-assessments. The comparison showed that the internal self-assessment (based on BS7799) and the external benchmark (based on an ISF proprietary method) were almost identical, where the (minor) differences could be explained through the different ways of measuring.

Outlook

Security is (of course) an ongoing process. All too often, progress in one place is offset by increased risks in another. Today, the main issues that make it more difficult to achieve a high level of IT security are:

- New technologies (e.g., wireless LAN, Bluetooth)
- New devices (USB-attachable storage, PDAs, Blackberry)
- Still higher complexity in technology and business processes
- More automation leading to less reaction time
- More aggressive viruses and other malware
- Growing mobility of users

This is compounded by the changing legal and regulatory environment with (sometimes) contradictory requirements, the growing external dependencies on utilitarian services (e.g., exposure to terrorism) and the ongoing trend of outsourcing.

Swiss Re is looking into a new IT security strategy that will supersede the existing one. The "old" strategy with the four strategic initiatives was focussed on improving the (at that time) not-so-good situation. Now that Swiss Re has achieved a high level of maturity in regard to IT security, a different kind of strategy is needed to help maintain this level in light of all the new challenges. This will be a new story to tell in future.

Peter R. Bitterli, CISA
is an independent consultant who for the past six years has been substantially involved in the IT security activities of Swiss Re. Bitterli has more than 20 years of experience in audit, security and governance of information systems. He is the author/teacher of a successful 17-day CISA review course. Moreover, he has trained hundreds of auditors and IT professionals in topics ranging from IT audit and security to IT governance and IT risk management, and has been a speaker at many international conferences. Bitterli is a founding member of the ISACA Switzerland Chapter and a member of the chapter board. He can be reached at *prb@bitterli-consulting.ch*.

Thanks also go to Daniela Gschwend, CISA, IT governance officer for Swiss Re, for her support in realising this article.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. Information Systems Control Journal does not attest to the originality of authors' content.

www.isaca.org